US-China Law Review, March 2023, Vol. 20, No. 3, 113-125
doi:10.17265/1548-6605/2023.03.003

The Impact of Russia-Ukraine Cyberwarfare on the Application of the Right to Self-Defense in Cyberspace and Implications

HE Xiaotong
University of International Business and Economics, Beijing, China

The Internet plays a vital role in the life of every country, and cyberspace is essential for economic development and political communication. However, the development of the Internet has also brought about a new form of warfare between countries, that is, the use of the Internet to launch attacks that cause economic or human damage to a country. The question of how to redress an attack on a country through the Internet has become an urgent issue. This paper analyzes the importance and characteristics of cyberwarfare in modern warfare against the background of the Russia-Ukraine conflict in 2022, explores the concept of the right to self-defense in cyberspace and the dilemma of its application, and concludes with recommendations and insights.

Keywords: Russia-Ukraine, cyberwarfare, self-defense, use of force

Introduction

The primary purpose of the Charter of the United Nations (hereinafter UN Charter) is world peace, which is also a State of affairs pursued by the international community. In order to avoid world war recurrence, the principle of prohibition of the use of force is enshrined in Article 2(4) of the UN Charter, which prohibits the threat or use of force by States in international relations (Etezazian, 2016). However, Article 51 of the UN Charter is an exception to Article 2(4), insofar as Article 51 gives States the right to justify the use of force in specific circumstances (Chinkin & Mary, 2017, p. 129). The difference is that the form of modern warfare is no longer limited to "traditional warfare"; "cyberwarfare" being a paradigmatic example. Indeed, cyberwarfare is more secretive and is not necessarily associated with physical violence, unlike traditional warfare which is characterized by destruction and bloodshed.

In recent years, tensions between Russia and Ukraine have gradually escalated and cyberwarfare has become one of the main strategic tools between the two sides. In addition to direct cyber-attacks that cause system paralysis or data destruction, Russian-Ukrainian cyberwarfare also involves cyber information warfare to influence and compete for public opinion. The aim is to obtain information in cyberspace, interfere with each other's communications and infrastructure, and pose a threat to the security and stability of the other country.

On February 24, 2022, a war of aggression broke out between Russia and Ukraine when the former launched a "special military operation" in the Donbas region. Cyberwarfare against Ukraine was underway long before the start of the full-scale military conflict. Russia used data wiping malware, Distributed Denial of Service attacks

HE Xiaotong, Ph.D. candidate, Law School, University of International Business and Economics, Beijing, China.

(hereinafter DDoS), and other means to carry out destructive attacks against key areas of the Ukrainian government, military, and economy, causing social chaos and communication disruptions in Ukraine, and weakening the collaborative combat capabilities of government, military, and civilian institutions. Ukraine mainly relies on IT volunteer forces, hacker organizations, and other civilian forces to carry out cyber counterattacks, while some western cybersecurity companies and experts support cyber defense.

In the context of Russia-Ukraine cyberwar, the right to self-defense in cyberspace has become an important issue, and has thus attracted considerable attention from the international community. As a new type of network information comprehensive warfare, cyberwarfare poses a serious threat to national sovereignty, security, and development. Cyberwarfare is characterized by secretiveness, and is considered capable of impacting the national security of a target country with serious consequences. However, there are many disputes and difficulties in the application of the right to self-defense in cyberwarfare under the existing international legal framework. There are no clear answers on how to define the nature and extent of cyber-attacks and when the right to self-defense can be triggered by launching an armed attack. Therefore, the research on the theoretical basis and practical construction of the right to self-defense in cyberwarfare is conducive to clarify normative frameworks of international law, safeguarding national sovereignty and security in cyberspace, and maintaining the international order.

Clarification of the Concept of Self-Defense in Cyberwarfare

Sovereignty in Cyberspace

Comprising of a conglomeration of information technology, the likes of Internet, communication networks, and the computer information system, cyberspace has swiftly emerged as an indispensable element of quotidian existence across the global spectrum. Although it follows the rules set by human beings, cyberspace does not have a clear boundary. Cyberspace is dynamic and transcends national borders, thereby making it difficult to regulate across national jurisdictions. In addition, compared with traditional armed warfare, the limitations of time, space, distance, and cost to conduct cyberwarfare are greatly reduced. Therefore, cyberspace has become an emerging theme in contemporary conflict, and there is a great probability that countries will be the first to trigger war using cyberspace in the future. In short, the question of whether cyberspace belongs to the sovereignty of a country is as important as that of traditional space.

The principle of sovereign equality, established in Article 2(1) of the UN Charter, is a fundamental principle to be observed by all States in the international community. Sovereignty implies the supreme power and authority of a State over its territory and people, and is characterized by freedom from external interference by other States. The emergence of Internet technology has made the world more interconnected, therefore arguably making it the fifth “indispensable domain” for human production and life after the sea, land, airspace, and outer space (Clarke & Knake, 2019). At the international level, the UN General Assembly adopted the UNGEE Resolution (A/68/98), which states: “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory”.[1] The core principle of the Resolution is the acknowledgement that cyberspace is subject to the same rules of sovereign

[1] Article 20, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, https://dig.watch/wp-content/uploads/A_68_98_E.pdf (visited on 17 April, 2023).

equality that exist in the UN Charter (Huang, 2017). At the domestic level, Article 1 of the Cybersecurity Law of the People's Republic of China, enacted by China in 2016, states that one of the purposes of the law is to maintain sovereignty in cyberspace.[2] Although the United States does not have an explicit cyber sovereignty law, in practice its government exercises considerable control and intervention capabilities in cyberspace. For example, the Patriot Act expanded the scope of government surveillance and searches of cyber communications and increased efforts to combat cyber terrorism.[3] From the above legislative activities, it can be seen that almost countries recognize that cyberspace is an extension of State sovereignty.

The Definition of Cyberwarfare

There is currently no unified definition of cyberwar in the international community, and different countries and organizations may have different views and interpretations. The concept of cyberwarfare was first put forward in 1993 in an article named "Cyber Warfare is Coming" published by RAND Corporation, an American think tank. The article postulated that cyberwarfare constitutes a series of attacks and defensive actions against the enemy's network information system, aiming at disrupting and destroying its network information system to ensure the normal operation of its own network information system. In *Cyber Warfare*, a book co-authored by Richard Clarke and Robert Knake, former US national security advisers, cyberwarfare is defined as the practise of a nation-State damagingly entering another State's computer system or network (Clarke et al, 2014). Recently, the US military has put forward a new concept of cyber operations, trying to integrate new capabilities and form new advantages under the framework of joint cyber operations. It can be seen that cyberspace is regarded as an important war space, and cyberwarfare will become one of the most important modes of combat in the future.

Compared to traditional warfare, cyberwarfare has several qualities. First, cyberwarfare is extremely stealthy and difficult to trace. Cyberwarfare does not require an open declaration of war and can infiltrate, disrupt, or manipulate the enemy's network information systems without alerting the enemy. And the attacker can attack through anonymous networks, proxy servers, and malware, so as to achieve the purpose of hiding their identity and whereabouts. This leads to difficulty in identifying the source of the attack and the responsible subject in the act of cyberwarfare. Second, the attacks in cyberwarfare can cross national boundaries. The combat space of cyberwarfare extends around the world, meaning cyberspace is not constrained by physical geographic limitations. In other words, cyberwarfare can cross national boundaries and geographic areas to attack any target connected to the Internet. Third, the form of cyberwarfare available to the attacker is very diverse. Cyberwarfare uses a variety of attack methods and technical means. Attacks can be traditional viruses, Trojan horses, and Worm attacks, or more advanced phishing, Distributed Denial of Service attacks, ransomware, and Advanced Persistent Threats (hereinafter APTs). The diversity of attack methods increases the complexity and level of harm cyberwarfare is capable of inflicting on targets. Finally, the operational process of cyberwarfare is extremely fluid, and the attack's strategy and tactics may change at any time, such that cyber strikes are over before one side realizes that cyberwarfare has begun. This mutability makes the effects and impacts of cyberwarfare attacks

[2] Article 1, Cybersecurity Law of the People's Republic of China: This Law is formulated so as to ensure cybersecurity, to preserve cyberspace sovereignty, national security, and societal public interest, to protect the lawful rights and interests of citizens, legal persons, and other organizations, and to promote the healthy development of economic and social informatization.

[3] Article 201, Article 206, Article 214-216, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

potentially unpredictable, and both attackers and defenders may face unexpected situations and challenges. Although there are major differences between cyberwarfare and traditional warfare, the hazards that war brings to both the national and international level cannot be ignored.

Information technology began to develop rapidly by the early 1970s. The popularization of the computer network in every facet of social life also leads to the emergence of cyberwarfare as an unintended consequence. One early use of cyberwarfare occurred during the 1991 Gulf War, when the United States used a printer chip virus to disable Iraq's computerized air defense systems. In 2007, Estonia suffered a massive cyber-attack from outside. In 2022, a full-scale military conflict broke out between Russia and Ukraine, and the two sides engaged in a fierce confrontation in cyberspace. Under the narrow definition of "war" in international humanitarian law, most current cyberwarfare attacks are not in physical space and to some extent cannot be defined as actual war. But in terms of the function of cyberwar, like traditional war, cyberwar can achieve the function that "war" should have. There is no doubt that cyberwarfare will have different effects depending on the means and methods used, as well as the intention of the party committing the act. The most direct impact is the damage or destruction caused by cyberwarfare to the target computer or network, such as data loss, system breakdown, and communication interruption. Indirect influence refers to the influence of cyberwarfare on the politics, economy, and society of the target country or organization, such as panic, chaos, division, and negative public opinion. Traditional warfare typically involves the use of weapons and troops against an enemy, requiring more resources, personnel, and time, often resulting in extensive physical damage and loss of life, as well as environmental, social, and economic devastation. In contrast, cyberwarfare has the potential to be more consequential than traditional warfare because it can weaken an enemy, gain an advantage, and even change the course of a war without resulting in death or physical harm. It can be seen that cyberwar is a new kind of war as well as a new threat of war. The impact of cyberwarfare is not to be underestimated. It may have a profound impact on the target nation or organization, and even change the international landscape and strategic balance.

Doctrine of the Right to Self-Defense in Cyberspace

Right to self-defense and conditions of application. The concept of the right to self-defense is derived from customary international law. In accordance with UN Charter Article 51,

> the natural right of individual or collective self-defense shall not be considered prohibited in the present UN Charter until the Security Council has taken measures necessary for the maintenance of international peace and security when any Member of the United Nations is attacked by force.

According to the article, a sovereign State's right to self-defense is inviolable and inherent. The implementation of the right to self-defense needs to meet four requirements. A member State must first be attacked with force before exercising the right to self-defense (Alder, 2013). Second, the nation under assault by force is the subject of the right to self-defense, while the aggressor is the object of the right to self-defense. Additionally, the right to self-defense is used following an armed attack until the Security Council takes action that is required for the preservation of global peace and security. Finally, the standards of necessity and proportionality must be upheld while determining the boundaries of exercising the right to self-defense.

Qualifying "force" in cyberwarfare. The prerequisite for determining whether an attack in cyberwarfare constitutes a use of force is to determine whether the use of cyber technology to carry out the attack falls within

the prohibition on the "use of force" as stipulated in Article 2 of the UN Charter. According to international law, the extent of the harm a cyber-attack results in determines whether it constitutes a "use of force" or a "attack by force" (Zhang, 2021). If the consequences from a cyber-attack are comparable to those of traditional warfare, cyber activities may qualify as a "armed attack" or "use of force", invoking the right to self-defense.

The prohibition of the use of force is an important principle in international law and is aimed at maintaining international peace.[4] The term "an armed attack occurs" is used in Article 51 of the UN Charter as an exception to that rule to make it clear that the right to self-defense presumes the presence of an armed attack. Due to differences in history, culture, and politics among countries, the terms "use of force" and "armed attack" have yet to achieve a common understanding, and the UN Charter has not yet given a conceptual interpretation and clear distinction between these similar terms (Yuan & Liu, 2021). Regarding how the phrase "use of force" is to be interpreted in Article 2 of the UN Charter, there are two opposing viewpoints in scholarly circles. One group of scholars has interpreted the term "force" in a narrow sense, meaning that force in this context refers only to the use of military force (Brownlie, 1963, p. 362). In contrast, other scholars believe that the term "force" should be interpreted broadly, so that force can be armed or unarmed in nature (Schachter, 1984). In this way, the use or coercion of economic, political, and diplomatic means between States would be considered a "use of force" (Daniel & Matthew, 2002, p. 5). However, since the inception of the Internet and evolving global order, the use of armed force has become significantly less common. Rather, the use or threat of the use of unarmed force is more commonplace, as typified by the many "trade wars" that occur between nations. Such a "trade war" would be fatal to small and medium-sized countries as well as emerging countries. If non-armed forces such as political and economic powers are not included in the definition of "use of force", then it is arguable that the scope of the UN Charter is limited, since such types of force are capable of threatening world peace. In addition, NATO's Cooperative Cyber Defense Center of Excellence (hereinafter CCDCOE) published the Tallinn Manual in response to the serious consequences associated with Russia's cyber-attack on Estonia. The 2.0 version of the manual clearly stipulates that when a cyber-attack reaches a certain scale and causes serious casualties and property losses, it is regarded as a cyber force attack (Schmitt et al., 2013, p. 20).

The right to self-defense applies to cyberspace. Cyberwarfare is a type of warfare conducted in cyberspace, which is a virtual space, unlike traditional physical space. In this virtual space, if a country is attacked by a cyber-attack, whether it can counterattack with cyber self-defense is a question that needs to be explored. The existing law of armed conflict was developed for traditional hot wars and may not be applicable for cyberwarfare. But there are also many connections and similarities between cyberwarfare and traditional warfare, and it can be argued that the battlefield has simply shifted from physical to virtual, yet the damage effects can be the same. Moreover, according to the ICJ, the existing rules of international law can be borrowed for the newly emerged forms of warfare.[5] So it can assume that the doctrine of the right to self-defense can also be applied to cyberwarfare. In recent years, the cyberwarfare that has occurred, represented by the use of the ShockNet virus, has harmed political and economic growth of numerous nations in different ways. In the face of increasingly

[4] Article 2, UN Charter: All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

[5] International Court of Justice, "Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion", https://www.icj-cij.org/case/95, (visited on 22 April, 2023).

frequent and serious cyber-attacks, countries have adopted the principle of timely detection and timely counterattack, in an effort to counteract cyberwarfare. Therefore, in practice, it must acknowledge that the doctrine of self-defense exists and that the target countries have the right to use reasonable and legal ways to conduct cyber self-defense.

The Dilemma of Applying the Right to Self-Defense in Cyberspace in the Russia-Ukraine Conflict Cyberwar and the Attendant Implications

The Russia-Ukraine Conflict Highlights New Challenges and Dilemmas in the Application of the Right to Self-Defense

The scope of the object of the right to self-defense is unclear. A member State may exercise their right to self-defense, according to Article 51 of the UN Charter, however it is not specified whether the object of self-defense is a State or another subject. In Article 51, the objective of the right to self-defense is implicitly understood as the subject of launching military action. However, since the objects are not listed one by one in the articles, there is some dispute over whether subjects other than the State can be the object of the right to self-defense (Tsagourias, 2016).

For non-State actors, some of which are terrorist organizations, there is no legal recourse to self-defense when a State invades the territories over which they exercise control. If they existed independently, then these organizations would no longer be organizations but could claim that they are a State. Terrorist organizations are often attached to a State or hiding in the territory of a State. Therefore, other sovereign States will unavoidably be involved if the right to self-defense is used against a terrorist group.

According to the principle of State responsibility, the position of the State in which the terrorist group is located should be used to determine whether a State actor is recognized as the subject of the right to self-defense. If a State has complete control over and is involved in the planning of a non-State actor, then that State may exercise the right to self-defense against that actor (Tsagourias, 2016). The granting of financial autonomy, housing, equipment, or help by States to non-State actors should be included in the notion of complete control, such as when designing military plans in violation of international law and carrying out relevant instructions. Complicity is defined as active or passive support for non-State actors, such as sheltering or tolerating them. This implies that States bear some responsibility for armed attacks by non-State actors against the affected State. On the contrary, a State is not accountable and the damaged State cannot use the right to self-defense against it if it is powerless to stop or restrict the actions of a non-State actor.

Similarly, the subject exercising the right to self-defense in cyberwar is undoubtedly the member State of the United Nations, but the identification of the applicable object of the right to self-defense in cyberwar is also controversial. Unlike active combat, cyberwarfare requires only one computer to trigger a war. There are different subjects involved in the cyberwar between Russia and Ukraine. In order to resist Russia's digital invasion in cyberspace, Ukraine organized and called on IT Corps and Hacker Corps to launch cyber-attacks against Russian banks, enterprises, and government agencies, and set up Legion channels on the Communist Party of China. In addition, several hacking groups have explicitly backed Ukraine, including Anonymous, the world's largest group of hackers. From Ukrainian underground hackers, Russian private "cyber guards" to ransomware organizations and international hacking organizations, various forces have been active in the Russo-Ukrainian

cyberwar. It can be seen that cyberwar involves a wide range of subjects, ranging from States and State-supported spies or hackers to unorganized individuals, hacker alliances, or cyber terrorist organizations. The former constitutes emanations of State and thus gives rise to State responsibility, while the cyber-attacks by individual attackers, unorganized groups of hackers, and other subjects cannot be considered State acts and therefore falls short of the right to self-defense. If the right to self-defense cannot be exercised against cyber-attacks by non-State actors such as unorganized hackers, then it will make the international social order unsafe. In practice, various States have varying perspectives on whether non-State actors can be the target of self-defense in actuality. Several nations, including Israel, the Netherlands, and the United States believe that both State and non-State actors can be subject to the right to self-defense (Zhang, 2021). Other countries consider specific non-State actors like ISIS to be the subject of the exercise of the right to self-defense, such as Germany and France (Zhang, 2021). Cyber-attacks by non-State actors on other countries are often regulated by the domestic laws of that country. As an extension of national sovereignty, once a member State combats non-State actors without the permission of the territorial State, it violates the sovereignty of other nations in cyberspace. Moreover, in the case of existing cyber "wars", few have resulted in large-scale casualties and economic damage. And in international humanitarian law, sporadic attacks and attacks that are not widespread enough do not lead to the existence of an armed conflict. Therefore, it is not legally possible to resolve cyber-attacks by exercising the right to self-defense unless the attacks are of a sufficient intensity. At the present stage, blindly expanding the scope of the right to cyber self-defense will only backfire and lead to more tension in the cyber order.

The timing of the armed attack is unclear. As previously mentioned, Article 51 of the UN Charter only mentions the right to self-defense in the case of "an armed attack", but it makes no reference of the precise moment the armed attack occurs. There are so two different types of prerequisites for exercising the right to self-defense (Ørebech, 2014).

The first view is the expansive interpretation, which means that self-defense can be invoked following the real happening of an armed attack, as well as to the threat and imminence of a possible armed attack (Green, 2015). A potential armed attack is when a State accesses weapons of mass destruction, like nuclear weapons, and could threaten another State's national security. An imminent attack occurs when a country prepares to conduct an armed attack on another country, such as mobilizing troops to militarize a national border or conducting air patrols in an intimidating fashion. This implies that a country may engage in an armed attack before being attacked by another, which is known as anticipatory self-defense. There are many varied perspectives on anticipatory self-defense as well, but those who state that anticipatory self-defense is legal generally view urgency as a criterion for legitimating its use. Another theory of anticipatory self-defense holds that nations have the right to take pre-emptive action against specific nations and non-State actors to defend themselves when the time and location of an enemy attack are uncertain. This theory was advanced by the United States in its national security strategy from 2002. This principle is known as preemptive self-defense, and was exhibited by the US air force following the use of targeted killings against suspected terrorists during the Iraq War. On the basis of this theory, the concepts of "armed attack" and anticipatory self-defense are often considered disproportionate and at odds with the customary international law definition of self-defense. Applying the principle of preemptive self-defense may not only violate the UN Charter's prohibition on the use of force, but also lead to the abuse of the right to self-defense.

In contrast to the expansive interpretation, there is the restrictive approach to self-defense, which asserts that member States only use the right to self-defense in the event of an actual armed attack (Green, 2015). At present, much of the scholarship suggests that the international community is more inclined to support the narrow interpretation of self-defense according to the literal wording of Article 51 (Corten, 2005). Moreover, the application of the expanded interpretation as developed by the Bush Administration may lead to the destruction of the legal framework prohibiting force. In addition, the expansive interpretation also legitimates the preemptive self-defense of countries, making some countries with ulterior motives retaliate against other countries under the pretext of "imposing" or deliberately fabricating false information to justify jus ad bellum. It is worth noting that the draftsmen of the UN Charter could not have envisioned the rise of the Internet and the manner in which it has altered the landscape of contemporary warfare. Cyberwar can not only cause network paralysis, serious information leakage can potentially cause a country's economy to suffer heavily. If the current view of the right to self-defense is interpreted in a restrictive way, this may leave the target country with no legal recourse to lawfully defend itself against hostile cyberattacks.

The applicability of anticipatory self-defense in cyberwarfare is still a matter of debate. There are two kinds of situations to launch cyber-attacks. In the first situation, cyberwarfare acts as a prelude to traditional war, which means that traditional actions are imminent after launching a cyber-attack (Zhang, 2021). The cyberwarfare that took place before the commencement of the Russo-Ukrainian War is a case in point. However, the highly covert nature of cyberwarfare and the lack of concrete evidence capable of making the causal link between the aggressor State and the act, make it difficult to prove the existence of anticipatory self-defense. In the second situation, a cyber-attack emerges independently, followed by the imminent threat of a more destructive cyberwar (Zhang, 2021). In this case, it is difficult to identify the time and damage consequences of cyberwarfare after launching cyber-attacks, and according to the principle of necessity and proportionality, a country can remove threats by non-forceful means such as removing virus software, rather than exercising anticipatory self-defense.

In general, no expansionary and restrictive doctrine is completely correct and applicable to cyberwarfare. Expansionism and restrictivism should be combined organically, taking their strengths and eliminating their weaknesses. Therefore, in expansionism, the principle of preemption that is about to happen and be intercepted should be combined with the principle of limitation, and the Bush principle should be denied. A State may only exercise the right to self-defense in the case of an armed attack, according to the restricted principle. It is therefore logical to include the theory of expansion, which will not only help in the fight against terrorists, but will also lessen the harm brought on by armed attacks. If the location and timing of terrorist attacks are not known with certainty, this might be used as justification by one country to invade another, which could result in misuse of the right to self-defense and be harmful to world peace and stability. As a special form of act of warfare, cyberwarfare is characterized by the ability of attackers to conceal their identities and launch attacks quickly, Thus, adopting the principle of preemption can help detect and stop potential cyber-attacks in advance and protect the interests of the State and the public. Similar to the treatment of terrorism mentioned above, the restrictivism in cyberwarfare cannot be limited to exercising the right to self-defense only in the case of a substantial cyber-attack on the State. Adopting only restrictivism would miss the chance to stop potential cyber-attacks in time, leading to greater damage and threats. Therefore, the expansionism and restrictivism of cyberwarfare should be combined to ensure that necessary cyber self-defense measures are taken in compliance with legal, moral, and international norms.

Controversy over the exercise of the right to collective self-defense. When a nation with which it has close links is attacked by force by another country, regardless of whether it is attacked or not, it has the right to intervene and stop the attack with force. This is known as the right to collective self-defense. The right to individual or collective self-defense is enshrined in Article 51 of the UN Charter. This means that if the right to collective self-defense is to be exercised, the conditions set out in Article 51 must be met. There are different views in the theory of collective self-defense on the Internet. Some scholars believe that cyberwar is not much different from traditional war, and some countries with underdeveloped Internet can ask the international community for help (Schmitt & Vihul, 2017). However, some scholars believe that there is only the right of individual self-defense but not the right of collective self-defense in cyberwar (Waxman, 2011). The first requirement for the exercise of the right of collective self-defense is that a State must make an explicit request for another State to exercise the right to self-defense, which was established in the Nicaragua case in 1986. In that case, the judges restricted the right to collective self-defense to only apply in cases when a State declares an armed attack and requests assistance from other States. This principle was also confirmed in the 2003 Oil Platform case.[6] Besides, the need for the State to make a clear demand as a prerequisite for the exercise of the right to self-defense is significant. The lack of clear provisions will lead to retaliation by one country against another under the pretext of exercising the right to collective self-defense, which is detrimental to the stability of the international situation. Furthermore, the legality and reasonableness of a State's request to exercise the right of collective self-defense as a trigger for an armed attack against another State are questionable (Christine & Mary, 2017, p. 129). Some scholars have questioned the conclusion reached in this case, arguing that whether or not a State exercises its right to collective self-defense should be based solely on its will, without covenantal or legal restrictions on it (Visser, 2020). It is an act of "justice" for a country to take the initiative to help a country suffering from cyberwar, and it is also a process of saving others as well as oneself. But only a small minority holds the view that unrestricted participation in either traditional or cyberwarfare would cause turmoil in the international community and, from the perspective of modern society, is contrary to international norms and behavior, such as Article 2 of the UN Charter.

Some scholars have argued that there are major differences between cyberwarfare and traditional warfare in terms of how they are supported. Traditional warfare tends to provide assistance in the form of human and financial resources as well as lending passage. In cyberwarfare, on the other hand, what the attacked country needs most is often technical support, thus establishing technologies such as firewalls to eliminate the harm. Some scholars also argue that the right to collective self-defense does not exist in cyberwarfare similar to that which can be exercised in traditional warfare. Because the network is so covert, it can hide the identity of the attacker so well that the attacker cannot be identified. The attacker could then be a national of any country, a national of a member State of the coalition, or a national of a supporting country. In this way, the right to collective self-defense cannot be exercised against a covert cyber attacker, as in the case of the United States Prism Gate program. Under this perspective, each State should be responsible for protecting its own cyber security on its own and cannot rely on the collective defense of other States. This view emphasizes national sovereignty and independence, arguing that the special nature of cyberwarfare makes the right to collective self-

[6] Islamic Republic of Iran v. United States of America (1992-2003).

defense difficult to apply and that each country should take the necessary measures on its own to defend itself against the threat of cyber-attacks.

As for the ongoing cyberwar in the Russia-Ukraine conflict, there are different views on whether a Russian cyber-attack would trigger Article 51 of the UN Charter and cause other States to exercise collective self-defense. Some argue that collective self-defense is triggered by the premise that Russian cyber tactics are qualified as "armed attack" and that cyber operations lead to serious consequences. The opposing argument is that, due to the covert and anonymous nature of cyberwarfare and the fact that Russia has the sufficient cyber technology to hide its tracks, it is challenging to identify the target of the cyberattack, making Article 51 collective self-defense difficult to enact.

Impact of the Russia-Ukraine Conflict on the Application of the Right to Self-Defense in Cyberwarfare

The Russia-Ukraine war is a complex geopolitical conflict in which the application of the right to self-defense in cyberwarfare has been widely discussed. The cyberwarfare launched by the conflict between Russia and Ukraine has both positive and negative effects on the application of the right to self-defense in cyberspace.

The positive impact is reflected in the following aspects. First, the Russia-Ukraine cyberwar promotes the international recognition and practice of the right to self-defense in cyberspace. The outbreak of cyberwarfare has prompted more countries to once again recognize the threat of cyber-attacks to national security. Therefore, more countries support and recognize the legitimacy of the victim country's exercise of the right to self-defense in cyberspace, which helps to strengthen the international community's recognition of the actions of self-defense in cyberspace, so as to provide more legitimate means for the victim country to respond to cyber-attacks (Schmitt, 1999). And, the cyber-attacks during the conflict between Russia and Ukraine have forced the latter to improve its cyber defense capability to protect the security of its cyber space. The EU, the US, and other countries have learned from this and strengthened their own cyber defense measures, thus promoting the practice of the right to self-defense in cyberspace. Moreover, the Russia-Ukraine cyberwar has promoted the formulation and improvement of international legal rules for the right to self-defense in cyberspace. While traditional international law has focused on various forms of warfare, some controversies and challenges remain, despite the fact that cyberwarfare is a new means of warfare whose characteristics and implications have been defined and recognized to some extent in international law. The emergence of cyberwarfare has triggered international discussions on the interpretation and implementation of the principles and rules of international law, particularly concerning the right to self-defense, national sovereignty, and the use of force (Roscini, 2014, p. 1). This creates additional difficulties for the formulation and application of international law. The international community is beginning to realize the inadequacy of the existing international legal framework in cyberwarfare, so there are calls to advocate the formulation of international legal rules related to the right to self-defense in cyberspace. This includes legal frameworks and institutions against cyber-attacks, cyber espionage, and cybercrimes to ensure security and stability in cyberspace. Such calls have pushed the international community to conduct more in-depth studies and discussions on the right to self-defense in cyberspace, and are expected to establish a more specific legal framework for the right to self-defense in cyberspace. And, Ukraine has taken a series of cyber counter-actions in cyberwarfare, and publicly disclosed related cyber-attack incidents and technical details. This provides a

concrete case for the international community to study the practical application and definition of the right to self-defense in cyberspace.

The negative effects are shown in the following three aspects. First, disputes over the application conditions and limitations of the right to self-defense in cyberspace are intensified. The application conditions and limitations of the right to self-defense in cyberspace caused by the conflict between Russia and Ukraine have attracted widespread controversy. Different countries and international organizations differ on the specific conditions for the application of the right to self-defense in cyberspace, such as the definition of the timing, scale, and means of exercising the right to self-defense. The complexity of the conflict between Russia and Ukraine makes the discussion of these issues more complicated and difficult, and no consensus can be reached. This has intensified disputes over the application conditions and limitations of the right to self-defense in cyberspace, posing challenges to the formulation and implementation of relevant international legal rules. In addition, the Russia-Ukraine conflict may increase the risk of abuse and misuse of the right to self-defense in cyberspace. The exercise of the right to self-defense in cyberspace requires strict compliance with the principles of international law, including the principles of necessity and proportionality. However, in a complex cyberwarfare environment, it becomes difficult to distinguish the source and purpose of cyber-attacks, which can easily lead to miscalculation and overreaction. Some countries may use the right to self-defense in cyberspace to carry out unauthorized cyber-attacks on other countries to fulfil their own interests. This situation of misuse could lead to further instability and escalation of conflicts in cyberspace. Finally, the dispute over the right to self-defense in cyberspace arising from the Russia-Ukraine conflict could pose a threat to the balance and harmonization of other principles and obligations of international law. For example, conflicts may arise between the right to self-defense in cyberspace and the values and principles of national sovereignty, non-interference, and international human rights law. In practice, how to balance the right to self-defense in cyberspace with other principles and obligations of international law has become a complex issue. The impact of the Russia-Ukraine conflict may further increase the challenge of such balance, which requires in-depth discussion and exploration by the international community.

Suggestions

With the rapid development of information technology, the threat of cyberwar is increasing. During cyberwarfare, ensuring a country's right to defend itself is particularly important. Under Article 51 of the UN Charter, every State has the inherent right to defend itself in the event of an armed attack. However, there is still no clear consensus in international law on whether cyber-attack constitutes force attack, unclear object giving rise to the right to cyber self-defense, the temporal factors of a cyber-attack, and when cyber means can be used for self-defense. A clear legal framework should be developed at the international level to guarantee that the right to self-defense is correctly applied and defined in cyberwarfare. This will help to encourage the development of the notion of an applicable right to self-defense. This includes the definition of cyber-attacks, determining the extent and impact of attacks, the scope of objects applicable to the right to self-defense, and the methods to judge the source of attacks. Such a legal framework would provide a clear legal basis for the norms of cyberwarfare, helps countries better exercise the right to self-defense, and ensures the legality and rationality of exercising the right to self-defense. Furthermore, the international community should pay attention to the development of network technology in addition to updating legal regulations. Technological development can provide more

options and means for exercising the right to self-defense, such as strengthening network security defense and ensuring the authenticity and integrity of online information.

The war between Russia and Ukraine is a complicated conflict involving many actors. Besides the military battlefield, there is also the information battlefield. The West is conducting a public opinion offensive against Russia through media, social platforms, hacker organizations, and other means, in an attempt to gain support and sympathy from the international community and weaken Russia's influence in Ukraine. Russia has defended itself through its media, diplomatic channels, and civilian forces, stressing its legitimacy in protecting the interests of residents in eastern Ukraine and preventing NATO expansion. This cyberwar has not only affected the perception and judgement of governments and the public, but also exposed the imbalance, injustice, and insecurity in global cyberspace governance. Therefore, in the current situation, coupled with the characteristics of transnational and anonymous cyberwarfare, it is necessary to strengthen multilateral cooperation to jointly deal with cyber-attacks. For instance, countries should actively cooperate and share intelligence, technology, and experience to jointly deal with cyber threats. In addition, an international mechanism and cooperation platform for cyber security should be established to carry out international dialogue and cooperation in the field of cyber security and seek consensus and solutions within the framework of the United Nations and other frameworks. At the same time, cooperation with non-governmental organizations, academia, and industry should be strengthened to form a multilateral mechanism for the formulation of international legal rules. In addition, countries should enhance their awareness and capability of cyber security to better cope with cyber-attacks and safeguard their right to self-defense. The State should strengthen the construction of cyber defense and recovery capabilities, and improve the early warning and response capabilities to cyber-attacks. These steps will strengthen cybersecurity education and training, and increase the quantity and quality of cybersecurity professionals. At the same time, individuals should also enhance their awareness of network security and take necessary protective measures to reduce the risk of network attacks. Countries and the public should work together to build an open, cooperative, secure, and orderly global cyberspace order.

References

Alder, M. C. (2013). *The inherent right of self-defence in international law* (Vol. 19). New York: Springer.

Brownlie, I. (1963). *International law and the use of force by states.* Oxford: Oxford University Press.

Christine, M. C., & Mary, K. (2017). *International law and new wars*. Cambridge: Cambridge University Press.

Clarke, R. A., & Knake, R. K. (2019). *The fifth domain: Defending our country, our companies, and ourselves in the age of cyber threats.* London: Penguin Press.

Clarke, R. A., Knake, R. K., & Clarke, R. A. (2014). *Cyber war: The next threat to national security and what to do about it.* Old Saybrook: Tantor Media.

Corten, O. (2005). The controversies over the customary prohibition on the use of force: A methodological debate. *European Journal of International Law, 16*(4), 803-822.

Daniel, B., & Matthew, W. (2022). *The dynamics of coercion: American foreign policy and the limits of military might.* Cambridge: Cambridge University Press.

Etezazian, S. (2016). The nature of the self-defence proportionality requirement. *Journal on the Use of Force and International Law, 3*(2), 260-289.

Green, J. A. (2015). The ratione temporis elements of self-defence. *Journal on the Use of Force and International Law, 2*(1), 97-118.

Huang, Z. X. (2017). "Soft power" in the game of rules in cyberspace: A review of international law in cyberspace in recent years. *Renmin University Law Review, 19*(3), 236-240.

Ørebech, P. (2014). UN Charter Article 51 and the right to "anticipatory self-defence": Validity of the US preventive war doctrine against Al Qaeda. *Middle East Critique, 23*(1), 53-72.

Rao, P. S. (2016). Non-state actors and self-defence: A relook at the UN Charter Article 51. *Indian Journal of International Law, 56*(2),127-147.

Roscini, M. (2014). *Cyber operations and the use of force in international law*. Oxford: Oxford University Press.

Schachter, O. (1984). The right of states to use armed force. *Michigan Law Review, 82*(10), 1620-1646.

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: Thoughts on a normative framework. *Columbia Journal of Transnational Law, 37*(3), 885-937.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyberwarfare.* Cambridge: Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2017). Respect for sovereignty in cyberspace. *Texas Law Review, 95*(8), 1639-1671.

Tsagourias, N. (2016). Self-defence against non-state actors: The interaction between self-defence as a primary rule and self-defence as a secondary rule. *Leiden Journal of International Law, 29*(3), 801-825.

Visser, L. (2020). Intervention by invitation and collective self-defence: Two sides of the same coin? *Journal on the Use of Force and International Law, 7*(2), 292-316.

Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of Article 2(4). *Yale Journal of International Law, 36*(2), 421-459.

Yuan, Q., & Liu, J. (2021). The theoretical basis and construction of the exercise of cyber self-defense right. *Jiangxi Social Sciences, 42*(6), 210-218.

Zhang, H. (2021). The legal uncertainty of the application of the right of self-defense in cyberspace and the expression of China's position—Reflections on recent position papers of various countries. *Social Sciences in Yunnan, 41*(6), 81-92.