Proceedings of the 3rd International Conference on Literature, Language, and Culture Development
DOI: 10.54254/2753-7064/37/20240122

Research on the Inclusion of "Being Subjected to a Cyber Attack" as a Condition for the Exercise of the Right

Ruofei Du[1,a,*]

[1]*Academy of International Law, East China University of Political Science and Law, Shanghai, 201600, China*
a. 212125011053@ecupl.edu.cn
**corresponding author*

Abstract: With the development of information technology, the scale of cyber-attacks is getting bigger and bigger, and the serious harm to national life is growing, while the relief of international law for the regulation of cyber-warfare is in a relatively blank state. Based on the traditional right, this paper will argue the possibility, necessity, jurisprudence, and practicability of including cyber attacks into the conditions of exercising the right from four perspectives (i.e., the advantages of countering cyber attacks by forces of self-defense, the exclusion of other remedies, the jurisprudential basis for the exercise of the right, as well as the study of the legislative attempts and legal achievements of the present-day in the field) in order to illustrate the rationality of the right and construct the elements and structure of the operation of this right on the basis of the law of armed conflict. The author also discusses the elements and structure of the operation of this right on the basis of the Law of Armed Conflict, in order to rationalize the proposal and make it more in line with international law's spirit; and finally, discusses the disputes over the application of this system, provides new perspectives and suggestions for examining this issue.

Keywords: cyber attack, armed attack, right, Tallinn Manual, international law

1. Introduction

In April 2017, the United Arab Emirates launched a hacking attack on Qatar's news and diplomatic pages, generating false news about Qatar's official support for Hamas and Hezbollah by massively crippling Qatar's official information technology equipment and taking advantage of the opportunity to publish fake news on the captured Qatar News and Diplomacy Network, leading to a large number of Middle Eastern countries urgently severing diplomatic relations with Qatar and a large number of Qatari expatriates being asked to A large number of Qatari expatriates were asked to leave the country within 14 days. It wasn't until Qatar's technical department regained control of its internal networks at the end of May, and with the assistance of its allies, who had uncovered the UAE's next plan of action for military purposes and urgently deployed more troops along its neighboring borders, that the cyber attacks that lasted more than a month could be contained, resulting in a serious diplomatic disaster for Qatar.

It is worth noting that the cyber attack that paralyzed the Qatari press and diplomatic network is a public authority, so if the object of a cyber attack is a civilian facility used to maintain the livelihood

DOI: 10.54254/2753-7064/37/20240122

of nationals or a lethal infrastructure, such as a water supply or electricity supply, and if it results in serious casualties among nationals, does such an act constitute an act of war? And can a country launch armed self-defense in such a situation?

2. Sources, Elements, and Exercises of the Traditional Self-defense

2.1. Art 51 of the Charter of the United Nations: Exceptions to the Absolute Prohibition of the Use of Force

An important principle enshrined in the Charter of the United Nations is the prohibition of the use of force. This principle is clearly stated in Article 2(4) of the UN Charter [1]. However, Art 51 of the Charter of the United Nations provides for the right of Member States to self-defense in the event of an armed attack [1].

Clearly, Art51 is an exemption to Art 2(4), i.e., the absolute prohibition of the use of force in principle by a few States, unless he is subjected to an attack of force by a subject, such as another State/institutional organization, in which case it is granted immunity from the use of force and may exercise the right using force to defend itself. In short, it is a balanced system of "force against force - force in self-defense". In principle, the use of force is prohibited, but when the balance of non-use of force is disturbed by the actions of a unilateral State/organization, force can be applied in a balanced manner. However, there are certain conditions for this "balanced" application: i.e., self-defense by force must meet the criteria of necessity and proportionality. As to whether armed self-defense should be initiated when "attacked by force" or after the attack is over, there is a controversy in the academic community, and the controversy is presented as a restrictive interpretation of Art 51 of the UN Charter and a customary law interpretation, i.e., the right can be exercised only when an attack by force is being carried out and an infringement is occurring, similar to the restriction on the concept of defense in the criminal law, and the restriction on the concept of defense in the criminal law. The restriction of the concept of self-defense in criminal law is a kind of lawful exemption from the use of unlawful violence in the face of real-time imminent aggression, and when the aggression stops, the right to the lawful use of force is naturally lost; while scholars who hold the view of expanding the interpretation believe that the context is not limited to the "time of an armed attack", because Article 2(4) of the Charter does not prohibit the right of customary self-defense. The right of customary self-defense is not prohibited by Article 2, paragraph 4, of the Charter, and Art 51 of the Charter is not a restrictive but an empowering provision.

2.2. Elements of the right - Encounter with Force

With regard to the definition of being subjected to an armed attack, the present articles do not provide a very clear regulation, and at present, existing international law still understands it as the use of force in the traditional sense.

There is currently an international consensus on the specifics of an armed attack, such as An imminent armed attack (proven to be taking place) e.g. missiles that have been launched from missile silos, fighter jets that have taken off from airports can be considered to be an armed attack in progress and thus triggering the right [2].

In addition, an armed attack requires a certain degree of seriousness but is not necessitated by the scale of the armed action [3]. For example, the shooting down of a civilian aircraft in response to a single sortie could be considered an armed attack and trigger self-defense. In other words, Art51 does not exclude small-scale attacks, and the author believes that the most important factor in defining whether such an attack meets the standard of self-defense is the nature of the act rather than the scale and that the nature of the act constitutes an act of war, and is sufficiently severe that it can be regarded as an attack of armed force even if the scale of the act is small and does not lead to serious

DOI: 10.54254/2753-7064/37/20240122

consequential damages, e.g., attacks on the civilian population, the facilities that nationals of the State rely on for their survival, such as water and electricity facilities, and civilian personnel carriers. The target of the attack is an important measure. The target of the attack is an important factor.

2.3. The Right to Self-defense in Exercise

2.3.1. Obligation of the Right Holder to Inform

When a State is attacked by force and exercises its right to self-defense, it has an obligation to inform the international community. This obligation is largely based on the UN Charter and the relevant judgments of the International Court of Justice (ICJ). Art 51 of the UN Charter explicitly provides for a state's right to self-defense in the event of an armed attack. Although this Article does not explicitly provide for an obligation to inform, international law generally interprets it to mean that a state exercising its right to self-defense should report its acts of self-defense to the UNSC. Such reporting helps to ensure the legality and transparency of any self-defense measures.

In Nicaragua v. United States (1986), the ICJ examined the legality of acts of self-defence and emphasized the importance of informing the UNSC. This case exemplifies the principle that acts of self-defence need to be rationalized and explained within the framework of international law.

Legal experts usually consider the obligation to inform as an implicit principle in international law. Although the Charter of the United Nations does not expressly provide for an obligation to inform, this obligation is a consensus that has developed in practice to ensure international scrutiny and assessment of acts of self-defense [4].

In summary, states should inform the international community, particularly the UNSC, when exercising their right to self-defense, in order to ensure that their actions are consistent with the requirements of international law. This obligation to inform contributes to the maintenance of international peace and security and is an important part of the norms of international law.

2.3.2. Subject of Authorization of the Legality of an Act of Self-defence

Based on the obligation of the right holder to inform, it is not difficult to conclude that the subjects of review of the legality of the right are the ICJ and the UNSC. This is also the general conclusion of the academic community [5]: According to the UN Charter, the UNSC is the principal organ for the maintenance of international peace and security and is responsible for examining the legality of acts of self-defense by member states. After exercising its right to self-defense, a state must report to the UNSC, which will review it; the ICJ (ICJ) can give an advisory opinion or rule on the legality of an act of self-defense [1]. Although the Court's decisions are case-specific, its rulings and opinions are important to the understanding of the international law principle of the right to self-defense, and similarly, the Nicaragua v. United States case was instrumental in establishing the ICJ's status as a reviewer of the legality of the right to self-defense.

2.4. Traditional International Law Regime Vacancy - Misalignment of Traditional Definition of Force and Cyber Attacks

Unlike the international community's consensus on the timing and nature of an armed attack, there is a great deal of controversy over whether a cyber attack can constitute an armed attack. The fundamental reason for this controversy is that the definition of an armed attack in Art 51 of the Charter is too vague, and the San Francisco Constitutional Convention did not provide a clear scope, while the development of time and technology has led to the inevitable diversification of the means of attack and weapons. To date, there has been no case like the Nicaragua case, which was tried and regulated by the ICJ, that includes or excludes "information network attacks" from the scope of armed

DOI: 10.54254/2753-7064/37/20240122

attacks, and the inconclusive status quo has given this topic a certain amount of room for academic discussion.

The controversy that exists in academia and practice between the weapons used and what constitutes a forceful attack raises the most important question of this paper: whether an information network attack can constitute a forceful attack. This issue can be essentially deconstructed into three questions: whether information networks can be used as weapons; whether there exists a nature of war in information network attacks that is equivalent to conventional force attacks; and whether the use of force in self-defense in response to information network attacks exceeds the bottom line of Art 51 of the Charter.

However, the vast majority of forceful attacks that exist today originate from visible weapons, whether conventional or thermonuclear, as well as some of the weapons banned by the international community, which are essentially visible and tangible, and the changes before and after their delivery are obvious. Information network attacks, on the other hand, do not meet the above characteristics, and this mismatch between traditional force and its provisions, as well as the gaps in the Charter, have added practical difficulties to the exercise of the right of self-defence against information network attacks.

In the first part of this paper, the author spends a large part of the introduction summarizing the elements of the exercise of the right, the obligation of the right holder to inform the lawfulness of the right to review the main body of the right defects, to build a clearer structure of the exercise of the right: i.e., a country suffers from an armed attack, and at the same time of real-time to the subject of the attack to impose the right proportion of force to the counterattack in self-defense, notify the UNSC of the necessary evidence, the degree of counterattack, the identity of the subject of the infringement to fulfill the obligation to inform The UNSC and the ICJ will then review the legality of their actions after the fact. The clarification of this structure will help the author to construct an analogy of the right to exercise the right against special cyber-attacks in the following section.

3. Exercise of the Right in the Context of Cyber Attacks

3.1. The Necessity of Exercising the Right to Use Self-Defense Against Cyber Attacks Exclusion of Other Remedies

3.1.1. Information Network Attacks - Catastrophic Characteristics and Their Challenge to the Traditional Right

Cyber attacks are defined as harmful and disruptive behaviors carried out through computer technology and networked systems. These attacks encompass a wide range of technological methods and targets, creating new challenges for national security and international affairs. International law scholars have identified several key characteristics and types of cyber attacks:

Anonymity and tracking challenges:

The traditional norms of international law governing acts of self-defence against armed attack are set out in Art 51 of the Charter of the United Nations [1]. However, cyber-attacks are often carried out anonymously, making it difficult to track down attackers. This uncertainty hinders the identification of the source of the attack and the development of an effective response. Art 51 requires that the UNSC be notified immediately after the exercise of the right to self-defense and that the act of self-defense must be in response to an actual attack. However, the anonymity of cyber attacks and the difficulty of tracing them may make it difficult to identify the source of the attack, which makes it difficult for States to provide corroborating evidence when reporting and affects the international community's understanding and judgment of the incident [6].

Diversified technical means of non-traditional violence:

DOI: 10.54254/2753-7064/37/20240122

Cyber attacks employ a variety of techniques, including malware, network infiltration, and denial-of-service attacks, to achieve a variety of objectives, ranging from stealing confidential data to crippling critical infrastructure. Most importantly, these means of cyber-attacks are not traditionally categorized as "armed" attacks.

Potential global threat:

Due to the connected nature of the network, cyber-attacks involve multiple countries, such as a single country and its neighboring military allies, making it necessary for the international community to coordinate its response. It also makes it more difficult for the UNSC to be able to make a resolution at short notice [7].

Physical harm no less than a traditional force attack:

Despite the large number of cyber attacks, publicly reported cases of direct human casualties are rare. This is largely due to the fact that most cyber attacks are aimed at stealing data, destroying equipment, disrupting services, or as part of information warfare, rather than posing a direct threat to personal safety.

It is worth noting, however, that as critical infrastructure and life-support systems become increasingly dependent on cyber technology, the potential threat to the safety of personnel from cyber attacks is increasing. For example, attacks on health-care systems, transportation control systems or industrial control systems may indirectly lead to loss of life or injury, especially if they are not detected and responded to in a timely manner.

To introduce some examples: the hacking of Qatar by the UAE, which resulted in a serious diplomatic incident and the expulsion of expatriates, as well as the military intent behind the cyber attacks, can hardly be considered to have reached the level of an "attack by a force of hazard".

These features of cyber attacks significantly affect the conditions under which a traditional armed attack triggers the exercise of the right to self-defense. It is increasingly difficult to assess whether a cyber attack qualifies as a self-defense response from the perspective of the traditional right to self-defense.

3.1.2. Paralysis of Nonviolent Sanctions - The Logical Imperative of Self-Defense by Force

Existing international law generally provides two types of remedies: armed remedies and unarmed remedies. As a general rule, when a sovereign State is attacked, it tends to resort to armed remedies, i.e., the exercise of the right. Why are non-violent sanctions paralyzing in the face of a serious cyber attack?

This type of relief consists of economic sanctions, political countermeasures, and other measures, the effects of which take a considerable amount of time to materialize and are difficult to respond to in response to relatively rapid aggression. This is clearly related to the characteristics of cyber attacks discussed in the previous section, and it is not difficult to conclude that cyber attacks, unlike armed attacks in terms of medium, although difficult to be evaluated as force in the traditional sense, in the era of qualitative changes in information technology, are capable of causing harmful consequences indistinguishable from their inherent warlike nature behind them, and that in such cases if a state is required to use only nonviolent sanctions, the harmful effects To require a State to use only non-violent sanctions in such circumstances would have the same detrimental effect as prohibiting a State aggrieved by substantial force from resorting to self-defense remedies, a result that would be patently absurd.

If the controversy here lies in the dichotomy between the nature of an information network attack and the implied military purpose and warlike intent behind it, and the analogy of an information network attack to "force not yet unleashed" - i.e., fighter jets still parked in hangars, missiles not yet launched from silos - it is clear that such an "attack" that has not yet taken place is not sufficient for the exercise of the right of self-defence. Obviously, such an "attack" that has not yet taken place is

DOI: 10.54254/2753-7064/37/20240122

not sufficient to meet the requirements for exercising the right. However, although the information network attack and the underlying war intent or military purpose are two acts, the difference is that the reason why the right cannot be triggered by the force that has not yet been launched is that it is in a static and static state that is difficult to subjectively assess, whereas cyber-attacks of a serious nature occur dynamically, often with the purpose of information warfare, stealing information, intelligence, and indirectly causing the loss of life and property, which on the one hand, causes physical harm, and on the other hand, is also necessary to satisfy the subsequent military intent. On the other hand, also to meet the subsequent military intentions of the preparatory conditions, in terms of the correlation between the two acts before and after it is difficult to evaluate as a split between the two separate acts if we want to analogize the attack of force, in terms of its dynamic attributes, it should be from the latter stage of the analogy of the "imminent attack of force" (confirmed to be occurring), that is, similar to the missiles that have already been launched, A fighter jet taking off, a warship leaving a harbor, etc. The international consensus is that in the face of such an attack, "preventive self-defense", i.e., pre-emption, can be triggered.

This logic is also valid for cyber attacks, and it would be absurd to allow cyber-attacks, which are relatively quick to be carried out and last a relatively long time in terms of harmful consequences, to be carried out while the attacked State can only impose non-forceful sanctions, which would be tantamount to making the State that is about to face an imminent forceful attack to wait for the harmful consequences, which is clearly in contradiction with the consensus on preventive self-defense reached in the Nicaragua case, which was upheld by the ICJ.

3.2. The Possibility of Applying the Exercise of the Right to Cyber Attacks: The Significance of Self-Defense by Force

3.2.1. Efficient Exercise of Force in Self-defense

Compared to the lagging nature of nonviolent means of sanctioning, forceful self-defense is efficient in terms of means, which is undoubtedly most conducive to the maintenance of national security. First, forceful countermeasures can directly target the source of an attack, thereby quickly neutralizing the threat, especially if the attack poses an immediate danger to national security and the lives of citizens. Second, the strong deterrent effect demonstrated by force may be effective in deterring future cyber attacks, and even the latent military and force threats behind them, by conveying a zero-tolerance attitude towards violations, while at the same time being fundamental to the disruption of plans to steal information and thus deploy covertly with superior strategies by means of cyber attacks.

3.2.2. Normativity of the Exercise of Force in Self-defence

The international community's regulation of the exercise of force as a right is more systematic and mature ("jus ad bellum" and "jus in bello"), and it is more convenient for the lawful exercise of the right in a flawless situation. The conditions, circumstances, rights and obligations of the exercise of force in self-defense have already been described in detail in Part I of this article and will not be repeated here.

3.3. Jurisprudence of the Exercise of the Right as Applied to Cyber Attacks: Basis for the Legitimacy of Self-Defense by Force

The jurisprudential controversy over the exercise of the right against cyber attacks has two points: first, whether cyber attacks can be regarded as attacks with the use of force, and second, whether cyber means can be regarded as weapons. If the answers to these two controversial questions are positive, there is no doubt that cyber-attacks can be included in the conditions for the exercise of the

DOI: 10.54254/2753-7064/37/20240122

right. The answer to the first question should be based on the practice and understanding of the Charter Art 2(4) and Art 51, and should refer to the specific nature, subjective intent, and objective results of the act of cyber attack.

3.3.1. Prohibitions and Limitations

When the Substantial Constituent of an Act of Cyber Warfare Breaks Through the Charter Art 2(4) Prohibition into Limited Self-Defense under Section 51.

Article 2(4) of the United Nations Charter prohibits the use of force as a means of settling disputes, but when a State is subjected to armed aggression, Art 51 of the Charter, as an exemption from that Article, provides for the exercise of armed self-defense as a right of the aggrieved State to make restitution and cease the injury. This would support the view of one international law scholar that Art 51 of the Charter is itself an empowering rather than a prohibitive provision, and that it is only in the granting of a new right that limitations should be placed on it - i.e., how wide the pockets of the right can be triggered.

The greatest controversy here is that the inclusion of cyber attacks in the conditions for the use of force in self-defense undoubtedly expands this pocket and increases the use of force, thus fundamentally violating the purpose of the Charter of the United Nations, which prohibits the use of force for the maintenance of peace.

The problem with this view is that it simply emphasizes that the injured party's forceful response is a condition for expanding the scope of the use of force while ignoring the important fact that the rapidly growing destructive power of cyber-aggression is no less destructive than, or even qualitatively equivalent to, traditional forceful acts of war, as seen here in the Tallinn Manual. “the consequences of a cyber operation can be compared with those of the use of force, including actions such as causing injury, killing people, or destroying objects. When the scale and impact of a cyber operation are essentially equivalent to those of a non-cyber operation constituting the use of force, it can be determined as an act of using force.” In the first part, it can be concluded that the definition of an armed attack, while inextricably linked to its substantial and serious consequences, does not require necessarily large-scale military action - the nature of the act and the subjective intent are what defines the act itself, and to this extent, the shooting down of a single civilian aircraft in the airspace of another country with a missile, while not involving large-scale force, does not result in a large-scale military action, nor does it result in a large-scale military action. To the same extent, the act of shooting down a single civilian aircraft in the airspace of another country with a missile, although it does not involve large-scale force and does not result in a large number of casualties, can be regarded as an attack by force (the above has already been discussed, and will not be repeated). Similarly, a Trojan Horse implanted in a country's private civilian aircraft to bring down an important scientific and technological talent to complete the assassination of the act, a virus implanted to modify the water filter in a certain area, or a virus implanted to modify the water filter in a certain area. Similarly, the act of assassination of a person at the forefront of science and technology in a country by crashing a private civilian airplane using a Trojan horse virus implant, or the act of poisoning civilians by modifying the chemical composition of the water filters in a certain area through virus implantation, has obviously reached the level of serious harm that can be accomplished by conventional force, such as a missile attack or the bombing of hydroelectric plants.

Since the implementation of the right to self-defence depends mainly on whether it has been subjected to an "armed attack", when it is judged not to have been subjected to an armed attack, it can only resort to retaliation or countermeasures, as in the case of the Sino-Indian border conflict in recent years; however, when it reaches the level of "having received an armed attack", the medium and manner of its implementation should not be a reason to impede the implementation of the right to

DOI: 10.54254/2753-7064/37/20240122

self-defence. However, when it reaches the level of "receiving an armed attack", the medium and manner thereof should not be a reason to impede the implementation of the right to self-defense.

In September 2012, Professor Harold Koh, then Legal Adviser to the United States Department of State, submitted a paper to the United Nations on the position of the United States that a cyber attack may be considered to meet the criteria for "use of force" under the Charter and customary international law when the attack could result in death, injury, or substantial damage, especially a cyber attack that could result in significant physical harm such as the dropping of a bomb or the launching of a missile, or the launching of a missile, and that a cyber attack could cause significant physical harm [8]. Cyber-attacks that cause significant physical harm, such as the dropping of bombs or the launching of missiles. The views of existing scholars and States that support this doctrine can be summarized as "consequentialist", i.e., by looking at cyber attacks as being sufficiently consequential to achieve the equivalent of traditional force, and thus defining what constitutes a "use of force", and thus self-defensive counterattacks naturally do not constitute a "breach of the peace, use of force". The imbalance of "breaking the peace and using force" does not expand the pocket of "use of force" in terms of jurisprudence, but rather, it is the act of cyber-attack that has essentially constituted all the elements of traditional force in war, except for the medium of weapons.

In addition to consequentialism, Professor Schmidt, a professor of international law at the U.S. Naval War College, summarized the six characteristics of a traditional force attack - severity, urgency, immediacy, intrusiveness, measurability, and expected legitimacy [9] - that fundamentally distinguishes it from less physically damaging means of hostility, such as political incitement and economic sanctions, and therefore, to measure Therefore, by measuring which means a cyber attack is closer to, and whether it is more or less consistent with these six characteristics, it is possible to clearly define whether or not it essentially falls into the category of a forceful attack or, in other words, constitutes an equivalent substantive element of a forceful attack.

3.3.2. Expansive Interpretation of the Definition of Weapons - Networks Can Be Weapons Too

The traditional view is that cyber-attacks usually do not use the traditional physical form of weapons, they are mainly through computer language and specific code to carry out the attack instead of fighter jets, missiles and warships; and the harm they bring is often secondary and derivative through the modification and tampering in cyberspace, which leads to the difference between him and the weapon directly kills a person, and cyber-attacks seem to have a temporal-spatial gap in the middle between the behavior of the cyber-attacks and the results of harms rift.

There are different views and discussions among authoritative academics and international organizations on whether cyber means can be defined as weapons.

In its report on international humanitarian law and cyber operations in armed conflict, the International Committee of the Red Cross noted that cyber operations are subject to international humanitarian law during armed conflict in the same way as other weapons, means or methods of warfare, whether new or old. This suggests that, although there is no general consensus at present, there is sufficient reason to believe that international humanitarian law can be applied in cyberspace, particularly as it relates to the general principles and rules for the protection of civilians and civilian objects. The Commission is of the view that actions against computers or computer systems aimed at paralyzing them constitute an attack as defined by IHL, regardless of whether the paralysis is caused by physical destruction or by any other means [10].

In addition, Wu Shenguo, the United Nations Senior Adviser on Cybersecurity and Cybercrime, pointed out in his discussion on cybersecurity that there is a trend towards politicization of the current cybersecurity issue, and that there has been a surge in the discussion of issues involving the militarization of cyberspace. This suggests that it has become a recognized fact that cyber technology is being used in a weapons role to carry out attacks for military purposes. For example, the

DOI: 10.54254/2753-7064/37/20240122

development of automated lethal weapons and artificially intelligent weapons systems, as well as attacks against the critical information infrastructure of specific countries, are all manifestations of the weaponization of cybertechnology [11].

Although there is no clear written consensus in international law and the international community as to whether cyber means can be defined as weapons, there are academic discussions and resolutions of authoritative international organizations that suggest that cyber means are considered to have potential similar to that of traditional weapons under certain circumstances and can be subject to similar international law. The traditional view that cybermeans are not legally appropriate as weapons according to the definition of sources of international law in article 38 of the Statute of the ICJ has been resolved thanks to the silence given by jus cogens, treaties and customary international law, and the positive response from the academic community.

3.4. The Practicality of Cyber Attacks in Applying the Exercise of the Right and Attempts at International Law Legislation - The Reference Value of the Tallinn Manual as an Example.

The NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, invited 20 international law experts with reputations in the field of law of war studies in cyberspace to write the Tallinn Manual over a period of three years, with the assistance of the International Red Cross. Although there are certain differences between NATO's ideology and our country's strategic positioning, this Tallinn Manual, as a scholarly rulebook of international law, is not current international jus cogens and its scholarly and practical value is worth discussing: whether it can be used as a source of international law and be binding on some countries to use it as a legal basis in practice, especially because it supplements the current gaps in international law, it is clear that in this case, the Tallinn Manual is not a source of international law, but a source of international law [12]. It is clear that its application would be justified in this context.

The Tallinn Manual mentions that "an act of a state constitutes a use of force if it causes damage to or interferes with the use of another state's electronic infrastructure, and if this act is carried out by or under the direction of that state." This definition emphasizes that in cyberspace, which is not limited to traditional armed conflict, the conduct of any State that causes damage to or interferes with the use of another State's electronic infrastructure can be considered a use of force.

In contrast to the traditional definition of "armed attack" under international law, which usually involves direct and destructive armed conflict, the Tallinn Manual's definition of force expands the concept to encompass more complex and insidious attacks in cyberspace, such as cyber penetration attacks. The Tallinn Manual gives a broader definition of force, according to Article 11 of the manual "An act of a state constitutes a use of force if it causes damage to the electronic infrastructure of another state or interferes with another state's use of its electronic infrastructure, and if the act is carried out by or under the direction of that state.", thus giving a new interpretation of the applicability of cyber attacks. At the same time, it emphasizes the principle of proportionality in accordance with the right of self-defence in the event of an attack by traditional force and proposes the principle of seeking peaceful solutions to the extent possible in light of the characteristics of cyber-attacks.

In addition, the manual also gives detailed legislative attempts in specific rule-making, respectively from the "right of resort to armed force" and "laws of war" - two important aspects of international law on the regulation of war. In addition, the manual also gives detailed legislative attempts to formulate specific rules, respectively from the "right to resort to armed force" and "laws of war", which are two important aspects of international law on the regulation of war, and its full text of articles 10-95 all encompasses these two major segments, namely, articles 10-19 on the regulation of the right of recourse to armed force, and articles 20-95 on the regulation of laws of war, and legislative attempts are made in the conduct of hostilities; means and methods of warfare;

DOI: 10.54254/2753-7064/37/20240122

protection of specific persons, objectives and activities; occupation; neutrality and other indispensable aspects of the laws of war.

The publication of the Tallinn Manual, especially its second edition with the inclusion of non-Western scholars such as Chinese, Thai and Belarusian scholars in the codification team, is not only more persuasive from the perspective of discourse representation but also fills the gap in the international community on the legal system of cyberspace conflict and objectively provides practical reference for the international community in discussing and formulating a way to deal with the issue of cyberspace conflict and the use of force.

4. Construction of the Right to Self-defense Against Cyber Attacks

4.1. Normative Transplantation and Innovation of Established Constructs

As in the case of the traditional right, the exercise of the right in the face of cyber-attacks should, first of all, satisfy all the elements and rules of the traditional right, i.e., the rules and principles of the Tallinn Manual, such as the "rules of war", and, at the same time, due to the special characteristics of cyber attacks, the exercise of the right against cyber-attacks should be At the same time, due to the special characteristics of cyber attacks, the exercise of the right against cyber-attacks should be more deeply integrated with the full cooperation of the international community, as detailed below.

4.1.1. Principle of Military Necessity

Under the laws of war, the principle of military necessity means that, of all the means capable of achieving the objective, the one that causes the least harm must be chosen. In other words, the least intrusive means should be chosen without violating or diminishing the objective pursued, i.e., in accordance with the "principle of least infringement". This suggests that force should only be used when it has become a "last resort". Recourse to physical force should be made on the condition that the act of force used is in accordance with the law of armed conflict and that it ensures that the enemy is repulsed with the least sacrifice, time and resources to the maximum extent possible (i.e., with the minimum of effort) [13].

The Tallinn Manual 2.0 also notes that, under the Charter of the United Nations, States are obliged to seek the peaceful settlement of disputes, and that, in principle, peaceful means should be used whenever possible before resorting to the use of force. Therefore, when responding to cyber attacks, States should consider whether other means of unarmed dispute resolution exist.

Within the constraints of this principle, it would seem that the use of cyber means as a means of counterattack is the best way to go, since computer viruses, like attackers, cause minimal physical damage to the counterattacker as the party using them. It should be noted, however, that this approach would be somewhat of a dilemma in practice:

First, when countering with the same technical and physical means: cyber intrusions tend to be overwhelming, so often the country being technologically invaded does not have advanced cyber counter-hacking tools to match damage repair and technical counter-attacks. Comparative studies by international scholars have shown that the asymmetric nature of cyber warfare means that attackers are often able to use more advanced techniques that victims may not be able to respond to immediately. This asymmetry exacerbates the impact of cyber-based intrusions and makes it more difficult for victimized states to technically counter and repair them [14]. This is the classic victim paradox, where countering a "technologically superior" intruder with the same technical means is in most cases an objectively unattainable requirement, a de facto impossibility.

The second paradox lies in the question of proportionality in the use of cybertechnology to counterattack. The principle of proportionality [15] should be observed, even in the case of cybercountermeasures, for reasons of legality. However, to date, there has not been a single case in

DOI: 10.54254/2753-7064/37/20240122

international law in which information technology has been used as a means of self-defense, nor is there any existing jus cogens to regulate this, and the proliferation of information technology attacks is more difficult to predict and anticipate than the results of a traditional force attack. In this case, defining the proportion of legitimate cyber countermeasures is quite difficult and requires long-term international consensus, legislation and court practice. If it is not done under a legitimate proportionality regime, the right to self-defense becomes flawed, illegitimate, and more difficult to evaluate.

An analogy is drawn here with the domestic law of a particular country. For example, U.S. law allows companies to deploy anti-malware measures on their own networks, but at the same time criminalizes computer attacks on others (including counter-attacks). The ICJ (ICJ) upholds cyber attack responses that follow specific lawful countermeasure elements, adding to the complexity of the decision-making process. It is worth noting that the ICJ has only upheld lawful countermeasures, not counterattacks, and that normal self-defense force clearly reaches the limits of "counterattack". In other words, the current international community's upper limit for cybercountermeasures is set at damage restoration, but there is no supportive jurisprudence on the legality of using cyber as a means of attack.

4.1.2. The Principle of Proportionality

Just as traditional self-defense force countermeasures should be guided by the principle of proportionality, i.e., the force unleashed to stop the aggression of an intruder should not be more than necessary to protect the national legal interests of the State than it needs to be.

Determining a reasonable self-defense force ratio requires a thorough assessment of the substantial threat of a cyber-based attack. Different types of cyber-attacks may have different impacts and levels of harm and therefore require targeted action, in which robust measures are taken against attacks that pose a real threat while avoiding overreaction. In addition, the use of force should be governed by international humanitarian law with regard to the preferential treatment of prisoners of war, the protection of combatants withdrawing from combat and the protection of civilians.

4.1.3. Duty to Inform and Burden of Proof

The invaded State (the State using force in self-defence) should fulfil the duty of notification, i.e., inform the UNSC of the action taken in self-defence and bear the burden of proving that the cyber-attacks suffered by it came from a member of a certain State/consortium or organization, that the counter-attacks were directed against the State that initiated the cyber-attacks, and that the gravity of the damages was directly proportional to the gravity of the use of force. This is because the use of the right of self-defence needs to meet objective criteria and should not be based on subjective judgment alone, but should be able to withstand the review of legality by the ICJ in order to determine that the right of self-defence is flawless, and this applies, in particular, to "preventive self-defence". However, due to the various characteristics of cyber-attacks of anonymity, the attacked country in practice to trace the evidence may be in trouble, so the a need to establish a supportive international cooperation to ensure the realization of the right. Therefore, in the author's view, there is a need to build a new structure, a new security-based cooperation of the international community.

4.1.4. New Structure

Although the international community's to reach a resolution to take countermeasures is evaluated as inefficient, the construction of international/regional cyber defense and security cooperation has the feasibility and rationality of the first, the attacked country to fulfill the obligation to notify the UNSC and the regional cooperation organization to submit evidence, and through the unilateral force is more

DOI: 10.54254/2753-7064/37/20240122

powerful and accurate defense tracking force to identify the attacker can also help the victim to correctly exercise the right to the subject of the infringement. The right. At this point, the aggressor's right to self-defense is intact and the appropriate proportion of force can be exercised. A structure like the one shown in Figure 1.

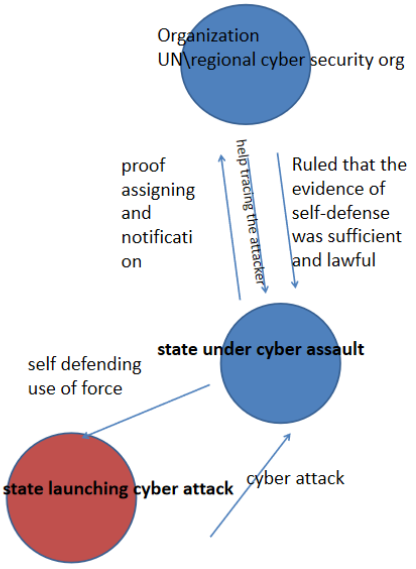

Figure 1: Structure of " attack-detect-counterattack " under international cooperation

That the sources of cyber attacks are often difficult to trace, that the technology of those being attacked is often backward, and that authoritative international organizations or regional cooperation organizations, as well as major powers such as the five permanent members of the UNSC, can assume the responsibility for maintaining regional stability and peacekeeping, promoting and constructing cybersecurity and defence networks, and, in fact, aborting the plans of the attackers even before they need to counterattack in self-defence, thus complying with the requisite principles of the law of armed conflict. deter further bloodshed. As mentioned in the introduction to this paper, Qatar eventually realized the truth of the UAE's cyber attack and its subsequent military intentions with the assistance of a friendly strategic partner and obtained support for additional border deployments in time to neutralize the potential military conflict and threat. Some cybersecurity scholars have hypothesized that successful "detection-measures" systems such as this one would require a greater responsibility on the part of countries like China and the United States, which possess powerful integrated forces. And it is foreseeable that in future cyber wars, with the major powers assuming their responsibilities, the construction of a security cooperation network to accurately track attackers will make it easier for victims to exercise their due rights and maintain regional and world peace.

4.2. New Issues and Controversies - National Security and Abuse of Power

In this paper, the author argues for the possibility of incorporating cyber attacks into the triggering conditions for the exercise of the right to self-defense in the form of an armed attack, which will inevitably lead to a heated discussion centered around nothing more than the topic of national security and the abuse of the right to resort to the use of force in the name of self-defense. This is also the inevitability of the common cooperation structure proposed above, human security is a common problem, and ultimately faced with the full cooperation of all mankind must be required to maximize the international rule of law society in the current supervision of large countries to fulfill their responsibilities, to protect the legitimate interests of weak countries, and to eliminate and constrain

DOI: 10.54254/2753-7064/37/20240122

the abuse of rights by any party. As a responsible big country that is increasingly active on the international stage, China will certainly play a leading role in this cooperative construction. Cyberspace is a common resource of mankind, and all countries in the world determine the development trend of cyberspace, which also affects the economic and political safety and security of all countries in the world. Therefore, all countries should build a community of destiny in cyberspace by adhering to the idea of "win-win" cooperation.

5. Conclusion

In this thesis, the author, by raising the issue of including cyber attacks in the conditions for the exercise of the right, which is a topic that has been left blank in international law, firstly analyzes the formal mode of the traditional right from a practical point of view to pave the way for the exercise of the right against cyber attacks; then argues for the feasibility of the issue from the perspectives of necessity, possibility and legality of the legal force; and analyzes the practical relevance and international law reference value of the Tallinn Manual, which is a masterpiece of the existing regulation of the cyber domain --It also analyzes the practical significance and international law reference value of the existing masterpiece of armed regulation in the cyber field, and finally rigorously provides a right structure for the exercise of the right against cyber attacks in accordance with the regulation of the laws of war, and on the basis of which it proposes an approach based on a regional/international cooperative organization, the attacked state, and the state that commits the act, and on the basis of the concept of "attack-detect-counter-attack". On this basis, it proposes a structure based on the principle of the use of force strictly regulated by the laws of war, with regional/international cooperation organizations, the attacked State, and the State committing the act, and with the mode of action of "attack-detect-counterattack".

References

[1] *Charter of the United Nations, Articles 2.*

[2] *ICJ. (1986). Case Concerning Military and Paramilitary Activities in and Against Nicaragua. Judgment. ICJ Reports. (Note: Seethe Nicaragua Case, Para. 194.)*

[3] *North Atlantic Treaty Organization (article 6)*

[4] *Simma, B., & Paulus, A. (2012). The Charter of the United Nations: A Commentary. Oxford University Press, Oxford.*

[5] *Franck, T. M. (2002). Recourse to Force: State Action Against Threats and Armed Attacks. Cambridge University Press, Cambridge.*

[6] *Smith, J. (2018). Cyber attacks and the use of force: Back to the future of Article 2(4). Yale Journal of International Law, 43(1): 19-46*

[7] *Johnson, M. (2017). Global governance of cyberspace: The search for a new equilibrium. Global Policy, 8(S4): 40-45.*

[8] *Shackelford, and Scott J., Managing Cyber Attacks in International Law, Business(Cambridge University Press, Cambridge, 2014), pp. 285-306.*

[9] *Schmitt, M. (2010).Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. National Academy Press, Washington, D.C.*

[10] *Twenty Years in Retrospect: International Humanitarian Law and the Protection of Civilians from Cyber Operations in Armed Conflict Laurent Giselle, Tilman Rodenhauser, Knut Dorman IRRC No. 913 March https://international-review.icrc.org/zh-hans/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913*

[11] *"Finding the Largest Common Denominator for International Governance of Cyberspace - Interview with Wu Shenguo, UN Senior Advisor on Cybersecurity and Cybercrime" December 2019 UN News https://news.un.org/zh/story/2019/12/1047311*

[12] *Statute of the ICJ, article 38*

[13] *Maritime Operations Act Manual of the United States Navy*

[14] *Libicki,C.(2009). Cyber Deterrence and Cyberwar, RAND Corporation, Santa Monica*

[15] *Additional Protocol I, article 51, para. 5 (b); article 57*