DE JURE NEXUS LAW JOURNAL

Author:
A. Raj Singh
JEMTEC School of Law
1st Year, BA LL.B.

RIGHT TO SELF DEFENCE AND CYBER WARFARE

ABSTRACT

Modern cyberwarfare represents a new type of weapon that can change the world battlefield. The various properties of these types of weapons and the ability to create large, widespread weapons Damage to national critical infrastructure to conquer and transform traditional means of violence This is the international community On the other hand, the existing paradigm of law for war and its legal regulation cyber warfare Victims' inherent rights in self-defense must be upheld and explained in detail Cyber attacks, rules on how to assign responsibility to governments taking action These governments must be taken to prevent them from escaping the consequences of their illegal activities. actually In this article, we will use analytical techniques to investigate whether cyber attacks can be viewed as such. Armed attacks provoke the right of self-defense in the victim country.

Keywords: use of force, cyber warfare, armed attack, self-defense, attribution.

Introduction

The principles of non-use of force as one of the most important principles of the *Charter of the United Nations* are: *Article 2, paragraph 4* this article deals only with military power and proposed prohibitions .This includes not only its use, but also the threat of its use. The ban on the use of force is accompanied by some exceptions made by customary international law, followed by the Charter of the United Nations and procedures. In addition to the *Security Council Chapter 7 Resolution*. Self-defense is the second exception and acts under the

principle of non-use of force set out in *Article 51*. The Charter of the United Nations is the result of more than 60 years of discourse on rights. So what does that suggest? *Paragraph 4 of Article 2 of the Charter* as a ban on the use of military force is: A classic and famous weapon. But today, the war has been stripped of its traditional concepts, including weapons, explosives, and technological advances have provided the government with new tools. The most important of these is the use of cyberspace to launch cyberattacks against government targets. Actually today, as military experts have done, cyberspace is becoming a new field for tracking military operations. Indeed, cyberspace is becoming a new war zone. This is while the great powers are arming themselves. Deploy their troops to cyber warfare more quickly and extensively and actively benefit their enemies and competitors.

In general, cyber-attacks have many destructive powers. For example, Cyber attacks can damage government facilities and private infrastructure such as power grids and railroads. Gas pipelines, airways, transportation infrastructure, and capital industry, among other things, are putting the nation's lives at jeopardy. Furthermore, the frequency of cyber attacks has risen in recent years, and many countries are focusing their efforts on them. Cyber attack, In contrast, some governments, such as the United States, were the main suspects in the attack. It was the target of several alleged cyber attacks by China. In April 2007, an incident in which Estonia was the target of a cyberattack attacked Estonia for three weeks. As a result, official government websites, TV stations, banks, etc. will not work. Cyber attacks in other countries such as the United Kingdom, Taiwan, South Korea, Kazakhstan, and Switzerland have also appeared. When our country, Iran, was also the target of a 2010 US cyberattack aimed at disrupting nuclear programs. Stuxnet virus. Today, due to the importance of the subject, U's secret service. S. Officially, it is claimed that about 20-30 countries form special forces for cyberwarfare and NATOPUT. Cyber warfare as a new priority on that agenda. According to the importance of the above issues, the subject of this issue, raised in the field debate on the right to war (violence), is whether these new measures are intentional. Also including the use of cyberspace to carry out cyber attacks, Article 2 (4) of the Charter provides rights to the government of victims of armed attacks. Legal self-defense subject to Article 51? On the one hand, you need to be careful in this regard. In addition, Article 51 is a requirement only if the victim government has the right to self-defense. We have discovered that the use of force is approaching the limits of “armed attack". Therefore, identifying the cyber attack as one armed attack is a legal issue and needs to be investigated and

investigated. On the other hand, in the case of such an attack, this important topic, which is the name of armed attack, finds projection skills such as attacks Assigned to suspects according to complex technical characteristics of attack. The purpose of this article is to present an analysis of cyberattack issues in a predicted dimension.

CYBER ATTACK AS A USE FORCE IN INTERNATIONAL LAW

Any purpose or motivation to provoke a government to run a cyberwarfare, and regardless of its normative assessment by the international community, the important subject is answer to the question of whether such cyberattacks, either invasive or defensive are considered as the illegal threat or use of force? And thus if it violates the rules of international law in this field?[1] To define cyberwarfare, the international community must somehow reach consensus on the meaning of these activities under the Charter, particularly *Article 2, paragraph 4*, which regulates the use of force set and *Article 51* that provides the right to self defense.[2]

Article 2 paragraph 4 of the Charter, which governs the use of force set and *Article 51* that guarantees the right to self defence. Article 2 paragraph 4 of the Charter explains the original statement on the use of force in international law. "All members must abstain from the threat or use of force against the territorial sovereignty or regional autonomy of any state or in any way detrimental to the Charter's goals in their international dealings," according to this rule.[3] With this structure in place, the question becomes: what constitutes the use of power? The Charter clearly has announced that the offensive force is illegal, while the inherent right of a state to self defense as individual and/or popular is identified in the *article 51*.[4]Thus, if the action of a government is considered as the use of force, according to the concept which is stated in *Article 2, paragraph 4*, of the Charter, it is illegal unless it is in order to implement the right of a country within the framework of *article 51* of the Charter for self defense. While the precise definition of what is the use of force, is not clear, some factors are well established.[5] For example, attacks by conventional weapons are in the context of *paragraph 4 of Article 2 of the Charter*.[6] Moreover, cyberattacks, which are used for the purpose of directly damaging physical property or causing human damage or death, are reasonably classified as the use of force and are therefore subject to this ban. In contrast, the

[1] MN Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999).
Columbia Journal of Transnational Law, Vol. 37, 1998-99.p.900, Available at SSRN: http://ssrn.com/abstract=1603800.

[2] DM Greekman, a Helpless America? An Examination of the Legal Options available to the United States in Response to Various cyber-Attacks from China, 17 AM. U. INT'L L, REV.641, 2002, p. 679.

[3] Article 2, paragraph 4, of the Charter of the United Nations.

[4] Article 51 of the Charter of the United Nations.

[5] J Barkham, Information Warfare and International Law on the Use of Force, Fall, 2001, 34 N.Y.U. J. Int'l L. & Pol. 57, p.70

Development of Government Efforts to Include Economic Pressure Related to *Paragraph 4 of the Article 2 of the Charter* at the time the Charter was enacted, these are clearly excluded from being included in the concept. Therefore, the analysis is in the context of the Charter of Article 2 (4).

Accepting this part of the Charter requires an interpretation that eliminates economic and political pressure. Inclusion of this article. The possibility of implementing *Article 2 (4)* of the Charter in cyberwarfare poses serious problems.

The question of interpreting the difference between violence and coercion. Including all acts related to cyberwarfare as the use of force requires a broad interpretation of Article 2 (4) charter. With such a broad definition of violence, political and economic constraints and forces disqualify themselves.

It is difficult to get out of this cycle of concepts. Because international law needs to distinguish between cyber attacks that cause physical injury, such as, electronic attacks and blocking political and economic pressures that cause physical harm. Anything that does not cause physical harm or has no such effect indirectly violates the prohibition of the use of force .[7]

To solve the deadlock in this category, Michael Schmidt is in politics Economic pressure and power based on six criteria:

1) Strength 2) Urgency 3) Causal relationship 4) Violation 5) Quantification 6) Obtained legitimacy .[8]

These criteria are intended to evaluate actions in cyber warfare in comparison to other actions. Determine if the outcome of these actions is closer to the effect of an armed attack, or if the action is similar to the effect of an armed attack. Must be removed from the area of armed attack. Implementation of Schmidt technology leads to this result. The predictable and logical outcome of the action determines whether an armed attack is involved. If the result is similar to the effect of an armed attack, the development of the concept of violence should be adapted accordingly. The measures are reasonable, otherwise there are acts that violate

[7] Ibid.p.913.
[8] Ibid.p.915

international law. Appealed to the provisions of international law other than the prohibition of the use of force [9].

THE CAROLINE DOCTRINE

The Caroline doctrine, identified as common law, provides a framework for governing the right to self-defense. The doctrine includes the principles of necessity, proportionality, and immediacy. The principle of necessity is primarily essential and aims to use force to thwart or avoid armed attacks when other alternative remedies are exhausted. The principle of proportionality determines the balanced response of the defensive state to the attack state.

The damage caused by the defensive state in self-defense must be proportional to the damage caused by the attack state. Finally, the principle of immediacy means that the victim's nation can only protect itself in the event of an imminent or ongoing attack. When this doctrine is applied to cyber warfare, the victim's condition is detected and advanced because the design and timing are set so that the attacker does damage only a few months after invading the attacker. It will be very difficult to counter the attacks in line. Therefore, the need and immediacy are unacceptable in cyber conflicts. As far as proportionality is concerned, the impact of cyber attacks is immeasurable given the huge interconnectivity of information networks. Unbalanced collateral damage and the "reverberation effect" involve everyone indiscriminately. In fact, due to the obvious and eccentric nature of cyberspace, Caroline doctrine is loosely inappropriate when it comes to cyberwarfare. In addition, *Article 51-2* provides for predictive self-defense in war, suggesting that the victim may attack another state that is allegedly planning an attack. The tricky problem is the application of predictive self-defense standards to cyber operations. Therefore, since cyber-attacks are virtual attacks, it is difficult to predict the intuition in advance of the attack. So, what is the indication that the victim's state is hacking the computer system of another's state? The end result is preemptive self-defense, not preemptive, that violates international law. Therefore, Caroline's doctrine and *Article 51* are outdated, incompatible with new cyberwarfare, and can the victim's nation attack in self-defense and legally break into someone else's computer to prevent cyberattacks.

[9] VM Antolin-Jenkins, Defining the Parameters of Cyber war Operations :Looking for Law in the Wrong Places?51Naval L.Rev.132, 2005,p.170.

CONCLUSION

Finally, the above analysis shows that the existing international legal framework is redundant and inadequate. Self-defense in cyber warfare seems to have astounding consequences due to the anonymous and improper behavior of cyberspace. However, the international group NATO Cooperative Cyber Defense Center of Excellence has created the Tallinn Handbook, a non-binding international work applicable to cyber conflicts. The Tallinn Handbook is a great development that scrutinizes the lex lata gap and skillfully provides lex ferenda for cyber policy. Recently updated to version 2.0. Rules 71-75 of the Tallinn Manual 2.0 deal with self-defense in cyber conflicts and also cover the above principles. It's just a blueprint for passing an international treaty. It can also be used to renew the Council of Europe Treaty on Cybercrime in 2001. This means trivial cybercrime such as child pornography and fraud, so it is not effective in handling large-scale cyberwarfare activities. Cyber warfare has emerged as a new global threat. Therefore, a robust international framework based on global consensus could only mitigate the threat of cyberspace and determine national rights and responsibilities.