Proceedings of the 2nd International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2024.24353

How is Cyber-attack Changing Warfare

Xiaolu Yang

Department of International Studies, Takushoku University, Tokyo, Japan
web_pub@ofc.takushoku-u.ac.jp

Abstract. This paper looks at how cyber warfare is changing the nature of war. It also discusses the problems with the current international legal system when dealing with cyber-attacks. The study focuses on how hard it is to define a cyber-attack clearly. It also explains the difficulties of using old international laws for these new conflicts. The paper shows the weaknesses in current laws by looking at examples like the Stuxnet virus and the Estonia power grid attack. These laws have trouble dealing with cyber warfare that governments support. The paper highlights the need to update international humanitarian law. This update would help protect civilians from the harm caused by cyber operations. The paper also says that we need clearer definitions. It suggests creating a new "Cyber Warfare Treaty" regulating cyber warfare. This treaty would be similar to the rules for traditional armed conflicts. It would make sure that civilians' property is protected. It would also ensure that states are held responsible for their actions in cyberspace.

Keywords: cyber-attack warfare, international legal system, humanitarian law

1. Introduction

With the fast growth of technology, cyber warfare has slowly become a big issue in international security. Cyber warfare, powered by digital technology and the internet, has moved from being talked about to happening. It is now a new kind of conflict between countries. However, the current international legal system seems outdated when dealing with this new threat. It does not cover the complicated issues of cyber warfare well. Because of this legal gap, some countries have started using cyber-attacks to violate the sovereignty of other nations. This is a challenge to traditional warfare and the power of international law.

Article 2(4) of the United Nations Charter clearly states that countries cannot use force against the land or political independence of other nations. However, as cyber-attack methods keep changing, the current laws do not give clear rules about what exactly counts as a cyber-attack. This legal gap has resulted in the international community being insufficient in imposing effective restrictions and regulations on activities in cyberspace, making cyber warfare a risk that is difficult to control.

Therefore, how does cyber warfare change the nature of warfare, and what are the shortcomings of the current international legal system in dealing with cyber-attacks? Can we limit cyber warfare and its impact on civilians by supplementing international law? This paper will focus on the impact of cyber warfare on modes of warfare, especially how to redefine and update the legal framework to

DOI: 10.54254/2753-7048/2024.24353

explain it. The author believes that although the United Nations Charter prohibits traditional forms of the use of force, the current laws do not clearly define what constitutes a cyber-attack. This legal gap presents significant challenges for the international community in limiting and regulating cyber activities. Therefore, this paper will review the literature on cyber warfare discussed by several scholars and conduct case studies on the Stuxnet virus incident and the Estonia power grid attack to further reveal the main shortcomings of the current legal system in dealing with cyber warfare and explore the necessity of establishing international humanitarian law to protect civilians under cyber warfare.

2. Literature review

In this respect, Buchan Russell and Nicholas Tsagourias have studied how cyber warfare fits within international law [1]. More importantly, the limits of current international legal rules for controlling cyber warfare activities. According to them, the current legal system has been scant in dealing with cyber warfare, particularly concerning determining whether cyber-attacks are lawful and who maintains responsibility for the attack. Moynihan Harriet [2] also talked about applying international law in cyber-attacks. She focused on the principles of sovereignty and non-interference. She said that though there is a consensus between many states that international law does apply to cyberspace, there is still considerable confusion and disagreement over what precisely those rules should look like in practice.

In this connection, although some scholars have considered the place of cyber war within conflicts today and how IHL should approach these new challenges, Gisel Laurent, Tilman Rodenhäuser, and Knut Dörmann concluded in 2020 that "although IHL may sometimes apply to cyber operations, the legal norms need to be clarified and consolidated, in particular about the protection of civilians against cyber-attacks.". They further reiterated that with the advancement of cyber technology, civilians are increasingly becoming victims of cyber-attacks, and the existing laws cannot solve the problem. In a related development, an article in the *International Review of the Red Cross* indicated that IHL has left some loopholes in considering the unique nature of cyber operations [3,4]. The article has also mentioned that while IHL can be applied to some situations in cyber warfare, significant legal and practical uncertainties remain as to how cyber operations pertain to combat actions and how they affect civilians and civilian infrastructure.

Pendino Stephanie et al. [5] researched ways the United States might achieve a more effective cyber deterrence strategy. The authors recommended using Offensive Cyber Operations (OCO) to fight unrelenting cyber threats.

They said that traditional defensive strategies are not enough to deal with ongoing threats from major enemies. Therefore, they suggested that the U.S. should adopt a more offensive strategy. This approach could act not only as a deterrent but also help set rules of behavior in international cyberspace. In totality, these works indicate that as cyberwar becomes increasingly significant in modern conflict, neither current international law nor international humanitarian law deals with all the new challenges posed by cyberwar. The scholars agree that the international community needs to review and expand the legal rules to better protect civilians and regulate cyber warfare in future conflicts.

These studies indicated the need for more specific and developed legal rules, pointing out the increasing need for international cooperation in establishing new agreements or adapting current laws to face complex problems created by cyber warfare.

DOI: 10.54254/2753-7048/2024.24353

3. Case studies

This study uses case studies to examine cyber warfare's challenges to the current international legal system. It also looks at the weaknesses in the existing legal framework when dealing with cyber-attacks. By studying two famous cases of cyber warfare, the Stuxnet virus incident and the Estonia power grid attack, this research tries to show the legal uncertainties about cyber warfare and its impact on international security.

The two main cases used in this study are the Stuxnet virus incident and the Estonia power grid attack. These cases show different types of cyber warfare and have led to many discussions in international law. This study collected information on these two events from academic papers, legal documents, government reports, and expert analyses. However, this study has some limits, such as relying only on case studies, which may not fully represent all types of cyber-attacks. Moreover, due to the secretive and complex nature of cyber warfare, many state-sponsored cyber-attacks may not have been disclosed, leading to data collection limitations. Additionally, the rapid development of international law in this field means that the conclusions of this study may change as new laws and international standards are introduced.

3.1. Stuxnet virus

The Stuxnet virus was first discovered in 2010. It was specifically designed to disrupt Iran's nuclear facilities. It is believed to be a state-sponsored cyber weapon, probably developed by Israel and the United States together. Stuxnet infected the control systems of targeted devices, causing centrifuges to malfunction and thus disrupting Iran's nuclear program [6].

The Stuxnet incident led to widespread discussions about the legality of cyber-attacks. According to existing international law, especially the United Nations Charter and the Geneva Conventions, armed attacks are generally understood to involve physical force. However, Stuxnet’s attack method was mainly through software code, which, although it eventually caused physical damage, was not widely recognized as an "armed attack" because of the lack of a clear legal framework. Also, the Stuxnet incident raised the issue of state responsibility. The virus was believed to be a state-sponsored cyber weapon. Still, since international law does not clearly define how to assign responsibility, the international community could not effectively hold the involved states accountable. This legal gap shows the limitations of current international law in dealing with state-sponsored cyber-attacks and highlights the need to redefine cyber warfare [6].

3.2. Estonia power grid incident

In April 2007, Estonia was hit by a series of serious cyber-attacks that had major impacts on government websites, bank systems, and the power grid. These attacks were mostly carried out using Distributed Denial of Service (DDoS) technology, which overloads target servers with traffic, causing service disruptions [7].

Existing international law mainly focuses on traditional physical armed attacks and does not clearly define whether cyber-attacks constitute "armed attacks" or "use of force." For example, Article 2(4) of the United Nations Charter prohibits states from using force against the territorial integrity or political independence of other states. Still, this legal framework does not cover the new form of cyber-attacks. Czosseck et al. [7] pointed out that the cyber-attacks in Estonia were carried out by digital means, and even though they had significant impacts on infrastructure, current international laws did not recognize them as "armed attacks" or "use of force."

DOI: 10.54254/2753-7048/2024.24353

In the case of Estonia, though the evidence would suggest that the attacks likely originated from, or were supported by, Russia, international law currently does not establish an appropriate regime for ascertaining state responsibility in such attacks. According to Czosseck et al. [7], current international laws give no detailed guidelines on managing state-supported cyber-attacks. Without these guidelines, it becomes much more tricky and challenging to hold the liable parties accountable and apply sanctions to them. Because of this legal lacuna, the international community cannot deal with such incidents, particularly about the question of responsibility and its prosecution.

Following that, Czosseck et al. [7] also mentioned some weaknesses in the present international legal system regarding cyber-attacks.

Although the Estonia power grid incident indicated large implications for the infrastructure in Estonia, the existing legal framework agreement does not spell out the methods of response or control for these forms of attack. This, in essence, positions the current international legal system to have key shortfalls to address cyber war. We need new ways of defining and addressing cyber-attacks that consider the realistic modern truths of cyber conflict. The Estonia power grid attack also points out the humiliating task set before international law to respond to cyber-attacks, as the very nature of such an attack often falls outside the definition given by traditional laws. Therefore, essentially what is needed is a rethinking of the existing legal framework and new standards for cyber warfare, according to Czosseck, Ottis, & Talihärm [7]. This case initiated many debates on how international law should cope with cyber-attacks and underlined the need for clarity in international standards and legal rules.

4. Conclusion

Analysis of the incident of the Stuxnet virus and the attack on Estonia's power grid displays, with remarkable similarity, the huge weaknesses in the current international law when dealing with cyber-attacks. Cases of this type show the dire need to refresh international humanitarian law to deal with difficulties such as unclear definitions and uncertain responsibility. To begin with, for example, the Stuxnet virus infected very harmful software in the nuclear facilities of Iran and caused serious physical damage. Yet today's international law is considerably bound to traditional notions of armed attack, and it does not identify if the cyber-attack in the form of Stuxnet should fall under the definition of "armed attack" or "use of force." Moreover, even though there was a major disruption of public services and national infrastructure regarding an attack on the power grid of Estonia, the nature and impact of the cyber-attack have not been brought under the categorization of an "armed attack.". This, in turn, creates legal uncertainty, which contributes to increasing difficulties in managing and responding to cyber-attacks.

Also, in that Stuxnet is assumed to be a state-supported cyber-attack tool, there are issues in determining who it is and whether the attackers could be held responsible. In its present form, international law does not have any clear system to deal with state-sponsored cyber-attacks; hence, it is hard to hold the responsible states accountable.

In the same way, although the Estonia attack involved state actions, international law does not explain how to attribute such cyber-attacks. Therefore, leaves the international community with problems in holding the responsible states accountable or applying sanctions efficiently. In both cases, it did show the need for a new legal framework and more clarity about cyber warfare. It would require a new legal framework that clearly defines cyber-attacks under international law for easy response and accountability of states over state-sponsored cyber operations. Both the Stuxnet incident and the Estonia power grid attack show issues with the adequacy of current international law in addressing cyber warfare. The nature and impact of cyber-attacks often exceed traditional

DOI: 10.54254/2753-7048/2024.24353

law's definitions and handling scope, forcing the international community to rethink and establish a new legal framework suitable for cyber warfare.

Therefore, to define cyber warfare clearly, this paper tends to compare it to the traditional use of force and give cyber warfare a similar legal status in international law.

In traditional armed conflict, war is usually defined as a conflict between two or more states using force, involving physical destruction, occupation of territory, or achieving political goals through military actions. Similarly, cyber warfare could be defined as intentional attacks between two or more states through cyber-attacks that disrupt critical infrastructure, disturb the economy or social order, or achieve political goals. Secondly, to limit cyber warfare, international law could say that cyber-attacks should only be considered legal when a state faces a substantial threat and no other non-military means can effectively respond. Also, in traditional war, international law distinguishes between combatants (like soldiers) and non-combatants (like civilians). Similarly, in cyber warfare, it should be clearly stated that non-combatants' cyber assets should be protected, and attacking them should be considered a violation of international law. Lastly, like the Geneva Conventions for traditional war, the international community should promote signing a specific "Cyber Warfare Treaty" to establish the above-mentioned rules and create related enforcement and supervision mechanisms.

With these policy updates, international law can more clearly include cyber warfare into the existing legal framework, ensuring that cyber warfare is subject to strict legal regulation like traditional use of force and effectively protecting civilians from the potential harms of cyber warfare.

References

[1] Buchan, Russell, and Nicholas Tsagourias. "Cyber War and International Law. " *Journal of Conflict and Security Law* 17, no. 2 (2012): 183–186.

[2] Moynihan, Harriet. "The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention. " *Chatham House Research Paper*, December 2019.

[3] Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. "Twenty Years On International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts. " *International Review of the Red Cross* 102, no. 913 (2020): 287-334.

[4] "International Humanitarian Law and Cyber Operations during Armed Conflicts. " *International Review of the Red Cross* 102, no. 913 (2020): 481–492.

[5] Pendino, Stephanie, Robert K. Jahn, and Kirk Pedersen. "U. S. Cyber Deterrence: Bringing Offensive Capabilities into the Light. " *Joint Forces Staff College Academic Journal*, September 7, 2022.

[6] Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon. " *IEEE Security & Privacy* 9, no. 3 (2011): 49-51.

[7] Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 Cyber Attacks. " *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 24–34.