Proceedings of the 4th International Conference on Educational Innovation and Philosophical Inquiries
DOI: 10.54254/2753-7048/17/20231249

When Can Cyberattack Constitute Use of Force: A Case Study of Cyberattack in the Russia-Ukraine Conflict

Yaxuan Leng[1,a,*]

[1]*Law School, Southwestern University of Finance and Economics, Liucheng Street, Chengdu, 611130, China*
a. 1811431234@mail.sit.edu.cn
**corresponding author*

Abstract: In today's international community, cyberattacks occur frequently, and cyberspace has become an important battlefield for political games among major powers. Under the push of cyberattacks, the tension between Russia and Ukraine has further escalated. However, due to the unique nature of cyberspace, the rules under the existing international law are difficult to directly apply to the field of cyberspace. This has allowed states and non-state actors to willfully disrupt the network systems and other infrastructure of other countries, causing damage to people or property. One major issue is when can a cyberattack constitute use of force under international law. Only by clarifying this issue can we further discuss the issues of cyber warfare and the exercise of self-defense right. This article will start with a cyberattack that occurred in the Russia-Ukraine conflict, explore the essence of use of force, discuss the three mainstream theories about when can cyberattack constitute use of force, and use the framework of the Tallinn Manual to analyze whether the aforementioned cyberattack falls under the use of force in cyberspace. Through this series of analysis, we can further clarify the meaning of use of force in cyberspace and promote the construction of a legal framework for international law in cyberspace.

Keywords: use of force, cyberattack, Tallinn Manual

1. Introduction

Russian invaded Ukraine in February 2022. It was not the first instance of Russian aggression towards Ukraine. Prior to the invasion, the most destructive of these attacks was NotPetya, which was deployed in 2017 and caused $10 billion in damage. While it infiltrated most Ukrainian networks and spread to systems across Europe and the UK, no deaths were attributed to it, and it was not a ransomware attack [1].

During the ongoing war between Russia and Ukraine, limited Russian cyberattacks have undermined the distribution of essential goods, such as medicines and relief supplies. These attacks have also included disinformation and deep fake technology. As the invasion began, a cyberattack which is deemed to be attributed to Russia has influenced the broadband internet provided by Viasat [2]. This attack also influenced satellite internet access of Europe, and a number of German wind turbines remained offline. While disruptive, this was the only significant cyberattack at the start of the invasion, as most cyberattacks against Ukraine have been largely attenuated by the strength of

DOI: 10.54254/2753-7048/17/20231249

Ukrainian cybersecurity, which has been bolstered by Western and independent hackers' assistance [3].

Here, the cyberattack on Viasat's broadband Internet services is chosen as an example to analyze. It is crucial to discuss the cut-off point for force usage in cyberspace as it can aid in defining a legal framework for the appropriate response to cyberattacks that qualify as use of force under international law in the cyber field.

2. Problem Statement

2.1. Overview of Cyberattack

2.1.1. Definition

Nowadays, armed conflicts in many states are accompanied by a large number of cyberattacks, which have greatly enriched the forms of armed conflicts. Some governments are attempting to transform cyberspace into a second battlefield by conducting espionage operations or attacking infrastructure of other states through cyber technology. Since the 1990s, with the military's use of cyberattacks in conventional military operations, discussions about "cyber warfare" have gradually emerged. Especially after the "distributed denial of service" (DDoS) attacks on Estonia during 2007 and the "Stuxnet" attack on the Iranian nuclear power plant in Natanz in 2010, discussions about "cyber warfare" in the international community reached a climax.

At present, it is generally undisputed that cyberattacks between states may amount to "use of force" under international law in some circumstances. However, since the UN Charter does not provide a clear standard for use of force. There are still many debates in the international community regarding when can a cyberattack constitute the use of force.

2.1.2. Literature Review

There are three prevailing theories consisting instrument-based theory, purpose-based theory and scale and effect theory, which can answer when does cyberattack constitute use of force in cyberspace [4].

The first theory is the instrument-based theory, which is supported by scholars such as Marco Roscini. According to this theory, the use of weapons is governed by Article 2 of the UN Charter. Traditionally, guns, tanks, and nuclear weapons are recognized as instruments of force. Marco Roscini believes that cyber can also be used as a weapon to achieve the same function as traditional weapons [5]. However, some scholars disagree with the instrument-based theory. For instance, Professor Huang Zhixiong argues that cyberattacks are fundamentally different from traditional weapons due to their distinct mechanisms, capabilities, and operational processes [6].

The second theory is the purpose-based theory, which is advocated by scholars such as Walter Sharp. According to this theory, economic or political force that damages the integrity of territorial and political independence should be subject to the rules of use of force for the purpose of peace and security in the international community [7]. Huang Zhixiong argues that Walter Sharp has a broader interpretation of use of force under UN Charter and it may expand the application of Article 2(4) in UN Charter. The broader interpretation may lead to potential conflicts with other international legal norms.

The "scale and effect" theory is the most widely adopted approach to interpret cyber-attacks as use of force. This theory emphasizes the consequences of cyberattacks, stating that if a cyberattack results in serious outcomes such as the damage of casualties and property, it may be considered a use of force, irrespective of the target of the attack. This theory does not require a comparison between cyberattacks and traditional kinetic weapon attacks in terms of their similarities. Its focus solely lies

DOI: 10.54254/2753-7048/17/20231249

on the scale and impact of the cyber-attack. Michael N. Schmitt proposed some elements to examine the scale and effect based standard, including damages, how fast the attack launch, connection, invasion, quantity, legitimacy, and how much the country involve in. Schmidt's views have had a significant impact in Western academia, not only reflected in the "Tallinn Manual" he edited but also be supported by some Western countries like U.S. The drawback of this theory is that the factors of scale and effect do not have a uniform standard to assess. So far, the rules contained in the Tallinn Manual have not been recognized by any country. And some researchers like Ji Hua, believe that the rules in the manual are a transplant of existing international legal norms and do not create a new set of rules applicable to international cyberattacks and cyber warfare [8].

2.2. Definition of Use of Force

To consider when a cyberattack constitute use of force, it is necessary to first define use of force. In 2015, the UNGGE which is a group trying to maintain peace and security in cyberspace, affirmed the applicability of the principles of the prohibition of use of force under the United Nations Charter and other international law principles in cyberspace [9]. Article 2(4) of the UN Charter provides that the use or threat of force against the territorial integrity or political independence of other states is forbidden. This prohibition on the use of force is a treaty obligation under international law and an obligation under customary law. In Nicaragua v. United States case, ICJ confirmed this obligation based on consistent and widespread state practice and opinion juris. Therefore, the prohibition of resorting to force is binding not only on member states of the United Nations but also on all states except those who persistently object to it.

Since the interpretation of "use of force" is not specific, there are differences in interpretation from various perspectives, resulting in significant controversy regarding the extent of the prohibition against the use of force set out in this Article. Here are other standards and principles that provide the scope of use of force.

Some scholars interpret 'use of force' in a narrow way. They held that force shall be strictly interpreted as armed force and economic or political threat should not be included [10]. And according to Corfu Channel case, the Court denied request of U.K that entry of Albania territorial water by military vessels was not use of force because it was not against territory integrity or political independence of Albania. It is a support for the theory which holds that use of force should be restricted to purposes against territory integrity or political independence of other states.

Some scholars have provided a broader interpretation of the use of force. Based on the textual and systematic interpretation, they argue that Article 2(4) of the UN Charter uses the term "force", while other provisions use "armed force", indicating that "use of force" not only includes traditional "military forces", but also contain more extensive forces, such as economic and political forces. Under this doctrine, cyberattacks, as non-traditional military forces, can be recognized as use of force. However, the author believes that such an interpretation is biased, as the UN Charter simply alternates between "force" and "armed force", and the nature of the two terms is the same [11].

Based on the above, the author believes that "force" should be understood as "armed force" or military force. As technology rapidly evolves, the interpretation of legal terms should also be updated to better align with the original purpose of the legal provisions. Therefore, we should also expand the interpretation of the term "military force" to include not only traditional kinetic weapons but also non-kinetic weapons such as biological and chemical weapons. According to the definition, cyber weapons should also be classified as "military force". Moreover, in Nuclear Weapons Advisory Opinion, ICJ stressed that Article 2(4) of the UN Charter does not mention specific weapons and is applicable to the use of any force, no matter what kind of weapon used [12]. Regarding the question of whether the prohibition of the use of force should be interpretated generally or restrictively against territorial integrity and political independence, this essay argues that the prohibition should be

DOI: 10.54254/2753-7048/17/20231249

considered as general. This is because interpretate the prohibition of the use of force generally is more in line with the purpose of the UN, which is to maintain international peace and security.

Today, some scholars constantly provide legal justifications for governments' domestic and foreign policies, thereby expanding the interpretation of Article 2(4) and Article 51 of the United Nations Charter, and lowering the threshold for the use of force in self-defense. If the force usage threshold for cyberspace is not high, it may easily lead to the militarization of cyberspace. This may cause some technologically advanced countries to fabricate a cyber-attack and use it as an excuse to exercise their right of self-defense or collective defense. In today's information society, such unregulated behavior not only violates the aim of the UN Charter but also seriously undermines international security order, damages the interests of countries, especially those with underdeveloped networks.

2.3. Research Gap and Question

The aforementioned theories are relatively mature and have been widely discussed by many scholars. Based on these theories, many new theories have emerged. Overall, these theories face two problems. Firstly, many scholars' viewpoints lack practicality, as they fail to consider more political and economic factors, making it difficult for them to be adopted by countries and resulting in the issue of cyberspace military operations remaining unresolved. Secondly, many of these theories come from the West or developed countries, making it difficult to form diverse discussions and difficult to confirm a unified standard of universality globally.

3. The Threshold for Use of Force in Cyberspace

3.1. The Prevailing Theory of the Threshold of Use of Force in Cyberspace

The threshold for the use of force is mainly based on the Nicaragua case, in which the ICJ stated that the "scope and effects" of specific acts must be considered to determine if they constitute an "armed attack". This analytical approach is also reflected in the popular Schmitt analysis today. Professor M. Schmitt intends to analyze when a cyberattack constitute the force usage by assessing the quantitative and qualitative factors [13]. These factors include severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility. The Tallinn Manual 2.0 further elaborated and supplemented the Schmitt analysis. The original seven factors have now become eight, namely severity, immediacy, directness, invasiveness, measurability of effects, military character, presumptive legality, and presumptive necessity. These eight considerations can be used to measure the scale and effect of cyberattacks, to determine if a cyberattack is capable of reaching the force usage threshold. Among them, severity and measurability of effects are used to measure the scale factor, while immediacy, directness, invasiveness, military character, presumptive legality, and presumptive necessity are used to measure the effect factor.

3.2. Critics and Case Analysis

Regarding the scale factor of cyberattacks, the Tallinn Manual considers any cyberattack that causes harm to individuals' lives or property, or damage to national interests, to be regarded as force usage. However, the determination of the scale factor in practice is more complex, requiring consideration of factors such as the scope of the attack's impact, the number of targets affected, and the size of the losses. Moreover, there are technical difficulties in determining the extent of the losses, as current network technologies make it difficult to accurately identify the specific number and scale of individual cyberattacks.

DOI: 10.54254/2753-7048/17/20231249

In terms of determining the effect factor, the Tallinn Manual believes that the impact of cyberattacks must be immediate, but there is controversy over how to define immediacy. There is only a simple lower limit requirement for immediacy, and cyberattacks that do not produce effects until several weeks or months later are generally not considered the use of force. “Directness” is mainly used to determine the causal relationship between behavior and consequences, but there are many subjective factors involved in determining causality.

For example, if a cyberattack causes a brief power outage in a hospital, which delays the rescue of people who urgently need medical facilities, resulting in injury or death, can this injury or death be attributed to the cyberattack? The determination of invasiveness and military character is relatively straightforward, as cyberattacks are inherently invasive. The issue here is the degree of invasion, as the degree of intrusion into a nation’s critical infrastructure is certainly higher than that into its commercial infrastructure. However, there is controversy over what constitutes a nation’s critical infrastructure. The Tallinn Manual’s view is that cyberattacks that constitute the use of force should target high-level political and military organizations of states.

The difficulty in determining state involvement lies mainly in practice. Some countries today hire hacker organizations to launch cyberattacks against other countries. Due to the anonymity of the network, it is difficult to track down the specific actors behind cyberattacks, resulting in countries accused of launching cyberattacks often shirking responsibility for various reasons. The Tallinn Manual’s provisions regarding presumptive legality are relatively vague. The Tallinn Manual cites the “Lotus case” established by the PCIJ in 1927, which established the principle that “ everything which is not forbidden is allowed “, believing that if there is no rule in the international community that recognizes certain network activities as violating international law, then such network activities are in compliance with international law. However, some scholars point out that the principle established in the Lotus case only applies to states’ handling of internal affairs and not to handling external affairs and jurisdictional boundary issues. The emergence and results of international cyberattacks cannot all occur within a single country’s borders, and the future legal rules governing them will inevitably involve national network jurisdiction and external affairs. Applying the “Lotus” principle to the regulation of international network behavior is a misreading of international judicial practice in the Tallinn Manual.

Although there are many controversies surrounding the Schmitt analysis and Tallinn Manual, it can be said that they are the most widely known framework for analyzing a cyberattack and provide reliable reference for states to construct laws in cyberspace. Despite international experts repeatedly emphasizing that the Tallinn Manual is just a research publication and does not represent the views of any country or organization, its influence cannot be ignored. Some countries have expressed their recognition of the legal status of the Tallinn Manual and use it as an important reference for policy-making.

3.3. Case Analysis

In this article, the Tallinn Manual’s analytical framework will be used to determine whether the cyberattacks in the Russia-Ukraine conflict constitute force usage under international law. The key problems in this analysis are the assessment of the severity of the attack and the involvement of the state. Specifically, we will examine these two elements to argue whether the cyberattack launched by Russia just before invading Ukraine, constitute the use of force. It should be noted that although the Tallinn Manual has been the subject of much controversy and is only a research work that does not represent the views of any country or organization, its influence cannot be ignored. Some countries have recognized the legal status of the Tallinn Manual and used it as an important reference standard for policy making.

DOI: 10.54254/2753-7048/17/20231249

3.3.1. Severity

A senior Ukrainian cybersecurity official stated that Ukraine suffered enormous loss in communications at the beginning of the conflict because of the cyberattack, which also disturbed a number of German wind turbines. Although the cyberattack did not cause physical harm to individuals, it did cause damage to property. However, the loss of communication only caused minor discomfort or irritation, and the network was largely stabilized within hours and fully stabilized within several days. Furthermore, the damaged wind turbines did not belong to critical infrastructure. Therefore, it is difficult to argue that this cyberattack significantly impacted critical national interests and met the severity criteria. And the assessment of this criterion is not final, because the cyberattack may influence or even decide the development of the latter armed conflict. However, there is currently no evidence to suggest that this cyberattack has played an important role in determining the subsequent development of the Russia-Ukraine war.

3.3.2. State Involvement

Under Drafted Articles on Responsibility of States for Internationally Wrongful Acts, conducts of state organs including organizations and any person shall be considered as conducts of state under Article 4. And conducts directed or controlled by a state shall be considered as state acts under Article 8. UK and US intelligence suggest that Russia can be attributed to a cyberattack which disrupted American commercial satellite internet company Viasat. But the official lacked the evidence to say so publicly. Therefore, it is accurate to say that it is difficult to argue that this cyberattack meets the criteria of state involvement.

In conclusion, the cyberattack targeting Viasat during the conflict between Ukraine and Russia is not a use of force in cyberspace.

4. Suggestions

4.1. Determine the Applicable Legal Framework

Currently, there is no specific standard of the threshold of force usage in cyberspace. Many practical issues stand in the way of law enforcement in cyberspace. For example, Article 2(4) of the UN Charter and customary international law do not govern non-state actors, including individuals, organized groups and terrorist organizations, unless their conduct can be considered as state acts [14]. In Russia-Ukraine war, there exists many volunteer hacker groups, which are non-state actors. They operate in a relatively unregulated environment, making it difficult to track and prosecute them. Some countries may secretly hire non-state hacker groups to attack the network systems of other countries in order to achieve their political goals and evade the responsibility that they should bear as a state. Therefore, one of the key challenges is identifying the applicable legal framework for regulating the actions of non-state actors in cyberspace. And states should strengthen international cooperation and collaboration to better track and prosecute cyber criminals.

4.2. Ensure the Widespread Application of the Tallinn Handbook Globally

Another issue is that some rules in the Tallinn Manual are one-sided, representing the interests of Western cyber powers and ignoring the interests of many developing countries or countries with underdeveloped networks. In order for the Tallinn Manual to be universally recognized by the international community, it needs to solicit opinions from various countries and consider the needs of different countries. Based on this, relevant rules should be adjusted to ensure that the Tallinn

DOI: 10.54254/2753-7048/17/20231249

Manual can be widely applied and ultimately become customary international law, better addressing the problem of international cyber conflicts.

5. Conclusion

Since the international community lacks clear legal guidelines for cyberspace, there exists unregulated behavior by state and non-state actors, resulting in an increasingly militarized and competitive environment. International law does not currently provide a clear definition of force usage in cyberspace, nor does it establish a standard for the threshold of such force. To address this issue, this article discusses various theories on "use of force" and analyzes the cyberattacks during the Russia-Ukraine conflict. Despite the shortcomings of the Tallinn Manual, governments can use it to clarify their stance on use of force in cyberspace and unify their understanding of its definition. This will help establish international legal norms for cyberspace. As a new and evolving field, there is much room for exploration in cyberspace. Countries should prioritize global peace and development, abide by the United Nations Charter, and use cyberspace as a platform for global communication, rather than as a tool for political competition between states.

References

[1] *Andy Greenberg. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved form What is NotPetya? 5 Fast Facts | Security Encyclopedia (hypr.com).*

[2] *James Pearson, Raphael Satter, Christopher Bing and Joel Schectman. (2022) Exclusive: U.S. Spy Agenc' Probe: 5abotqge of Sn/ellie Internet Dung Russan Invasion, Sources Say. Retrieved form Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say | Reuters.*

[3] *Marcus Willett. (2022) The Cyber Dimension of the Russia–Ukraine War. Survival, 64:5, 7-26.*

[4] *Marco Roscini. (2015) Cyber Operations as a Use of Force. Research Handbook on International Law and Cyberspace, Edward Elgar Publishing.*

[5] *Macro Roscini. (2010) Worldwide warfare—jus ad bellum and the use of cyber force. Max Planck Yearbook of United Nations Law,14, 96.*

[6] *Huang Zhixiong. (2015) International Legal Issues concerning 'Cyber Warfare' and Strategies for China: Focusing on the Field of Jus ad Bellum. Modern Law Science, 5, 148.*

[7] *Walter G. Sharp Sr. (1999) Cyberspace and the Use of Force. Aegis Research Corporation, 88-91.*

[8] *JI Hua. (2016) Use of Force in the Cyber Warfare as Defined in Tallinn Manual: Analysis from the Angle of the International Law. Jianghan Academic, 35.3, 28-34.*

[9] *United Nations General Assembly. (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of Internal Security, A/70/174, para.26.*

[10] *Yu Mingyou and Ma ran. (2006) UN Collective Security System's Legal Control of the Use of Force: Challenge and Reform. International Law Review of Wuhan University, 2, 60.*

[11] *Zhang Hua. (2022) Legal Pathways for the Application of the Prohibition on the Use of Force Principle in Cyberspace. China Legal Science, 2, 286.*

[12] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports (1996). p.226, para.39.*

[13] *Foltz and Andrew and C. (2012) Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate. Joint Force Quarterly, 64, 42-43.*

[14] *J. Valuch and Ondrej Hamuľák. (2020) Use of Force in Cyberspace. International and Comparative Law Review, 20, 174-191.*