Page 462 - 478 **DOI:** *https://doij.org/10.10000/IJLMH.113811*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 6

2022

The Need to Fill Legal Vacuum in International Law to Deal with Non-State Actors in Cyber Operations

ANKIT LAVANIA[1]

ABSTRACT

The increasing involvement of the cyber domain in modern-day living has impacted the world order and its various actors. Cyberinfrastructure is involved in most societal activity, which becomes more accessible and vulnerable. It is essential to regulate any conflict around this space as these conflicts impact human life. However, Due to the lack of legal framework, non-attribution and existing ambiguity concerning cyber-attack, the non-state cyber attackers pose a global security challenge. This paper contributes to the ongoing discussion on the necessity of obligatory norms and rules under International Law to regulate such conflicts. International cooperation is necessary due to the limited scope of international law to deal with non-state actors, as there are difficulties in applying general international principles. The paper concludes that cyber governance is urgent and requires the attention and cooperation of the international community to stop the possible future destruction due to cyber-attacks by non-state actors. After a decade-long experience of alarming cyber-attacks, the international community could not agree on a specific governance mechanism to deal with non-state cyber-attacks.

I. INTRODUCTION

Arbitration Technological advancement is a deal. We all sign up for this deal to conduct our day-to-day tasks efficiently. A large part of our daily lives revolves around cyberspace, from electricity to healthcare and clean water to communication; our major activities depend on the cyber world. It connects individuals and communities across geographical borders, and they socialize beyond sociocultural boundaries. Cyber Infrastructure is a crucial part of our economy, healthcare, banking and security. However, this space has never been considered a democratic space as decisions related to its functioning are taken by a few individuals or companies. In contrast, web designs involve traditional political issues such as privacy, security, and sovereignty that have to work in a democratic setup.[2] The cyber domain is known as a lawless

[1] Author is an Attorney at SBA Group Solicitors & Consultants, India.

[2] Harari, Y. *Homo Deus: A brief history of tomorrow.* (1st edn Harvill Secker 2016).

 [ISSN 2581-5369]

zone in its basic functioning. Such an unrestricted cyber world makes it a vulnerable infrastructure where state or non-state actors can become victims.

The cyber revolution brought several new issues and threats due to our dependency on the cyber world and increasing integration. Also, it exists in unrestricted space, which consists of minimal control in its functioning as it is regularly evolving. It is harder to regulate an area that transforms itself ten times until the governmental tortoise moves and intervenes to restrict the internet space. One such example is the Department of Justice (US) stated on 5 December 2016 regarding the Avalanche case, where the operation to take down a cybercriminal group with the cooperation of 40 countries took four years.[3]Also, it stated that the criminal group had used their technology against them for years, and their cyber network became more complex and hosted more than two dozen cyber malign software for years.[4] These operations afford corroboration because cyberspace is transforming faster than the government initiatives to regulate them.

However, as Noam Chomsky, the American philosopher and political activist, wrote, "optimism is the best strategy for making a better future. Because unless we have faith that the future can be better, we will not step up and take responsibility for changing it."[5] When the Internet space cannot be kept away due to our dependency, it needs to be regulated for protection from the malign cyber activities conducted by states or non-state actors. However, various states have established cybersecurity regimes to deal with such operations in their country. For example, the US Department of Defence has been expanding its cyber command operations to deal with non-state actors attacking from another state's territory.[6] These developments in the defence strategies of countries show the increasing threat of non-state actors in cyberspace.

This paper analyses how non-state actors have become critical in cyberspace protection and how the domestic legal mechanism to deal with such operations is insufficient. We will examine how these cyber-operations do occur in a legal vacuum. Also, why do we need international regulation to deal with such cyber operations conducted by non-state actors? I argue in this paper that more significant cooperation and coordination are required in order to deal with such cyber operations rather than just focusing on domestic defence strategies. I advocate that to

[3]Department of Justice, Office of Public Affairs, The United States, *Avalanche network dismantled in International cyber operations*, 5 December 2016, https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation Accessed Date 10 July 202.
[4]ibid.
[5]Why we study International law 1.
[6]The New York Times, *US cyber commands expand the operation to hunt hackers from Russia, Iran and China* 2 November 2020 https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html Accessed Date 11 July 2021.

 [ISSN 2581-5369]

achieve stable and robust cyber deterrence, the international community must approach the international legal framework mutually. Also, this paper analyses the need for explicit norms and binding international rules to reduce the risk of global cyber conflict. I do not advocate that existing international laws should be interpreted for their better application; instead, this paper analyses how they are insufficient to address these conflicts.

The paper is structured as follows: Section II defines some basic concepts to understand the issue in a better way and discusses the existing term of debate. Section III describes the cause of action or cyber operations conducted in recent times by non-state actors and the danger associated with these cyber-attacks. Section IV offers an attempt at defining the scope of existing international law to deal with non-state actors in cyber operations—this section explicitly analyses specific international law principles which deal with the issue of cyber-conflict. Section V argues that international law lacks adequate regulatory norms to deal with cyber operations by non-state actors. Section VI presents a case for establishing an international legal regime and filling the legal vacuum. This section highlights the limitation of the existing international regime and argues why we need consensus for such an agreement. Also, I outline a few suggestions that the international community may follow to address the issues of framing such an agreement. Section VII concludes by stating that constituting an international framework is urgent more than ever to deal with the global cyber conflict.

II. DEFINITIONS AND TERMS OF DEBATE

There are unsettled terms and definitions in cyberspace as it is an emerging discipline not codified by any law unanimously. In this section, we will engage with a few phrases to understand the issue in a better way. To analyse the whole case of cyber conflict, it is a prerequisite to understanding the essential term such as "cyberspace", defined in the Tallinn Manual 2013 that cyberspace is information, communication and technology infrastructure to control and store data.[7] This infrastructure helps us communicate and conduct the day-to-day life of humans more efficiently through internet services. Other terms such as cyber warfare and non-state actors also need specific attention to understand the issue better.

Countries are shifting from traditional armed attacks to cyber-attacks as we depend on the cyber world where cyberspace is misused. Cyber-attack weapons are made of software and data built for targeting cyberinfrastructure.[8] These cyber-attacks conducted by non-state actors can lead to conventional war between states. For instance, a cyber-attack on a state's electric grid can

[7] Schmitt MN, *Tallinn Manual on the International Law Applicable to Cyber Operations* (Cambridge University Press 2013).
[8] Eilstrup Sangiovanni, Why the world needs an International Cyberwar Convention (2018) 31 philos Technol 379.

 [ISSN 2581-5369]

disturb the electric supply to hospitals, banks, and other essential places. Such an attack can disrupt people's lives, similarly to a traditional attack. Cyberinfrastructure can also be used as a weapon to destroy the strategic assets of another country. Hence, these cyber-attacks can rise to the level of international conflict, which may lead to cyber warfare.[9]

There are state actors who can be preparators of cyber-attack, such as Russia and China. Apart from state and non-state actors, other actors are involved in various cyber-attacks, such as hacktivists and cybercriminals. As this paper primarily deals with cyberattacks by non-state actors, we need to understand this in detail. The non-state actors in cyber-attack are individuals or groups "that are perpetrators or victims in various malign cyber operations".The conduct of these actors in cyber operations is primarily not regulated under international law.[10] Although, in minimal cases, international laws apply to them. The point of conflict with non-state actors in cyber operations is its attribution to the state discussed in the paper. The issue of attribution is relevant here, as this gives a legal argument for proving the state's responsibility for non-state actors' conduct.

III. CYBER-ATTACK IN ISSUE

In April and May of 2007, Estonia saw cyber warfare in its territory, leading to a large-scale disturbance of the political and economic framework. The cyber-attack in Estonia targeted various websites, including the office of the Prime minister and President, Media organizations, banks, and whole internet infrastructure and information systems.[11] After the attack, the Estonian government initially claimed that non-state actors from Russia were involved in the attack based on Internet protocol (IP) addresses traced from Russia. Nevertheless, Russia denied all the claims made by the Estonian government, and there were inadequate international regulations available for Estonia to proceed under international law.[12] However, all those attacks were mild and simple DDoS cyber-attacks. Nevertheless, these attacks took the international community's attention and the discussion on the vulnerability of cyberinfrastructure was initiated within global communities.

In 2009, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), a training institution based in Tallinn, Estonia, started preparing a manual with a few independent

[9]ibid.
[10] Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn Cambridge University Press 2017).
[11]The Wall Street Journal,*Cyber Attack vexes Estonia, poses debate18* May 2007https://www.wsj.com/articles/SB117944513189906904 Accessed date 2 July 2021.
[12]Haataja, S, The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach (2017) 9 Law, Innovation and Technology 159.

groups of experts on the international law governing cyber warfare. This initiative of NATO CCD COE came up with two manuals, namely "Tallinn Manual on the International Law Applicable to cyber warfare in 2013". Afterwards, in 2017 ", Tallinn Manual 2.0 on the International Law Applicable to cyber operation" (hereinafter referred to as "Tallinn Manual 2.0"), which deals explicitly with the issues related to cyber-attack by non-state actors. The International community appreciated the manuals prepared by these experts, which began the international cooperation and regulation debate. However, the manual could not get support other than the NATO Countries which sponsored the group and merely interpreted the existing international law without providing any distinct legal mechanism".[13]

In addition to the Estonian cyber-attack, in December 2016, the department of justice, US, announced an international cyber operation to dismantle the cyberinfrastructure called "Avalanche", which launched a cyber-attack in 180 countries and was responsible for damaging economic assets.[14] Avalanche cyber network used to provide protected infrastructure to hide from cybersecurity experts, and through that network, non-state actors conducted cyber-attacks in various countries.[15] Since 2010, the Avalanche network has stolen information from 5,00,000 computer systems of victims daily.[16]After an exhausting four years of an international operation, in which the police system of 25 countries was involved, they dismantled the infrastructure. They arrested a few criminals operating in cyber-attack.[17]The avalanche case showed the international community to what extent the non-state actors can harm the nations without a proper mechanism and that it is difficult to stop these non-state actors from conducting cyber-attacks.

Several other countries faced similar cyber-attacks conducted by non-state actors and lacked legal regulation of International law. The Colonial pipeline, which was supplying 45% of fuel to the east coast of the US, had to shut down due to a cyber-attack in May 2021.[18]The Federal Bureau of Investigation (FBI) in the US has confirmed that the attackers hold the data hostage till the colonial pipeline company does not pay the ransom. This attack led to fuel shortages across the east coast of the US and also an increase in fuel prices.[19]Similarly, a news report from

[13] Eilstrup Sangiovanni (n 7) 388.
[14]Department of Justice, US (n 2) 1.
[15]ibid.
[16]Department of Justice, US (n 2) 2.
[17]France 24,*Ukraine Arrest Avalanche cyber-crime organiser,* 26 February 2018 https://www.france24.com/en/20180226-ukraine-arrests-avalanche-cybercrime-organiser-policeAccessed date 5 July 2021.
[18]Indian Express,*The dark side cyber-attack on a US oil pipeline and how it impacts price*, 15 May 2021 https://indianexpress.com/article/explained/explained-the-darkside-cyberattack-on-a-us-oil-pipeline-and-how-it-impacts-prices-7310822/ Accessed date 2 July 2021.
[19]ibid.

 [ISSN 2581-5369]

the New York Times claimed that a criminal group based in eastern Europe hacked the data of the Washington police department. Including this incident in the US, there are 26 cyber-attack on government agencies conducted by these non-state actors.[20]

The cybersecurity and infrastructure security agency (CISA) of the US and the national cybersecurity Centre (NCSC) of the United Kingdom have warned other countries that they must be ready to battle cyber attackers. The cyber attackers are trying to steal and disturb valuable information related to healthcare and research institutions and acquire sensitive data associated with the covid19 pandemic.[21] Microsoft also claimed that cyber attackers from Russia and North Korea are trying to infiltrate India, France, South Korea and the US vaccine companies.[22] In October 2020, there was an electricity blackout in the mid of the pandemic in Mumbai, when it was dealing devastating effects of the Covid-19 pandemic. However, this blackout was only for a few hours, but it could have harmed the infrastructure majorly. Due to the covid-19 pandemic, the healthcare system has already burdened the city due to short oxygen and bed. In the mid of this crisis, all the hospitals had to switch to emergency electric supplies for ventilators and other healthcare facilities to the extent they could manage. This incident could have been catastrophic if this blackout had been extended for a couple more hours. The preliminary report of the cybersecurity investigation team indicated that this blackout was a cyberattack and not a human error.[23]

A highly reputed cyber intelligence platform, Recorded Future, based in the US, published a report stating that a Chinese hacker group named RedEcho targeted the Indian power sector. Since early 2020, Recorded Future's inskit group has seen an increase in suspected cyber intrusions from Chinese territory.[24]All these continuing incidents of cyber-attacks show the vulnerability of cyberinfrastructure. These cyber operations prove how a cyber-attacker can disturb the whole system from another country's territory. Also, such an attack does not hamper just cyberinfrastructure but ultimately affects the individual and entire countries who are victims of these attacks and dependent on the cyber world.

---

[20]New York Times,*DC. US police department data lacked in cyber-attack*, 27 April 2021https://www.nytimes.com/2021/04/27/us/dc-police-hack.html?searchResultPosition=1 Accessed date 2 July 2021.

[21] Reuters,*state-backed hackers targeting coronavirus responders, US and UK warn*, 5 may 2021 https://www.reuters.com/article/us-health-coronavirus-cyber-idUSKBN22H1UG Accessed date 2 July 2021.

[22]Microsoft,*Cyber-attack targeting healthcare must stop*, 13 November 2020 https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ Accessed date 2 July 2021.

[23]The Hindu, *Cyber sabotage led to October 2020 outage in Mumbai*, 1 March 2021https://www.thehindu.com/news/cities/mumbai/cyber-sabotage-led-to-october-2020-outage-in-mumbai-minister/article33964939.ece Accessed date 2 July 2021.

[24]Recorded Future, *China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions*, (CTA - CN - 0228, 2021).

 [ISSN 2581-5369]

IV. Scope of international law concerning cyber-attack by non-state actors

The prerequisite is to look into existing rules and regulations to inquire about the need for a legal mechanism that deals with cyber operations in a sovereign state. In that case, we need to determine whether cyber operations by non-state actors occur in a complete legal vacuum or if any regulatory mechanism exists presently. Does the international community have any specific laws which bind non-state actors under an umbrella of international law?

In this chapter, we will discuss the laws governing such cyber operations. Cyber operations are governed by established international law in all countries. However, it is not decided how these laws will be applicable and what kind of replacement or change is needed. This chapter will inquire about the applicability of international laws when cyber-attack occurs by non-state actors. We will look into a few general international law principles, the law of armed conflict and their interpretations of how these laws will govern such operations. So, we can determine whether cyber operations by non-state actors occur in a legal vacuum.

A. Law of war:

The application of the law of armed conflict needs to be determined for a holistic understanding of the present governance of cyber operations under international law. In the era of technology, where states are connected through the cyber network, we have seen vulnerabilities in cyberinfrastructure in various cyber operations worldwide. Although the cyber operation is new in attacking another state, these operations harm the states as the non-cyber operation would have affected them. Then how this whole conflict will be regulated under international humanitarian law? Here, the discussion would lead to two specific questions to resolve such an issue. Whether the application of international law of armed conflict will extend to governing the non-state actors? Furthermore, what boundaries does the law of armed conflict follows while dealing with cyber operations in another state by a non-state actor?

To answer these questions, we need to understand the provisions which deal with the law of war. The law of armed conflict limits the effects of armed conflict due to humanitarian reasons. It also establishes safeguards for the protection of those who are no longer participating in hostilities and lacks the means and method of warfare. Common Article 2 of the Geneva conventions provides that armed conflict signifies the de facto hostilities conducted in the territory of another state. Also, it states that this provision will apply to peacetime as well.[25]The

[25]Geneva Convention I-IV, Art. 2.

use of force, within the meaning of Article 2(4) of the UN charter, covers cyber operations when it affects the territory in a way that can be compared with the hostilities of traditional attacks or non-cyber operations.[26] In the Prosecutor v Tadic case, the ICTY noted that when private entities or individuals are conducting operations on the armed forces or state authorities, they will be considered de facto state organs.[27] Hence, the state will be responsible, and IHL is applicable in such a situation as it will be regarded as an attack launched by a de jure state organ.

The complex situation lies in dealing with the individuals or entities involved in the attack, which are neither state organs nor authorized by the states. Here it is important to note that individuals do not attract the law of armed conflict when they are not attributable to the state.[28]Only providing material for an attack, such as software or computer hardware, is not sufficient to attribute an individual's action to the application of International Humanitarian Law.[29] The Prosecutor v. Limaj case in the ICTY stated that the party must have some degree of organization to establish the armed conflict.[30]For instance, the cyber-attacks on Estonia in 2007 where attackers were not authorized or attributed to the host state. Also, the individuals conducting these cyber-attacks do not fulfil the organized criteria. Hence, Estonia in 2007 did not attract the law of armed conflict. Establishing the applicability of international humanitarian law here is considered a challenging task where the law of armed conflict will not be able to govern the cyber-attack by non-state actors when they are not attributed to the host states. However, the fact that these actors are not attributed to the host state does not stop them from attacking and damaging the targeted state's infrastructure is problematic. This is the most discussed issue among international law experts related to cyber-attacks.

However, when dealing with non-state actors' position in peacetime, the Tallinn Manual 2.0 projects a critical argument. When states are in peacetime, and a cyber-attack occurs in a targeted state's territory, the law of armed conflict does not govern such attacks. Hence, the law of war does not regulate non-state actors that are not present in the armed conflict.[31] For instance, if a group of thieves attack the cyber network of a state or non-state corporation for a ransom demand. In principle, the law of war does not deal with or regulate such actions of non-state actors. Now we can answer the second question as well, which we posed at the beginning of this chapter: if the law of international armed conflict has not reached the non-state actors, it

[26]Schmitt (n9) 330.
[27] [1999] ICTY-94-1-A,144.
[28]Michael Schmitt, Classification of Cyber Conflict (2012) 17 JCSL 245.
[29]ibid.
[30] [2005] ICTY03-66-T Para 89.
[31]Schmitt (n 9) 376.

also can not regulate the cyber-attack they do.

Hence, we can say that international humanitarian law does not regulate the cyber-attack conducted by non-state actors or private entities in peacetime. However, this does not prove that such activities are conducted in a legal vacuum. In the other parts of this chapter, we will inquire about the extent to which cyber operations by non-state actors are regulated by international law and whether existing international law effectively deals with such activities.

B. Principle of state sovereignty:

The theory of sovereignty and obligation is the product of modern international law. Sovereignty, as the fundamental principle of international law, guides the states to analyze the behaviour of states among themselves. This principle sets the essential criteria of legal obligation on countries, where they will respect the sovereignty of each other through expressing their consent. The principle of state sovereignty binds various kinds of cyber-attack and state cyber operations under an obligation to respect the sovereign rights of each state.[32] Also, it implies that the state has sovereign rights and control over the cyber operation and infrastructure available on the territory concerned with the state. The Island of Palmas arbitral award case in 1928 stated that sovereignty consists of the Idea of independence among nations, which signifies the exclusion of other states from the internal function of the state.[33] As specified in Article 2(1) of the UN Charter, all states are equally based on the principle of sovereign equality. Every state must consider other states' territorial integrity and political independence. Also, it is essential on the part of every state to comply with its international obligations.[34]

Infringing the sovereign rights of another state through cyber operation is considered to disregard the international obligation of sovereign equality. The act of cyber-attack violates the principle of sovereignty. Cyber operations should not be conducted beyond the borders as they can damage the physical objects or cyberinfrastructure which is part of the targeted state. Also, states can exercise sovereignty over people who conduct these cyber operations. There are two kinds of options available to deal with unwanted cyber activities. First, the cyber-attack can be governed by the state's domestic laws and controlled by them. The second is the international obligation of the states under sovereign equality to protect and safeguard the infrastructure from

[32]THE DIGITAL WATCH GENEVA INTERNET PLATFORM, 2015 UN GGE - REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS ON DEVELOPMENTS IN INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY, 26 JUNE 2015 HTTPS://DIG.WATCH/UN-GGE-REPORT-2015-A70174 ACCESSED 8 JUNE 2021.

[33] Island of Palmas Case, (1928) II RIAA 829, ICGJ 392.

[34]Nicaragua vs United States of America [1986] ICJ Rep 14.

any cyber activity on its territory.

Although in the Tallinn manual, the experts opined that the principle of sovereign equality only binds states and does not extend to non-state actors. Further, they agreed on the argument that non-state actors do not have any obligation to respect the sovereign equality of states, whereas this principle only deals with the states.[35] For example, the cyber operation by a terrorist organization does not violate the principle of sovereignty when it is not attributed to the states. When non-state actors are involved in cyber operations that are not attributed to the states, it does not imply that they can be considered legal. The above statement signifies that the domestic laws of the victim state will apply to these actors rather than the international law of sovereign equality.[36]The international group of experts also stated that countries must comply with their due diligence obligation against another state when non-state actors operate from their territory.[37]

C. Due Diligence:

The due diligence principle specifies that every state has a responsibility to not knowingly allow any activity on its territory that infringes the right of other countries.[38] Inactive behaviour concerning wrongs committed on the state territory violates the due diligence principle's legal obligation. A state is supposed to ensure that its territory is not used to attack and harm another state.[39] In cyber operations, the Due Diligence principle considers the association of three parties—first, the state, which is targeted through a cyber-attack. Second is the territorial state where cyberinfrastructures exist. Third, the parties involved in the cyber operation. Here, while interpreting the due diligence principle, the group of experts in the Tallinn manual stated that it would govern any third party, whether it is an individual or organization considered as a non-state actor.[40]

However, the due diligence principle will only apply when the non-state actor conducts a serious harmful cyber operation against the target state.[41] The cyber operation by non-state actors could be considered harmful only if the same attack caused a violation of international obligation if the state had executed that act. For instance, if a non-state actor has conducted cyber operations against the targeted state, thereby causing severe harm, then the territorial state from which the

[35] Schmitt (n 9) 18.
[36]ibid.
[37]ibid.
[38] Island of Palmas Case, (1928) II RIAA 829, ICGJ 392.
[39] Corfu Channel Case (UK v Albania) [1949] Rep 4, 22 (ICJ).
[40] Schmitt (n 9) 32.
[41]Schmitt(n 9) 36.

 [ISSN 2581-5369]

non-state actors operate will be held accountable for the operation. Hence, the due diligence principle will be applicable in this scenario.

In the trial smelter case, it was decided that the threshold of serious harm for application of the due diligence principle is not settled in international law.[42] Also, the group of experts in the Tallinn manual could not draw a line to distinguish what should be considered severe harmful acts when a cyber-attack occurs in a state. The experts have tried to interpret the due diligence principle so that when non-state actors cause severe adverse consequences to the target state, the obligation is on the states. Contrary to that, the group of experts mentioned in rule 4 of the manual that when the actions of non-state actors are attributable to states only after that, the principle of sovereign equality applies and states will be considered responsible.[43] Hence, it is difficult to understand whether cyber-attacks pass the threshold of serious harm for the application of due diligence. There are no established norms to recognize to what extent any cyber attack damages the cyberinfrastructure for considering it serious harm to the targeted state. In this situation, the due diligence principle cannot protect the victim state.

D. Jurisdiction:

The general rule of jurisdiction indicates the regulation of a person, object or activities under a country's national law governed by civil or criminal laws.[44] The usual basis for exercising the principle of jurisdiction is territory. The Tallinn manual stated that jurisdiction in cyber operations occurs when it originates or occurs on the targeted state's territory and if this operation seriously harms the targeted state.[45] The cyber domain is interconnected worldwide, which distinguishes domestic jurisdiction in this matter where an individual can harm the targeted state from another state. However, the above-mentioned sovereign equality doctrine restricts the states from interfering in other states' matters.

The international group of experts in the Tallinn manual stated two requisites to determine the role of the jurisdiction principle in cyber operation. First, the cyber operation must deal with a targeted country's internal or external actors. Furthermore, second, state or non-state actors must have intervened in the targeted states so that the use of force was there and the free will of states compromised due to the attack.[46] The customary international law of jurisdiction does not obligate the international community to cooperate in domestic matters. However, international

[42]Trail Smitter case, [1963].
[43]Schmitt (n 9) 20.
[44] Malcolm N Shaw, International law (7th edn, CUP 2008).
[45] Schmitt (n 9) 52.
[46]Schmitt(n 9) 55.

 [ISSN 2581-5369]

law, such as human rights laws, obliges the states to cooperate in cyber-crime matters.[47] Nevertheless, there is a limitation to applying such laws, and states could not investigate the crime in other states' territorial jurisdictions. In comparison, Informal cooperation in the cyber-crime among states subject to domestic laws is more prevalent and beneficial when no specific legal instrument is present to deal with such a situation.[48]

E. Attribution of cyber-attack by non-state actors:

The general understanding is that private entities or individuals, i.e. non-state actors are not attributable to states.[49] The act of non-state actors must relate to the direction given by states to establish the attribution of states. Article 8 of the article on the responsibility that cyber-attack by the non-state actor is only attributable by states when cyber-attack was conducted on the direction of states and states does not deny that they have attacked indirectly.[50] The ICJ in the Nicaragua case held that if a state has effective control over the action of the non-state actor, then it is considered attributable by the state.[51] For instance, if a non-state actor has conducted a cyber-attack on the medical research institution in the pandemic in the direction of a state due to its border conflict with another state, then this action of the non-state actor will be attributable to the host state.

However, a state's general support for encouraging non-state actors is not sufficient to establish attribution.[52] A state must effectively control non-state actors' actions and not just supplement the cyber activities. For instance, if a state makes a confidential contract with a cyber intelligence company to leave sabotage in the governmental software of another state, then the former state has effective control over the action of that company. Hence, states that are not controlling the non-state actor have no obligation under the law of international responsibility for the acts of non-state actors. Also, International law does not provide rules that determine what and how much evidence would be enough to establish attribution in the cyber operation.[53] In this scenario, the victim state cannot retaliate against the host state unless the action of the non-state actor is attributable to the host state, which creates a certain degree of legal vacuum in dealing with such operations.

[47]Schmitt (n 9) 75.
[48]ibid.
[49] Draft articles on Responsibility of States for Internationally Wrongful Acts 2001, SI A/56/10.
[50]ibid.
[51] Nicaragua (n 31) 140.
[52]Schmitt (n 9) 97.
[53]The Hague Program for cyber norms, *Three tales of attribution in cyberspace: Criminal law, international law and policy debates*, 2020 https://www.thehaguecybernorms.nl/research-and-publication-posts/three-tales-of-attribution-in-cyberspace-criminal-law-international-law-and-policy-debates Accessed Date 8 July 2021.

 [ISSN 2581-5369]

V. ISSUES IN THE APPLICATION OF INTERNATIONAL LAW

After understanding the scope of the existing international legal framework, it is determined that Public International law does not entirely regulate non-state actors. It has a very limited scope in regulating non-state actors as no legally binding instrument is available for cyber-attack. However, Tallinn Manual has tried to interpret the existing international law, but the manual is not a binding instrument but produces opinions from an international group of experts. Majorly, International law has a few problems which restrict its application to extend to non-state actors. First, the international community has not been able to make a consensus on defining the application of terms such as the use of force, armed conflict, effective control and serious harmful acts. An international group of experts in The Tallinn manual could not provide proper definitions of terms, but they have provided terms such as severity and immediacy.[54] Whereas International law needs uniformity in these terms, it helps the states interact among themselves and establish a common legal framework to deal with international legal issues.

Second, international law focuses primarily on states where International Public Law only revolves and interacts among states. States ultimately regulate non-state actors when they are subject to state sovereignty and not otherwise.[55] This approach to international law creates a legal vacuum when dealing with non-state actors in cyber operations. Third, as there is no legal mechanism present to establish the attribution that can create a link between state and non-state actors in cyber operations, this issue has become a challenge for the victim state to establish a relationship between the state and non-state actors, which causes a situation of no accountability that could be determined in the cyber-attack. Finally, there is no penalty for violation of international law. At the same time, there is no incentive mechanism for international law compliance due to the lack of specific legal instruments concerning cyber-attack. Hence, this proves that international law disassociates the non-state actors from its regulatory framework, which shows the state-centric character of international law and creates issues while dealing with non-state actors. These challenges in applying international law in dealing with non-state actors push the international community to negotiate among themselves and establish an entirely new legal framework for such cyber operations.

[54] Just Security, New York University School of Law, *France's Major Statement on International Law and Cyber*, 16 September 2019 https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/ Accessed Date 8 July 2021.
[55] Schmitt, M. N. and Watts, S. Beyond state-centrism: international law and non-state actors in cyberspace (2016) 21(3) JC&SL, 595.

VI. THE NECESSITY OF CYBER WARFARE LEGAL MECHANISM

As we have seen above, cyber-attacks have evolved with the transformation of the world with technology, and such operations are taking place every year through a protective cyberinfrastructure. There are minimal instances where cyber-attack by non-state actors like individuals or groups can be regulated through international law if they are attributable to the state. Otherwise, international law principles apply only to state actors, while non-state actors do not seem to violate these legal frameworks, as we have discussed above. International law faces challenges in regulating non-state actors, and they are operating in a somewhat legal vacuum while only domestic laws try to bind them to a certain extent.

Such cyber operations can have a severe impact on nation-state relations. The victim states can retaliate in the cyber world or extend to the conventional military retaliation in a legal vacuum. For instance, due to mistaken belief, the victim state conducts a traditional military attack against the host state after a cyber-attack conducted by non-state actors from the host state's territory. This situation may lead to a traditional war between states after just a cyber-crime. Another issue is the escalation of cyber operations to the diplomatic issues between the host state of these operations and targeted states. We have seen a similar situation between Russia and the USA after a recent cyber-attack on US Pipeline.[56]

Here, it becomes more mandatory to stop these actors when they have no obligation to bind themselves with legal regulation under international law. It is essential to create a preventive mechanism that can regulate these operations and helps the international community to prevent further conflict. Another critical issue is the discrimination against the developing or least developed nations who will need resources to get the appropriate information regarding the cyber operation. They would find this challenging due to a lack of technological advancement.

Cyber-attack victims like individuals and nations face challenges the cyber-attack and lack a legal framework to regulate them. The international community must take cyber-attack seriously and show international cooperation to deal with such cyber operations as they have done against the traditional terrorist attack. Although states are actively preparing themselves to deal with such cyber operations domestically, such as in 2009 US created cyber command, India has set up a cyber and information security division. Almost every nation has created such an agency and has some regulatory mechanism to deal with cyber-attacks domestically.

[56] The Print, *how cyberattack on major US pipeline has become a diplomatic issue between US and Russia,* 11 May 2021, https://theprint.in/theprint-essential/how-cyberattack-on-major-us-pipeline-has-become-a-diplomatic-issue-between-us-and-russia/656384/ Accessed Date 8 July 2021.

It becomes essential to have a regulatory mechanism to deal with such operations. Here, we can understand the majorly few factors which push the need for such a legal framework. First, every individual has access to cyberspace and becomes a stakeholder in the cyber-attacks due to the easy accessibility of the cyber world. Also, when there are different and large groups of stakeholders present on the offensive side of these attacks, it becomes mandatory to establish a regulatory and compliance mechanism to deal with such heterogeneous actors in centralized coordination.[57]There must be cooperation and coordination among state actors to effectively deal with such heterogeneous actors, which calls for a specific central legal mechanism in international law.

Second, as we have discussed above, the victim states will not be able to monitor non-state actors residing in another state. This factor of cyber conflict gives a solid argument for having a detailed and obligatory agreement that sets states responsibility, prohibition mechanism, and sanctions on norm-breakers. The rationalist cooperation theory also provides the Importance of such agreements in the same manner.[58] Third, when cyber weapons are widely present and accessible to any individual in the cyber domain. This vulnerability of cyberspace provides another argument for adopting explicit prohibitory norms. The International community has developed a legal framework to deal with other weapons with similar characteristics. Weapons such as chemical or biological weapons were also widely and easily accessible and needed to be regulated by specific international law.[59] Similarly, cyberweapons must also be regulated through international law after a consensus among states.

Although, this is a long process that needs time and cooperation among such heterogeneous actors, which will be challenging. The states dealing with such cyber operations as host or targeted states need to initiate the discussion among the international community to frame specific legal regimes to fill the existing legal vacuum. The most challenging part of such a regime is obtaining consensus among state actors. The "Paris agreement on climate" can be considered an Ideal example and should be followed by the international community. The Paris Agreement aims to achieve the common goal of reducing the rising temperature and bringing it to pre-industrial times. This agreement gave the goal to the countries of reducing the carbon emission to zero by 2030.[60]

The states need to focus on the collective agreement, as cyber operations threaten the world and

[57] EilstrupSangiovanni M, Varieties of Cooperation: Government Networks in International Security, In Miles Kahler (ed), Networked Politics: Agency, Power, and Governance, (1st edn, CornellLQ, 2009).
[58] Koremenos, B., Lipson, C. & Snidal D, The rational design of international institutions (2001) 55 Int organ 761.
[59] Price, R, A genealogy of the chemical weapons taboo, (1995) 4 Int organ 73.
[60] Paris Agreement 2015.

severely impact human life and day-to-day functioning. An unambiguous legal regime needs to be established, like the Paris agreement, which imposes an obligation on all the countries to reduce such cyber-attacks. Also, this regime should establish a system where countries have obligations for achieving the common goal of zero malign cyber activities in the legal vacuum. This governance mechanism should also establish a management system that can deal with all the stakeholders in cyberspace and work to prevent and cooperate among the state actors to deal with cyber operations by non-state actors. It can derive such a system from an existing internet naming management system that deals with states and non-state actors simultaneously on the international front.

VII. CONCLUSION

History teaches us that whenever we need to address problems arising from heterogeneous actors, strong cooperation and central authority are needed to solve that issue. For instance, climate change becomes an issue that has to be resolved through an international coordinated action plan like Paris agreement. When non-state actors become active in the cyber-crime domain, they are considered problematic in cyberspace regulation. Cyberspace regulations should not find their root only in the regulation of states. Cyber-attack by non-state actors affects international borders, and the cyber infrastructure of individual and private entities is also disturbed through such operations. The International community cannot afford to be ignorant of non-state actors who are a significant threat to cyber infrastructure. However, states and other international agencies try to interpret international law, but we have seen that the scope and application of existing international law are limited.

Secure borders are essential in this integrated world where borders have become more complex due to cyber activities across state boundaries. In the covid19 pandemic, humans have shifted to the cyber world, where all activities have become more dependent on digital tools.[61]The pandemic has shown its effects in more than 150 countries, which means a drastic shift to cyberspace for work, human interaction, and other activities.[62] As history has shown us, after the industrial revolution in the mid-nineteenth century, a train of various states went into the future of industrialization and never looked back. Similarly, in the early twenty-first century, a train of progress through the tunnel of cyberinfrastructure again leaving the station, which has been forced to move fast because of the pandemic. In this scenario where users and

[61]World Economic Forum, *why cybersecurity matters more than ever during the coronavirus pandemic*, 20 March 2020, https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/ Accessed date 11 July 2021.
[62]ibid.

 [ISSN 2581-5369]

cyberinfrastructure boarded this train in a hurry, there are chances that the cyber domain and its users will not be able to protect themselves as they were not ready for this shift. In simple words, work-from-home culture will stay with less intensity after the pandemic gets over.[63]Now, cybercriminals pose the challenge and take advantage of such vulnerable situations.

Hence, it is an urgent need for the world to integrate and find common ground for international cooperation and stop cross-border attacks. An effective international governance mechanism will give critical victory over the non-state actors within the expanding cyberspace issues. This mechanism will give countries an advantage in regulating cybercriminals, responding to non-state actors, and increasing resources to deal with such operations. The ongoing war on terror also needs to deal with the cyber arena. The twenty-first century has to be cautioned about cyber terrorism and the fight against cross-border cyber-attacks, which can only be fought with international cooperation rather than individual state efforts. Hence, the state needs to adopt a balanced and sensible approach to address cyber operations by non-state actors. The global defense mechanism needs to be quick to agree to deal with cyber-terrorism sponsored by non-state actors, and they have to make sure that such cyber operations do not occur in a legal vacuum.

*****

[63]BBC, Mickey and Company, *The future of work after Covid*, 18 February 2021, https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19# Accessed Date 11 July 2021.

 [ISSN 2581-5369]