Page 2416 - 2426 **DOI:** *https://doij.org/10.10000/IJLMH.116367*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

State Responsibility on Cyber Attacks: Legal Frame Work and its Implications

SAAISHRI R.[1] AND SUMANTH RAVI[2]

ABSTRACT

The distinction between conventional warfare and clandestine state-sponsored activities has become more hazy in the digital age as cyber strikes have become a pervasive and disruptive type of aggression. The "State Responsibility for Cyber Attacks" within the framework of international law is the topic of hour. Understanding how states are held responsible for their involvement in such operations is of utmost relevance given the frequency and sophistication of

cyber attacks. The need for hour is a thorough analysis of the legal system governing state liability for cyberattacks, which includes international treaties, common international law, and state practise.the complex network of laws and standards that govern this field and deals with the difficulties of linking particular state actors to cyberattacks are to be carefully watched before giving decisions.this article digs in into the practical implementation of state accountability principles through an investigation of well-known case studies and actual instances involving state-sponsored cyber activities. The international community's responses to cyberattacks and efforts to ensure accountability are closely examined, including those of the United Nations and other institution.

Keywords: *state responsibilities, cyber attacks, public international law.*

I. INTRODUCTION

In the framework of cyberattacks, "state responsibility" pertains to a nation-state's liability for actions or activities that take place across its boundaries and result in cyberattacks involving other states, organizations, or people. With an upsurge in the malevolent use of cyber capacity, this idea is an emerging field of international law that has attracted a lot of interest.The necessity for legal help in cyberspace is expanding as the web evolves more and more significant in contemporary society. Internet Crime, theft of information, slander, and cyberattacks on essential systems are just a few of the legal concerns that people, organizations, and nations face. Legal remedy frequently necessitates taking action outside of the state borders because of the cross-frontier nature of communication via the internet.Countries are on the hunt for a

[1] Author is a student at Sastra University, Thirumalaisamudram, Thanjavur, India.
[2] Author is a student at Sastra University, Thirumalaisamudram, Thanjavur, India.

 [ISSN 2581-5369]

workable legal solution to the problems that technological advances have brought forth. The web has an impact on how governments carry out their most basic responsibilities of upholding the health of society and the economy, preserving harmony and security, and upholding the rights of individuals. Internet access is having a greater and stronger impact on nations' obligations to their inhabitants and to one another internationally.The world's legal system continues to argue and evolve around the problem of state responsibility in the light of cybercrime. Stability and security in the cyber domain depend on the principles of international law being made more evident and powerful, especially as the reliance on digital infrastructure increases.

II. WHAT IS STATE RESPONSIBILITY AND ITS BACKGROUND

In laymans term according to international law, states have been given certain rights, which come with obligations. States are responsible for any violations of their own laws as long as the violation can be traced back to the state. When a state violates the boundaries of any other state or breaks a treaty, it is accountable for the infringement of international law. A state is additionally accountable for violations made by its own organizations, as defined by local laws, by organizations and individuals holding official positions, and by individuals functioning within the state's guidelines or control.

These obligations persist even in cases where an organization or person has surpassed its authority. In addition to that, for the individual's private actions also the state is responsible[3].

(A) Background

There are two fundamental sources of tethering international law: treaties and Customary international law. States may collaborate together to establish enforceable but advantageous connections with each other by means and use of treaties Treaties can establish a duty to abstain from specific actions or beneficial obligations. State traditions and the idea that governments have a legal duty to follow them and to conform to that practice.

There is no Law of Cyber with regard to the cyber domain in international law Because cyberspace is still a relatively fresh area to engage in conflicts, States lack significant State practice and opinio juris to support traditional international law and their conduct. Without a formal international agreement or established tradition, governments, researchers, and law scholars and intellectuals implement current international humanitarian law (IHL) to activities on the internet or to the cyber space. Although a lot of challenges encouraged the States have

[3] Bluebook 21st ed. Carter D. Westphal, Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace, 126 PENN St. L. REV. 809 (2022)

 [ISSN 2581-5369]

shortcomings in accountability when it comes to the development of present regulations and their implementation in the cyber domain. States exploiting non-state actors to carry out nefarious online crimes in order to circumvent worldwide accountability for those non-state actors and their behavior is one such gap and the main subject of their activities

(B) What is cyber attack

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device. Any deliberate attempt to gain illicit access to a network, system of computers, or electronic device with a view of stealing, exposing, altering, disabling, or destroying information, apps, or additional assets is known as a cyberattack.

Cyberattacks are carried out by attackers for a range of motives, which include acts of war to minor stealing. To enter the targeted systems without authorization, they use a number of methods, including stealing passwords, psychological manipulation scams, and attacks involving malware, etc. Businesses can be disrupted, damaged, or completely destroyed by attacks from hackers. A breach of information typically costs USD 4.35 million. This price tag covers the expenses of identifying and rectifying the violation, revenue losses and interruptions, as well as the long-term harm to a company's reputation.

(C) Why do cyber attacks happen

Hackers are frequently linked to the threat of cyberterrorism digital warfare, or hacking. Nation-state actors often choose important facilities or government organizations as targets in cyber warfare. For instance, Ukraine as well as Russia have seen an increase in cyberattacks against important organizations since the beginning of the conflict. hackers, might not inflict significant harm on those they are targeting. Rather, they usually make their assaults public in an effort to draw attention to their triggers. Corporate espionage, in which hackers steal intellectual property to obtain an unfair edge over opponents, and vigilante hacking, in which hackers capitalize the system shortcomings to alert others regarding them, are less frequent reasons for cyberattacks. For some, hacking is just a hobby that they enjoy the mental challenge.

III. STATE RESPONSIBILITY IN THE DIGITAL ERA

The fundamental humanitarian goals of the law are still applicable in the age of the virtual world, just as they were hundreds of thousands of years ago, when our distant ancestors first began utilizing laws to structure human civilization. The purpose of the law is to govern the liberties and duties of the people and the institutions they create, whether they be nations,

 [ISSN 2581-5369]

corporations, or organizations. Although science, innovation and technology has developed along with the prolonged existence of human civilization, the fundamentals of the law continues to be in effect. The primary obstacle for implementing relevant legal regulations in the age of the internet is the intense cross-border electronic communications. Everyone agrees that internet access remains as a subject to current global legislation. The principle i[4]n question is outlined in the UN Government Group of Experts (GGE)7 2013 Report and was eventually reinforced in further decisions concerning policy. In the area of human rights, the decisions of the The UN Human Rights Council and the UN General Assembly have reinforced the idea that an individual's online liberties must be equivalent to those they enjoy offline activities. Despite the response to the controversy of whether international law applies to the digital space in the affirmative note, the primary unresolved issue remains on how to put the laws previously in place into practice. Assuring remedies in cyber cases with global components, for illustration, is a significant difficulty. While state governments can employ international public law instruments, people as well as companies can rely on international private law. Both approaches have a long tradition and originated during a time when cross-border interactions were less frequent. They must be investigated and, if necessary, improved in order to offer reasonable justice to the matters relating to individuals and the organizations across the world.

IV. CYBER ATTACK AND LAW APPLICABLE

It is unclear what qualifies as cyberwarfare legally, if it falls under the present International Law of War, or whether or not it has an alternative legal status that calls for application under national laws. Therefore, it is necessary to decide whether attacks via the Internet should be subject to special international criminal law and if it makes sense to define this kind of attack in terms of international treaties. There isn't currently an exhaustive international convention or treaty in place to control cyberattacks. States have therefore been applying standard legal methods: either they have recognized the event as a criminal act and prosecuted it according to local criminal law, or they have recognized it as a foreign attack and responded to it according to the Law of War. The inability to determine whether or not a cyberattack qualifies as a war crime or a violent assault under international law or the Law of War, as well as whether or not the harm or injury caused can be compared to that resulted from an ordinary threat, have led numerous scholars to classify cyberattacks as crimes under domestic legislation. In addition, the Law of Wars requirement that a physical attack by a single nation towards a different be followed in order to exercise the right to use force in self-defense has also been cited.

[4] Cyberattacks in the context of international law enforcement Deymah Alweqyan Department of International Law, School of Law, Kuwait University, Kuwait City, Kuwait

 [ISSN 2581-5369]

Consequently, given their justifications, it may be advantageous to apply domestic criminal laws in cyberattack scenarios.

A few scholars have classified cyberattacks that comply with customary international law. it should be agreed with this viewpoint for a number of explanations. First, applying local laws would hinder the State from utilizing its right to defensive tactics under international law, which is binding on other nations, because attacking a State's facilities may cause just as much harm and injury as an armed attack. Additionally, it is inefficient to apply local criminal law in such a scenario as some States may refuse to extradite or investigate the perpetrators under the laws of a different State, by which neither the criminals nor the nations in question are bound. Third, planning a cyberattack in compliance with the rules of international law would give States legal protection when addressing problems with regard to global relations States can resolve such problems by depending on the equal sovereignty principle between States. Given that cyberattacks are an exceptional type of strike that has the potential to harm another nation as well as traverse state borders, they present more difficulties for law enforcement. Such overseas harm has the potential to endanger the stability of the world, violate the UN Charter, and turn into a global issue that deserves to be handled by global law enforcement instead of responding to domestic law, which might not hold an attacking state accountable globally or have consequences for its citizens. Furthermore, although the decision to classify a cyberattack as a domestic attack as opposed to a worldwide attack can be made based on accountability, demonstrating that the crime originated from a different state either sets the state's obligations under international law or holds the state accountable for the actions of the non-state actors that launched the attack from their own territory, If the perpetrators acted criminally within the state's boundaries, local criminal law will apply as the perpetrators are offenders. thereby, classifying cyberattacks as domestic offenses would make it harder to apply international protections for nations" sovereignty or to engage in a form of passive defense, considered a form of preemptive state protection. This is because states would discover it difficult to rely solely on passive defense to reduce the number of computerized attacks against their critical infrastructure. Notably, a more effective approach would be to classify a cyberattack as an international crime because criminal law has not been able to discourage cyberattacks adequately. For instance, some countries, like China and Russia, have not brought charges against their attackers for cybercrimes against other countries, regardless of whether the perpetrators were present within their own borders or were third parties hired by them.

 [ISSN 2581-5369]

V. INTERNATIONAL LAW AND CYBER ATTACKS

Attacks by hackers represent an unusual type of warfare. Cyberattacks are primarily used to compromise hardware and software, destroy networks, and obstruct communication, including between a nation or an organization.

(A) Cyber attack by state actors

Cyberattacks against various nations, entities, or people that are carried out by authorities or government departments are commonly referred to as state-sponsored cyberattacks, also known as nation-state cyberattacks.

Because these attacks are backed by the enormous assets and capabilities of a nation-state, they are identified by their exceptional level of organization, expertise, and resourcefulness.Since cyberattacks are growing so quickly, it is becoming more difficult to find the countries and terrorist groups that are behind them. Therefore, it is necessary to provide evidence that the aggressor State carried out the attack in order to establish a State's liability. Determining the perpetrator of the cyberattack is one of the challenges in this case. An electronic address that connected a person to the internet in the initial stages of the web was called a unique IP address, and it unmistakably identified the person to whom it was allocated. However, because individuals can now alter their IP addresses and/or the location (such as the country in which the IP address is active), IP addresses are becoming harder and harder to identify. Consequently, As a result, even though an agent is situated in State A, it is still possible for it to launch an attack against State B using an IP address from State C.

For all of these reasons, when a cyberattack reaches the level of an assault with weapons, the attacker State must enable its representative to use passive defenses to target the computer system belonging to another State with the goal of causing enormous harm. This enables the victim the State to exercise its right to protect itself from such an intrusion.

(B) Cyber attacks by non state actors

Cyber Non-State actors are important players in the world we live in because, like states, their conduct may have a big and significant effect on governance, the economy, and international affairs[5].

International companies, hacker organizations, non-governmental organizations, cybercrime associations, media, terrorist groups, trade associations, arranged ethnic communities, lobby

[5] Bluebook 21st ed. Stephen Moore, Cyber Attacks and the Beginnings of an International Cyber Treaty, 39 N.C.J. INT'l L. & COM. REG. 223 (2013).

 [ISSN 2581-5369]

categories, illicit organizations, small companies, and others are examples of non-state actors. There used to be a widespread belief that state actors posed the greatest threat to cybersecurity, even though non-state actors carried out the vast majority of the enormous number of cyberattacks that occur every day. The necessary financial resources to invest in the extensive and protracted work required to develop the cyberattacks that have the potential to seriously disrupt societies overseas could only be raised by states. However, in recent years, states that employ non-state actors in their cyber operations have come to receive an increasing amount of attention as a hybrid type of actor in cyberspace.

How can a state respond or react to non state actor's cyber attacks?

1. The earliest and easiest course of action is to ask a host state to take action against the non-state actor when there is ample evidence that the individual in question is conducting or has carried out a cyberattack from its territory. This state would then, in many cases, take actions to put a conclusion to the malicious activities and stop the non-state actor from doing so in future instances. A request for action may be made at the level of international relations, politics, or assistance with technology. One advantage of pressing a state to take action to stop cyberattacks coming from its borders is that the request is non-accusatory and, as a result, has minimal chance of getting worse.
2. A reasonable course of action would be to support the state in taking effective action against a non-state cyber-predator if the "host" state is willing to take so but is unable to fulfill its obligation. This could be accomplished in two ways: either by initiating a long-term capacity-building procedure to help the nation prevent similar nefarious cyber-activities in the future, or by taking immediate action, such as dispatching some technical or police experts to take a specific act against a non-state actor.
3. A diplomatic objection could be a good option if the "host" state hasn't responded to the demand for help in a way that it is supposed to be capable to, or at all. A courteous statement that can be made both publicly and in confidence can accomplish this. Expelling certain diplomats or other state representatives could reinforce diplomatic protests along with a diplomatic declaration. This type of diplomatic retribution may be somewhat detrimental to the host state's reputation abroad since it indicates that the government is unwilling to take action against hostile non-state actors, which may even give rise to suspicions that the government helps these actors.
4. Legal actions could also be taken to put a conclusion to the non-state actor's malicious cyber activities and to prevent similar actions in the years to come. Indicting the

 [ISSN 2581-5369]

company or individuals engaged makes it very evident to the public that the cyber attackers were successfully located and will be held accountable. However, prosecutions will typically take place at the federal level, for instance, in accordance with federal criminal law. Regretfully, this also suggests that legal actions are frequently of a symbolic character since those who are charged can typically only be taken into custody if they travel to the nation they are charged against (or any ally thereof). Furthermore, the non-state entity responsible for the cyberattack may choose to merely adopt a new identity in order to avoid facing legal consequences. Any public announcement of the state's participation in an enforcement action against a non-state actor may have the effect of "recognizing and humiliating," which may serve to partially discourage future cyberattacks. Legal action against a nation-state that refuses to put an effective stop to the nonstate actor's internationally detrimental conduct could also be taken through the International Criminal Court or the International Court of Justice. However, in most cases, this does not seem like a proportionate or practical course of action.

5. Additionally, the non-state actor and/or the state that is failing to effectively prosecute this individual could be the target of sanctions. One way to apply sanctions is to put the people responsible for the cyberattack on a list of undesirable individuals or make it more difficult for them to travel overseas or transact financial business internationally. Certain business dealings with the country that hosts them, such as the import or export of specific goods or financial services, may be prohibited by economic sanctions aimed at the host state. Sanctions imposed in retaliation (and deterrence) may undoubtedly have an impact, particularly if the sanctioned nation is heavily dependent on prohibited imports and/or exports. To encourage a real behavior change, it ought to constantly become apparent what has to be done to remove the sanctions.

6. Beyond diplomatic channels, an innocent state may invoke the principle of due diligence to launch a countermeasure in response to a widespread cyberattack. The most straightforward course of action is to launch another cyberattack in retaliation. It might make sense to start a cyberattack to compromise the non-state actor's computer network and prevent it from doing more damage. However, the actor could simply accept his defeat, buy fresh computers, and carry on with his nefarious actions. It could be more efficient to break into the machine without causing any damage, to find out how it operates, and to disrupt its operations for as long as possible by repairing the vulnerabilities that the hackers are known to be aimed at as soon as possible.

 [ISSN 2581-5369]

7. The last and most effective course of action is to use conventional military force to retaliate, for instance, by carrying out a proportionate strike against a particular location connected to the non-state actor responsible for the cyberattack or the state from which it originates. A strong signal that cyberattacks are not acceptable could be sent by military retaliation, discouraging any prospective cyberattackers in the near future. However, it also carries the risk of inciting a military reaction from the opposing side, which could begin a risky process of escalation.This diplomatic option appears unlikely to be regarded unless the country engaged is a much weaker state militarily, in which case any escalation would be deemed less dangerous, or unless the cyberattack is more destructive and involves actual physical damage and/or victims.

VI. LEGAL IMPLICATIONS RELATED TO CYBER CRIMES

(A) European convenction on cyber crimes

The European Convention on Cybercrime, which took place in Budapest on November 23, 2001, established the most important strategy for dealing with cybercrime and global cyberlaw. It is among the most significant multilateral agreements addressing the problem of digital evidence and cybercrime. Along with the United States of America, Canada, Japan, and South Africa, it was put together by the Council of Europe. There are four chapters and forty-eight articles in this convention. This Convention is a multilateral agreement on criminal justice that offers states the following:

The legalization of[6] specific online and computer-related behaviors; procedural law pertaining to the investigation of cybercrime and the admissibility of electronic evidence in any criminal case; and cooperation between foreign law enforcement and courts regarding evidence and cybercrime.

(B) The group eight

The Group of Eight (G8) at the Denver Summit of 1997 was primarily concerned with prosecuting high-tech offenders and advancing legislative and technological advancements to combat cybercrimes across international borders. The concepts of international collaboration and harmonization for cybercrime were adopted at the Okinawa Summit 2000 and included in the Okinawa Charter on Global Information the Community. The Group of Eight concurred on the significance and guiding principles for the safety of interactions, the free exchange of

[6] How states could respond to Policy Brief non-state cyber-attackers-clingendale-neatherlands institute of international relations

information, and privacy protection.

(C) Global international efforts by united nations

The UN General Assembly passed the Guidelines Concerning Computerized personal Data Files in 1990 with the intention of taking appropriate precautions to safeguard the files from both man-made and natural threats.

The UN General Assembly has supported a number of resolutions with the same goals in mind: raising awareness of cyber security globally, combating illegal information system misuse, and preventing cybercrime.

- 2020 SolarWinds Cyberattack:

In December 2020, it was found that a highly proficient cyberattack had compromised the popular software SolarWinds Orion, which is used by government agencies and commercial organizations. The attackers—who are thought to be Russian—inserted a backdoor into the program, giving them the ability to access private information from multiple companies. Because it specifically targeted the supply chain and had wide-ranging effects, this attack is noteworthy.

- The 2021 attack on the Colonial Pipeline ransomware:

A ransomware attack was launched against the Colonial Pipeline in May 2021, which provides fuel to the eastern United States. Due to an attack by the DarkSide ransomware gang, Colonial Pipeline was forced to temporarily cease operations. A lack of fuel was brought on by the incident, which also made important facilities more susceptible to cyberattacks.

VII. CONCLUSION

Every year, there is an increase in the number of cyberattacks and significant data leaks. Attackers employ sophisticated strategies, instruments, and tactics, and in certain situations, they have the assistance of the government. Certain attacks have the potential to seriously damage vital infrastructure, endanger human life, and result in previously unheard-of data leaks of sensitive and classified material that could spread widespread chaos. Cyberattacks are not covered by traditional international law or its provisions for attacks against territorial principles. It can be challenging to decide which laws should that apply to cyberattackers as cyberspace and the internet have no restrictions. The issue with cyber conflicts brings up questions about international responsibility, nonstate actors, and aggressor nations. as well as the idea of self-defense. Currently, applying traditional international law alone in cyberwarfare situations is inadequate, and the world community needs to pass legislation that controls and governs

 [ISSN 2581-5369]

cyberwarfare and cyberspace. Furthermore, precise standards ought to be applied globally to Develop the CIL in order to handle the 21st-century cyber challenges.

*****

 [ISSN 2581-5369]