CYBER-SECURITY AND INTERNATIONAL LAW: CHALLENGES IN ATTRIBUTION AND ACCOUNTABILITY

Jyoti Bhakta*

ABSTRACT

The increased frequency and complexity of cyber threats revealed inherent weaknesses in current norms of international law as the governing framework of cyberspace. Since incidents occur in cyberspace, problems are associated with assigning guilt and sanctions to the offender's compromised attempt to maintain international cyber security. However, attribution, that is of the responsible actor, is frequently hindered by technological features like operational deceit and anonymizing technology. At the same time accountability frameworks under international law such as state responsibility and due diligence still lack sufficient basis to deal with cyber-specific issues. Current conceptual models, including the Budapest Convention on Cybercrime and advice from the Tallinn Manual, provide an initial structure[1], but they are not nearly as broadly applicable or authoritative[2]. Attributing responsibility in cyberspace remains one of the significant problems this paper assesses and identifies such cases as the Solar-Winds breach and WannaCry ransomware attack[3]. It further examines possible outcomes such as the formation of a world cyber-attribution organization as well as the formulation of international normative instruments on cyber-security. Through the development of attribution technologies, promoting international cooperation, and improving the legal environment of cyberspace, the global society can improve the legal regulation of Internet space and prevent the use of cyberspace for various conflicts.

Keywords: Cyber-security, Attribution, Accountability, International Law, Cybercrime, Cyber Norms.

*LLM, VIT SCHOOL OF LAW, VELLORE INSTITUTE OF TECHNOLOGY, VIT CHENNAI.

[1] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.

[2] Budapest Convention on Cybercrime, Council of Europe, 2001.

[3] SolarWinds Attack Report, Cybersecurity and Infrastructure Security Agency (CISA), 2021.

1. INTRODUCTION

Today, cyberspace has become a new battleground where new forms of attacks have emerged; therefore, existing and new models of how to manage cyberspace must be created. Cyber threats like cyber war, ransomware attacks, data tampering and cyber espionage have given rise to cyber conflicts which have put the relations of nations at a higher risk and challenging the concept of international law[4]. Even though there are doctrines in international law hence the rules governing cyberspace such as the rule banning the use of force as prescribed in article 2(4) of the UN charter the main problem of identifying the attacker is highly impossible. If offenders cannot be accurately attributed, it is almost impossible for the responsible party to be dealt with[5] and evildoers can continue committing crime knowing they will not be punished. This paper focuses on the main question of the present article, which regards the possibilities of attributing responsibility in cyberspace through the application of international law and analysis of existing measures for holding the culprits of cyber attacks accountable. At the same time, it discusses how cooperation on the international level can be advanced in the field of cyber security and offers avenues on how the governance of cyberspace can be made better in the latter to make cyberspace safer in the future.

2. LITERATURE REVIEW

2.1 Attribution: Issues in Cyberspace

In the context of the cyberspace environment, attribution means the process of determining the author of the cyber incident. The complicating challenge is due to the new dynamics of using digital technologies and basic proxies or third-party architectures. This view is shared with writers like Rid and Buchanan (2015) who observe that while these attacks are common, they include compounded methods that make the forensic processes costly and extensive[6]. Tallinn manual analyzes in detail the applicability of international law to cyber operations and recognizes certain issues in current attribution such as the lack of standard technical framework[7] and differentiation between state conduct and that of non-state actors. It also notes challenges of evidence recovered especially because cyber attacks are international in nature

[4] UN Group of Governmental Experts (UNGGE) Reports on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations, 2015-2021.
[5] Rid, Thomas, and Buchanan, Ben. "Attributing Cyber Attacks." Journal of Strategic Studies, 2015.
[6] Schmitt, Michael N. "Cyber Operations and the Law of Armed Conflict." Cambridge University Press, 2013.
[7] Rid, Thomas, and Buchanan, Ben. "Attributing Cyber Attacks." Journal of Strategic Studies, 2015.

and the assailants are very keen to conceal their acts. Further, Clark through Landau (2020) also views the "false flag", which is a situation where the attacker hides his identity.

2.2 The Role of Accountability Mechanism in International Law

In the context of cyberspace there is especially a need for legal responsibility and its means of implementation. The UN Group of Governmental Experts (UNGGE) specifically considered state responsibility in mitigating cyber adversarial actions from their territory. Nevertheless, as Goodman (2019) highlighted, there is still no legally binding international instrument focusing on cyber security[8]. Current instruments like the Budapest Convention on Cybercrime deal with the criminal aspect of the problem but lack clear reference to state responsibility for cyber incidents. The last sessions in the OEWG have witnessed calls for elaboration of state obligations and measures to address violations thereof.

3. METHODOLOGY

This article uses a research approach whereby primary and secondary data are compared, compiled and analyzed with the use of international treaties, case laws and policies. Real-life examples including the WannaCry Ransomware attack of May 2017[9] and the Solar Winds Cyber-attack in December 2020 are employed to drive home the lessons in attribution and legal lacuna[10]. By analyzing the national cyber security policies from three different countries such as the United States, China and the European Union one is able to identify different approaches towards accountability.

4. RESULTS

4.1 Attribution: A Technical and Legal Problem

The study reveals that accurate attribution of cyber threats entails the applicability of a broad perspective involving technical dimension, intelligence platform as well as diplomatic acumen. From an IP address or through the study of the malware, there may be certain leads, but technical approaches are usually not very helpful[11]. This is made worse by the fact that there is

[8] Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." Atlantic Council, 2012.
[9] SolarWinds Attack Report, Cybersecurity and Infrastructure Security Agency (CISA), 2021.
[10] WannaCry Ransomware Attack Case Study.
[11] UNGGE Reports, United Nations, 2015-2021.

no commonly agreed definition regarding which cyber attack should be attributed. The Solar-Winds attack in 2020 by sources tied to Russia established the potential effect on political relations and support for mutual consensus.

4.2 Accountability Deficits in International Law

The paper points out a major shortcoming in the law in addressing the identification and prosecution of holding states and other non-state actors involved in cyber attacks. Thus, even being bound by the due diligence principle that requires states to prevent actions that are hostile to other states from being made on their territory, enforcement measures are still unsatisfactory. The goals laid down by the UNGGE remain unfulfilled of being transformed into concrete obligations meant to govern responsibly the state's behavior in cyberspace. Furthermore, private entities especially multinational corporations have something to do with cyber security despite the fact that they are not well incorporated in international law.

5. DISCUSSION

5.1 Building Attribution Systems

In an effort to counter the problems of attribution, this article recommends that the United Nations develop an international cyber attribution organization. It would be some kind of an entity that would give impartial and objective measurement in case of cyber attacks, thus, avoiding the problem of political manipulation of accusations[12]. Technologies such as artificial intelligence and blockchain could make improvements to forensic features and transparency, among minor enhancements.

5.2 Accountability in Context: Legal Reforms

One proposal that could sort out the problems could be the formation of a more strict cyber security convention like the Geneva Conventions in which norms and penalties for cyber attacks would be outlined[13]. Specific details of such a treaty might include provisions for state responsibility for stopping cyber operations emanating from its territory, the requirement of states to disclose certain important cyber incidents to an international body and sanctions for non-compliance such as fines or restrictions on technology transfer. Furthermore, it could make

[12] Tallinn Manual 2.0, Cambridge University Press, 2017.
[13] General Data Protection Regulation (GDPR), European Union.

nations use excellent domestic cyber security policies as well as promote international cooperation in forensic examinations. It has suggested that this treaty should contain information concerning state-related responsibility, further investigation assistance, and punishment for the states' breaches. Examples of those undertaking regional measures that can help to create a balance between security and sovereignty are the European Union regulations in the General Data Protection Regulation (GDPR).

5.3 Building Global Partnership

Cybersecurity is an issue of international interest and one which cannot be solved by individual effort. Measures including confidence-building measures like exercises, and exchange of information will go a long way in addressing mistrust. Recognized institutional players such as the states, international organizations, and private actors should embrace an inclusive global cyber norms system that shall support sustainable cyber security governance.

6. LIMITATIONS

One of the few drawbacks of this research is that its information is based solely on the available public data on cyber incidents since many of the factors remain classified or are non-disclosure[14]. The mentioned limitation could be solved in future studies by developing cooperation with governmental agencies and other private cybersecurity-related organizations to get access to the wider dataset[15] and more profound findings. They may also offer a way to lessen the gap between academia and implementation by including case studies and professionals. It also has to be noted that due to constant change, the threats related to cyberspace are highly likely to change, thus making some of the findings irrelevant. Further research relevant to the future of cyber attribution should attempt to build such models, in order to make future predictions accurate and concrete, as well as the investigation of how accountability tools are affected by technologies in their development stages.

7. SUGGESTIONS

The directions of the future cyber security governance will be carried by further development of international legal instruments and norms, innovative technologies and international

[14] UN Group of Governmental Experts (UNGGE), 2015-2021.
[15] Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." Atlantic Council, 2012.

cooperation. In fighting the constantly growing complexity of threats from cyberspace, it is crucial to build treatise international law: norms, obligations, and liability for actions in cyberspace. This will lead to a better organization of the response to cyber incidents as well as better prevention and punishment of offenders. Since attribution is still an issue, then the use of more advanced tools and technologies like artificial intelligence, machine learning, and blockchain all have the potential of helping in identifying the culprit thus delivering improved attributions as well as better handling accountability tools. Independent international cyber security organizations under multilateral systems like, the United Nations could afford neutral reports on cases of cyber terrorism. This would help guarantee that escalation of political tensions hampers the fight against cyber events and provide a level playing ground for assessments. Also relevant is the need to build up national cyber security systems as a response and challenge. Governments have to dedicate efforts and resources to the protection of their cyberspace, to guarantee all parties of the civil society, governmental and non-governmental, the capacity to prevent, detect and react to a potential attack, and to coordinate with international partners, to protect infrastructure.

To facilitate closer cooperation in this regard it is necessary for states and private actors to trust one another. Subsequent initiatives should build on strengthening cooperation between governments and firms so that both entities can address cyber security strategies and measures, as well as the sharing of information and responses to cyber threats. However, what is missing is the ethical and human rights perspective on cyber security to facilitate a sustainable consideration of sovereignty and liberty as vital aspects of national security.

Finally, there clearly exists a paucity of literature to advance better and more complex approaches to cyber attack identification and blaming, particularly where international law is pertinent to the subject of cyber security. Increasing trust-based cooperation with other countries and improving the advertising technological base will significantly reduce the threats of cyber operations and provide stability in the contemporary world.

8. CONCLUSION

In cyberspace, issues of attribution of authorship and, therefore, responsibility contribute to the need to develop strong international legal systems as well as cooperation logistics. Regardless of the existing legal framework, it has to be developed further because of the features of cyber warfare. In other words, by improving the effectiveness of attribution mechanisms, promoting

greater levels of responsibility, as well as engaging international cooperation, thus the world can effectively manage threats of cyber incidents and remain stable in the context of the new world.

REFERENCES

1. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.
2. UN Group of Governmental Experts (UNGGE) Reports on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations, 2015-2021.
3. Rid, Thomas, and Buchanan, Ben. "Attributing Cyber Attacks." Journal of Strategic Studies, 2015.
4. Schmitt, Michael N. "Cyber Operations and the Law of Armed Conflict." Cambridge University Press, 2013.
5. Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." Atlantic Council, 2012.
6. Budapest Convention on Cybercrime, Council of Europe, 2001.
7. SolarWinds Attack Report, Cybersecurity and Infrastructure Security Agency (CISA), 2021.