Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 11, 2239-2245

Attribution Of Cyber Attacks: A Proposed Dispute Resolution Mechanism

Dr. Mian Muhammad Sheraz[1], Dr. Fazli Dayan[2], Sajida Faraz[3], Dr. Muhammad Zubair Khan[4], Ashraf Ali[5]

[1]Assistant Professor, Faculty of Law, Grand Asian University Sialkot, Pakistan. Email Id. Sheeji333@gmail.com
[2]Assistant Professor, Department of Shariah & Law, Islamia College University, Peshawar, Khyber Pakhtunkhwa, Pakistan. Email Id. dayansherpao@gmail.com; dr.dayan@icp.edu.pk
[3]PhD, Scholar, IIU, Islamabad; Lecturer, Law & Shariah, Women University, Swabi, Email Id: sajidafaraz1@gmail.com
[4]Associate Professor, Department of Law, Abdul Wali Khan University, Mardan, Email Id: mzubair@awkum.edu.pk
[5]Associate Professor, Department of Law, Abdul Wali Khan University, Mardan, Email Id: ashrafali@awkum.edu.pk

Abstract

Definitely, technical growth opens up a worldwide technological realm subject to cyber intrusion. Individual safety and confidentiality are intended to be safeguarded by the governments under the legal traditions. Transnational cyber infiltration targeting state entities raises new issues. The subject of whether jus ad bellum is adequate to regulate different cyber intrusions has been widely debated. Similarly, the issue of defining cyber-attacks as armed assaults has been heavily contested. Hence, some argue that the legal norms regulating war are inadequate to cover new types of assaults carried via global internet. Therefore, this article examines the question of cyber warfare from the angle that, when cyber attacks take place? And what possible remedies are available to the victim state? Accordingly, a measure of the remedial mechanism for nations in international law is taken into account based on current circumstances. Since, the existing system of remedies does not address the concerns of governments about cyber activities. Thus, a new possible platform for state remedies is presented.

Keywords: cyber warfare, cyber attacks, technology, remedy

I. Introduction

Cyber warfare[1] is a circumstance in which a nation-state or international organization conducts a cyber-attack or an attack on another nation utilizing computer system software.[2] The goal of this attack is to disrupt or damage the infrastructure through the deployment of computer viruses or denial-of-service attacks.[3] This cyber warfare strike can take many forms, including attacks on the country's or nation's money system, transportation works, security infrastructure, or defence system. Electrical blackouts, failure of military equipment, and breaches of national security agencies are all

possible outcomes of these attacks, as well as distrust in the phone and computer network systems. Since a result, a solution to this problem is critical, as it poses a threat to the country's security system.[4]

Consequently, in this regard, this article will address whether or not minimizing the threat of cyber warfare can be accomplished by a dispute resolution mechanism in the attribution of cyber-attacks, and if not, what suggestions can be made to enhance it?

II. Understanding Cyber Warfare

In the classic definition of war, cyber warfare is a current phenomenon that is difficult to describe.[5] Two or more states engage in an act of collective aggression in order to attain an economic, political, or religious goal that the adversary group might or would otherwise impede. In contemporary warfare, a military's goal is to take out the other side's military andbring it to heel. The cyber-attacks would constitute an assault if they resulted in harm or disruption. Law of war and law of wartime are distinct concepts with their own definitions and interpretations. The legal doctrine known as *jus in bello*, which deals with law in times of war, has its own set of standards for categorizing assaults. Cyber-attacks are now included in the concepts that govern the rules governing armed conflicts (*jus in bello*), making it more difficult to evaluate and implement such laws.[6]

III. Jus ad Bellum and Cyber Warfare

At present, war regulations do not directly include cyber warfare, there are no clear cyber-attack treaties or agreements, and the UN Charter is quiet on the matter. To be sure, the Additional Protocol I to the 1949 Geneva Conventions makes it plain that the rules of international law apply[7], which governs the legality of weapons, would pertain to cyber-attacks as well. However, neither the scope nor the mechanism of application has been specified. This legal ambiguity may allow cyber attacks under the lotus principle, which states that what international law does not forbid, it permits. Thus, we must investigate the applicability of current ideas to both object-based and subject-based cyber-attacks. The jus ad bellum will operate if the assault qualifies as per a given concept or condition. In the lack of direct legislation, the norms will remain ambiguous. In the lack of formal laws or state norms, states have traditionally created new laws or regulatory frameworks to incorporate new arms. Presently, the jus ad bellum is inadequate; an upgrade to bring cyber-attacks within international law is required.[8]

IV. Cyber Attribution System

When cyber-attackers are detected, the issue of attribution to a state arises. Principles and regulations of jus ad bellum may only be implemented if modalities of state accountability are met. As previously said, cyber warfare is not traditional warfare. The assault modes are easier than in traditional combat, allowing for several actors. Even if the assaults are not ascribed to a state, they may be deemed an act of war provided they meet the conditions. However, in order to enforce the state's remedies, the assaults must be linked to a state or a non-state actor. A state's wrongdoing includes international accountability so do state practice and opinion jurists. In the Corfu Channel decision, the ICJ concluded that a state must not allow intentionally its territory to be exploited for conduct detrimental to the interests of other states. The attribution of wrongdoing to a state

may have two dimensions; first: attribution for state activities, and second: attribution for non-state actions.[9]

However, in order to address this, it is required to identify the person or group of people responsible, as well as collect evidence related to the cyber-attack. As a result, cyber attribution is the process of identifying the perpetrators of this cyber warfare crime and gathering proof. So, in this case, cyber attribution is the process through which security analysts gather information, create time lines, and piece together evidence in the aftermath of a cyber-attack in order to determine who is responsible for the cyber security attack.[10] The purpose of this cyber attribution is to obtain answers to issues such as why, how, and when a cyber-attack happened. This is a critical step because, in a world full of criminals and computer networks where hackers have access to vast amounts of information, any small piece of information about the cyber-attack is regarded a step closer to the perpetrators. As a result, cyber attribution is the first stage in resolving a conflict over a cyber warfare strike on a country's security.[11]

V. Dispute Resolution Mechanism: To Resolve the Dispute Related to Cyber Warfare Attack

However, simply collecting evidence in the cyber attribution procedure is insufficient; these evidences must also be kept somewhere, such as in front of an authority, where the matter will be decided using such evidence and applying the applicable laws provisions, and the responsible person will be held liable for his actions. As a result, the legal authority in charge of deciding the dispute will be the Dispute Resolution System.[12] When a cyber attack is related to a nation's security, such as in the form of cyber warfare, it's difficult to find attributions for it, or when the act is not considered wrongful by a nation or state, or when it involves legal or political issues, it's necessary to resolve the matter in a peaceful manner, and this is the situation where dispute resolution system comes into picture. Negotiations, medicines, and conciliation are examples of these dispute resolution systems. Arbitration and the judicial settlement procedure are two further adjudicative methods.[13]

In terms of the technique for peaceful dispute settlement, if the issue is not too serious, it can be resolved with the assistance of domestic authorities. On the other hand, whether the conflict is over a legal or political issue, or something less serious, such as technical challenges, it is resolved by arbitration or judicial settlement courts. The parties appoint the arbitrator, who then decides the case after a comprehensive inquiry. If an outside expert opinion is required, it can be obtained under UN Charter Article 51.[14] In addition, a permanent court of arbitration has been established to resolve the dispute through arbitration. Aside from these, a number of other authorities have been founded in response to various disputes. The International Court of Justice might also be contacted in this situation. If the issue is not resolved, it is referred to the Security Council under Article 37 (1) of the UN Charter. When a member of the United Nations is subjected to an armed attack, the right to self-defence is invoked.[15] This dispute resolution technique is useful, but

in the case of nations, due to a fault with the cyber attribution method or a failure to recognize it as a wrongdoing, nations are unable to reach a decision using the dispute resolution mechanism. Despite the fact that it is a conflict resolution mechanism, the absence of remedies available to the parties and the lack of amicable remedies accessible to nations against any cyber-attack would add to the uncertainty and aggravate the matter. And as a result, international peace and security will be jeopardised. As a result, a prompt, efficient, and relevant solution for all aspects of cyber-attacks must be provided.[16]

With such a serious threat to international peace and security, it is critical to control state behavior in order to provide states with viable options. Hence there are three suggestions to improve these situations as first in the development of the law. In this context, law refers to the development of laws that will solely address the situation of international cyber-attacks or cyber warfare in a larger sense. The key goal of enacting these laws is to ensure that they are strictly enforced, even if it means relying on a peaceful settlement system, because national security is a major priority. Furthermore, as the second recommendation in this cyber warfare situation, an intermediary conflict resolution body that applies current principles to the use of new technology in cyberspace will be crucial in controlling the state reaction to cyber-attacks. The actions of this intermediary entity offering a dispute settlement mechanism will shape customary international law in this area.[17]

VI. Remedies in Cyber Warfare

Even if a state isn't involved, a wrongdoing's legal position remains unchanged. Any remedy, or at least available to one, is required when a state is wronged. A state might not even be able to readily trace an act to another state or may not deem an act to be unjust. These disagreements might be legal or political in nature. The UN Charter requires governments to resolve disputes peacefully. This is well defined by the PCIJ in the "Mavrommatis Palestine Concessions" case[18] as differences over law or fact, legal viewpoints or interests between two people. All state parties may opt to resolve a disagreement amicably, or the UN Security Council might request that they do so. Negotiation, inquiry, mediation, conciliation, arbitration, judicial settlement, or regional agencies or agreements are all peaceful conflict resolution procedures. All peaceful conflict resolution procedures need the cooperation of the respective governments.[19]

A conflict might be about legal or political issues. Negotiations, mediations, good offices, or conciliation are approaches of resolving conflicts via diplomatic offices. Arbitration, judicial settlement, and inquiry are some of the adjudicative processes used to resolve conflicts. The adjudicative procedure may serve as an essential weapon of preventative diplomacy in more complicated situations, says Jennings. When dealing with international cyber-attacks and cyberspace acts, diplomatic offices may help resolve issues that are not difficult factually or legally. However, as previously said, the growing dependence on technology by state actors makes online acts increasingly technical and harder to comprehend. To resolve these conflicts peacefully, governmental actors would need to use investigation, arbitration, or litigation.

VII. Proposing a Dispute Resolution Mechanism

Keeping in mind the previous debate, let us now analyse the remedies available to state "X" if state authorities of state "Z" or other non-state entities functioning transnational acquire control of state "A" vital infrastructure through cyberspace operations. The assaults are carried out using DDoS or other accessible cyber-attack tactics, substantially hurting state X's economy. A different set of CNE assaults compromises the security of both the state X's defensive mechanism. The rapid cyber intrusions threaten state X's economy and defence system. To discover legitimate retaliation against by the state "Z", legal experts must first prove that the assaults constitute armed attacks or international wrongful actions, and second, that perhaps the attacks are due to the state "Z". After the attribution, self-defence methods might be considered.[20]

As previously stated, it is difficult to define such operations as armed assaults. Even if the assaults are armed, they must be ascribed to state "Z". It is a bilateral problem when state "Z" formally acknowledges or accepts responsibility for the assault. In circumstances when state "B" refuses to accept responsibility, an investigation is required. If the UN Security Council adopts a resolution establishing an investigation committee, a special committee will be constituted on a case-by-case basis to investigate.[21] If the actions are attributed to private entities, the cyber crimes statute applies. If the assaults are state-sponsored, the legal possibilities are limited. In these situations, state "X" has no recourse except to take steps of its own will. This might jeopardize global peace and security.

The problems of governmental responsibility for cyber-attacks in whatever form are difficult to address. According to the ICRC, the solution to these problems will presumably be decided only by future state practise.[22] In light of the urgent danger to international peace and security, it is essential to regulate state activity and provide nations with realistic remedies. Thus, state practice would include developing legislation dealing with global cyber-attacks or cyber warfare. Furthermore, the proposed dispute resolution process would generate laws based on the facts of the case and use jus ad bellum norms. The analogical approach is suggested by the wisdom of international law. The norms that emerge from state practice might subsequentlybe incorporated into a framework of customary international law. Because of the varying speed of technical advancement, nations will be reluctant to embrace any structure for cyberspace governance.[23]

The creation of an Arbitration and Enquiry Tribunal for Transnational Cyberspace Operations is the last idea in this regard. It is recommended that an Arbitration and Enquiry Tribunal for Transnational Cyberspace Operations (AETTCO) be established to address transnational cyberspace challenges and the limited remedies available to governments. When it comes to the legality of cyber-attacks, the states are in a state of disarray. There are no precise standards that govern these situations, and the current norms do not eliminate the ambiguity. The founding of AETTCO will aid in the removal of ambiguity and doubt; it will advance state practice on this subject by offering proper remedies; and it will minimize the threat of

cyber warfare to international peace and security.[24]

VIII. Conclusion

Resultantly, after the discussion, it may be determined that cyber warfare is a significant threat for the nation's security, and that it requires immediate attention. It would not be practicable, however, without sufficient facts and authority to make a timely and effective decision. Consequently, the procedure for gathering evidence will be covered in cyber attribution and effective decision-making will only be possible when there are effective authorities and laws in place those focuses solely on cyber-attack-related matters and national security concerns, which cannot be accomplished through a dispute resolution system.

References

1. Mian Muhammad Sheraz, Fazli Dayan, "Cyber Warfare and Protection of Civilian under International Humanitarian Law", EEO 2020; 19(4):7904-7917
2. Mian Muhammad Sheraz, Dr. Fazli Dayan, "The Law of Self-Defence in Cyber Operations", EEO 2021; 20(1):7918-7934
3. Hanna, Katie Terrell, "Cyberwarfare", in "Techtarget Network", 2020; Ibid
4. "What is Cyber Warfare?" in "Fortinet", 2021
5. Thomas Rid, "Cyber War Will Not Take Place", "Journal of Strategic Studies", 35(1):5-32, 2012
6. Dietrich Schindler and Jiri Toman, "Declaration Renouncing the Use, In Time of War, Of Explosive Projectiles under 400 Grammes Weight", In "The Laws of Armed Conflicts", Martins Nijhoff Publisher, Leiden-Boston, 91-93, 2004; See also Op cite note. 1
7. Chris af Jochnick and Roger Normand, "The Legitimation of Violence: A Critical History of the Laws of War", Routledge, 2017; See, Op cite note. 1
8. OHCHR, "Protocol Additional to the Geneva Conventions of 12 August 1949", 2021
9. James A Green, "Cyber Warfare, AMultidisciplinary Analysis", Routledge, London-New York, 2015; Op cite note. 1
10. Shakarian, Paulo, et all, "Cyber attribution: An argumentation-based approach", In "Cyber Warfare", Springer Cham, 151-171, 2015
11. Payne, Christian, Lorraine Finlay. "Addressing obstacles to cyber-attribution: A model based on state response to cyber-attack", "The George Washington International Law Review", 49(3):535-568, 2016-2017
12. Muhammad Asif Khan, "Reducing the Threat of Cyber Warfare through a Suitable Dispute Resolution Mechanism", "Journal of the University of Latvia Law", 13:97-12, 2020
13. Ibid, see also, Op cite note. 1
14. Codification Division Publication, "Repertory of Practice of United Nations Organs 2020, Article 51"
15. "United Nations Charter, Article 37", 2020
16. See, Op cite note. 12 & note. 1
17. Pipyros, Kosmas, et all, "A cyber attack evaluation methodology", In" Proceeding of the 13th European Conference on Cyber Warfare and Security", The University Piraeus, Greece, ACPI "Academic Conferences and Publishing International Limited Reading", UK, 3-4 July, 2014, 264-270
18. Judgment of the "Permanent Court of International Justice Fifth (Ordinary) Session", in the case "Greece vs. Britain"
19. See, Op cite note. 12 & note. 1
20. See, Op cite note. 12 & note. 1

21. Peter Nadin, "UN Security Council Reform", Routledge, London-New York, 112, 2016
22. "Global Red Cross Network", "The Global Red Cross Network The American Red Cross is Part of a Global Network Dedicated to Relieving Human Suffering", 2020
23. Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls", "Global Governance: A Review of Multilateralism and International Organizations", 18(3):339-361, 2012
24. Op cite note. 1, note. 2 & note. 12