Cyber Warfare and Attribution: Exploring the Regulatory Role of International Law

Snikdha Balaji, Vedam Anand Kumar

Sastra Deemed To Be University

Abstract: ***Although not an archaic concept, the ever - unceasingly unfolding concept of cyber warfarenow has the center stage. This paper explores the mutually effectual relationship between international law and the regulation of cyber warfare. Governments that previously built physical borders to preserve their territorial integrity have since forced upon themselves a paradigm shift now fortifying their cyberspaces. The paper addresses the replacement of traditional weaponry and armour, and the expansion of the manifestations of "war", now with interpretations of asymmetry and anonymity. The paper whilst addressing the proliferation of transnational terrorism and the ensuing non - international armed conflicts spiraled into large - scale cyber operations by 'hacktivists', also proportionally deals with the adequacy of several strategies, measures, and studies, such as the Tallinn Manual, which was specifically launched to usher in clarity to the complex legal landscapes surrounding cyber operations, paying specific heed to those issues involving jus ad bellum and the jus in bello and interpreting the extended versions of both the Geneva Law and Hague Law that govern law relating to war. Considering the uncontrollably fast pervasiveness of belligerent activities in the digital realm, the paper places the responsibility on the international community at large to ensure the establishment of norms or suitable adaptation of ratified conventions aimed at regulating cyberspace. In conclusion, the paper seeks to make a substantial contribution to the ongoing discourse on the regulation of cyber warfare.***

Keywords: Cyber warfare, cyber attack, Tallinn Manual, attribution, cyber espionage

1. Introduction

1.1 Background and Rationale

In the contemporaneous era, cyber warfare has befogged the boundaries between traditional warfare and the digital sphere. The impact has been so momentous that, in addition to the conventional domains of land, air, water, and space, military reliance has been placed on what is now known as the fifth domain. This shift in paradigm has seen a drastic overturn from isolated incidents of hacking, exemplified by the Morris Worm (1), mutating into sophisticated state - sponsored cyber attacks, with the Stuxnet Worm (2) being perceived as the oldest in the chronology.

Attribution, which is the process of identifying the source of a cyber attack, has been historically impossible because of the allure for clandestinity and deniability that this dynamic landscape possesses. However, in view of modern developments such as intelligence sharing and digital forensics, the volatile field of cyber - attribution capabilities has been both clarified and obscured. It is in this context that the present predicament and international law collide with its intersection marking a focal point of inquiry.

Despite ongoing regulatory initiatives, such as the Tallinn Manual, which is a non - binding academic study, the international landscape at large remains inadequate. Consequently, international law becomes pivotal in such a nonconformist warfare approach that goes beyond conventional notions of sovereignty in order to stop escalation, improve attribution mechanisms, and most importantly, safeguard vital infrastructure. As cyber threats traverse boundaries of nationality and when normative conceptions of warfare undertake reassessment, such a quandary necessitates a renewed scrutiny of legal frameworks.

1.2 Research Objectives

Explore the Technical and Collaborative Aspects of Cyber Attribution: Examination of technical - natured complexities that highlight attribution challenges and emphasize the requirement for proficiency in cyber forensics, as well as overall technological capabilities. Exploration of cross - national collaboration to deduce optimal strategies.

Analyze the Regulatory Gap: Evaluation of the present frameworks to underscore the lack of comprehensive regulations and assessment of the regulatory void's effect leading to heightened vulnerability and an escalation in cyber threats.

Investigating the Role of International Law: Exploring how international law can standardise and streamline the process involved in attribution by outlining clear protocols and standards. Evaluating the impact of international legal guidelines in directing governments to determine perpetrators of cyber aggression.

Assessing the Tallinn Manual's Addressal of the Challenges: Examine how the Tallinn manual addresses and tackles significant concerns like transnational terrorism in the digital domain, in addition to evaluating the efficacy of the Manual in providing guidance on legal considerations.

1.3 Scope and Limitations

The scope of the research primarily delves into exploring an interdisciplinary subject by pervading into aspects spanning International Law and Cyber Law and analyzing the effectiveness of international legal frameworks in addressing cyber threats. The study researches the transition from physical borders to cyberspaces, as well as the evolution from traditional weaponry to cyber capabilities. The study further looks at the immediate challenges faced in the form of Transnational Terrorism in the cyber form. When it comes to the application of International Law the study analyzes how the Geneva Law and Hague Law are extended to cyber warfare and further looks into the collated Tallinn Manual.

Given the fast - paced changes in cyber technologies and strategies, it is difficult to cope with, frame, enforce, and regulate law. There is also a complexity of legal interpretations conspicuously with International Law given its application and enforceability. Due to sensitivity or lack of data in certain geopolitical conflicts, the research might not provide the exact information and hence would become a limitation in the study.

1.4 Methodology

A dynamic research methodology is essential to support the relationship between international lawand the regulation of cyber warfare. Hence, we try to explore the following methods:

- Literature Review: The first step of research is from understanding the existing scholarship onthe regulation of cyber warfare and its nexus with international law and thus Identify key concepts that have a lacuna.
- Case Studies: Contemporary cases that illustrate instances of cyber warfare and the legal challenges. Analyze these cases to extract the practical application of international law in conflicts that involve cyber warfare.
- Legal Framework Analysis: The International legal frameworks governing War can be categorized into a wide bracket of Geneva Law and Hague Law. Examining the provisions of the existing broad framework would help in culminating the possibility of applying the existing provisions. Further we also look into the Tallinn Manual and assess their adequacy and try to bring in clarity.
- Historical Analysis: Explore the evolution of cyber warfare and the parallel development of international Law and try to provide and highlight a geopolitical approach.
- Synthesis and Integration: Provide a holistic approach by synthesizing the findings from various research methods to construct a comprehensive narrative. Highlight areas of consensus, controversy, and gaps in the existing understanding of the regulation of cyber warfare.

2. Understanding Cyber Warfare

2.1 Definition and Characteristics

Considering how pervasive cyber attacks are a workable definition of the same is critical. Whereas a constrictive definition may allow evasive tactics to escape international war law, one that is too extensive and broad might compromise national interests. It may very well be noted that no universally accepted definition exists. [1]

In the dearth of a uniform definition, attention may be diverted to the U. S Army definition that refers to cyber - attack as the premeditated usage of disruptive activities, or a threat thereof, against computer or networks, with the intention to cause harm or further any social, ideological, religious or political animosity. [2]

The Matthew Waxman propagated school of thought defines cyber warfare as, “efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them. ”. [3]

A point of distinction between cyber - warfare and cyber - crime is pertinent. Whereas the former brings under its purview malicious hacking and defacement aimed at the destruction of civilian or military infrastructures, the latter pertains to fraud/offensive content and is governed by internal national criminal laws.

2.2 Manifestations of Cyber Warfare Attacks

The exhibitions of cyber - attacks as undergone an obtuse evolution in the interconnected digital landscape, with malicious actors employing tactics updated with the technological advancements to exploit vulnerabilities in the cyberspace. In a world that places undue reliance on digital infrastructure, deciphering the manifestations of cyber - attacks is the method to fortify cybersecurity

Denial of Service (DoS) attacks:
Regarded as one of the most prevalent attacks, these are attempts to cause obstruction against access to service. [4]Under such an attack, the attacker resorts to flooding a network with an excessive amount of data requests and information beyond its capability. This overload causes the deceleration of the network causing it to degrade or halt. The consequent result is users being prevented from accessing services such as emails, which are reliant on the affected network.

Distributed Denial of Service (DDoS) attacks:
DDoS attacks are akin to DoS, that empower the attacker to control multiple computer networks, marking its dominance over DoS, by the pre - infection with a virus that effectively hijacks the computer. In 2009, a number of both government and commercial websites were shut down by a series of coordinated DDoS attacks in South Korea and the United States of America, which led to large - scale data compromise. [5]

[1] (Arie J. Schaap (2009) Cyber Warfare Operations: Development and Use Under InternationalLaw, 64 A.F. L. REV. 121, 134

[2]DCSINT Handbook No. 1.02, U.S. Army Training & Doctrine Command, Critical
Infrastructure Threats and Terrorism VII-2 (2006),http://www.fas.org/irp/threat/terrorism/sup2.pdf.)

[3]Matthew C. Waxman (2011), Cyber-Attacks and the Use of Force: Back to the Future ofArticle 2(4), 36 YALE J. INT'L L. 421, 422

[4]Christopher D. DeLuca (2013), The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, 3 No. 9 PACE INT'L L. REV. ONLINE COMPANION 278, 281

[5]Oona A. Hathaway (2012) et al., The Law of Cyber-Attack, 100 CAL. L. REV. 817, 823

Malicious Programs

These programs serve as tools that aid attackers to disrupt normal cyber network functions by infecting the network or taking control of it. The effect of these may occur over a period of time or be immediate. Whereas a virus is a defective computer program with the ability to infiltrate a system by continuous replication causing it to spread, a worm is an independent program that erodes the network's data capabilities without tethering itself. In the year 2000, the "ILOVEYOU" virus caused substantial damages to nearly ten million Windows personal computers causing an estimated $6.7 Billion in damages[6].

Logic Bombs

Logic bomb being an intelligent computer bomb, perches on dormantly in a network, until specific and certain predetermined stipulations are met, after which its malicious capabilities are activated. Owing to its seemingly latent nature, it renders its detection challenging and the effect all the more devastating. The American government[7], during the Cold War, used logic bombs to obliterate a Soviet natural gas pipeline.

Other attacks

Some other cyber weapons include IP spoofing, which redirects users entering a web address that is legitimate to that which is fraudulent through trickery and Trojan horse that is a malicious software that is masquerading as a benign one, deceiving users into granting unauthorized access to a third - party under the pretense of performing a required operation.

2.3 Principle of Attribution

The concept of cyber attribution involves a dual assessment encompassing technical and political dimensions. The technical methodology includes analysis of malware and operational routines linking cyber effect operations to established entities. [8]Political methods are much more closely aligned with intelligence collection and evaluating the role of political decisions.

Attributing cyber - attacks is a completely different process as opposed to regular physical attacks, due to the heightened capability of the malicious actors to resort to veiling themselves behind the promise of anonymity by concealing their identities or engaging in impersonation.

The problem especially arises when policymakers call for targeted attribution that is precise, which is often difficult to deduce and may require complex reverse engineering and intelligence efforts. Despite these apparent challenges, there have been instances of successful cyber attribution such as the Russian involvement in hacking Hilary Clinton's presidential campaign in 2016. [9] This effort only further emphasises the necessity of input from a range of actors and sources to carry out successful attribution.

2.4 Cyber Espionage

Cyberespionage is a modern phenomenon made possible by information and communication technology, and it presents new difficulties. Cyber Espionage campaigns are frequently planned by advanced persistent threats (APTs), who use techniques like spear phishing, social engineering, malware distribution, and watering hole attacks. [10]It is worth noting that insiders in the targeted organisations may also be involved in cyberespionage by unintentionally or purposely revealing private information. Exploits and implants are among the many hacking tools that are readily available online, which has contributed to the growth of cyberespionage.

National and international legal frameworks seek to make it illegal to gain unauthorised access to computer systems and data, intercept communications, and commit other cybercrimes related to espionage. However, obstacles like extradition disputes and spying nations' unwillingness to assist with investigations restrict the effectiveness of legal measures. The complicated relationship between cybersecurity, national interests, and international relations is highlighted by the fact that national indictments against foreign nationals involved in cyberespionage frequently serve diplomatic rather than prosecutorial purposes.

The legitimacy of cyber espionage in international affairs is a topic of debate due to its evolving landscape. Some claim that widespread government actions have made a narrow exception for espionage, while others maintain that it is still up for debate among academics[11]how to distinguish between legal and illegal types of cyber espionage.

3. The Tallinn Manual on the International Law Applicable to Cyber Warfare

In 2011, an International Strategy for Cyberspace was set up by the US under the power of several renowned academics and this was headed by Professor Michael N Schmitt. 'This led to the development of a non - binding document for the State's conduct in cyberspace. The manual did not require a reinvention of customary international law and IHL interpreted them to also apply in cyberspace. ' This came to be known as the Tallinn Manual**.** The manual is Jus In Bello and hence applied only during armed conflicts. The manual had subsequent updates to 2.0 and 3.0 versions in 2017 and 2021 respectively.

The Tallinn Manual's emphasis is strictly on cyber - to - cyber. I. e. a cyber operation against a State's infrastructure or targeting enemy or attacking control systems. The Manual will not delve into kinetic - to - cyber operations, such as a bombing on a cyber operating machine. The Manual

[6]Jason Barkham (2001) , Information Warfare And International Law on the Use ofForce, 34 N.Y.U. J. INT'L L. & POL. 57,62

[7]Wolfgang McGavran (2009), Intended Consequences: Regulating Cyber Attacks, 12 TUL. J. TECH. & INTELL. PROP. 259, 262

[8]Kristen E. Eichensehr (2020), The Law and Politics of Cyberattack Attribution, 67 UCLA LAW REVIEW 520, 582

[9]https://digitallibrary.utah.gov/awweb/awarchive?type =file&item=8353

[10]Shulsky, Abram N. and Schmitt, Gary J. (2002). *Silent Warfare: Understanding the World of Intelligence*).

[11]Gragido, Will, John Pirc, and Russ Rogers. Cybercrime and Espionage: An Analysis of Subversive Multivector Threats. Rockland, MA: Syngress, 2011

addresses both international and non - international armed conflict thus having a wider scope in the ambit of International Humanitarian Law. [12]

The Tallinn Manual contains several rules that are followed by commentaries that were framed by several jurists in concurrence and differences in certain aspects and it brought in several aspects of Geneva Law and Hague Law into its purview and interpreted its applicability to cyberspace. Nevertheless, the manual accepted certain ‘unique attributes of networked technology requiring additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them’. Thus observed the wider scope of Cyberwars implicitly recognizing the necessity of an extended scheme of Laws for governance.

4. Strengthening International Cyber Norms & Enhancing International Cooperation

The United Nations Institute for Disarmament Research (UNIDIR) published a study which reported that thirty - three states have included cyber warfare in their military. They have expanded the number of individuals employed for the work and further set up specialized units. This included 12 of the l5 largest military states.

When it comes to the aspect of framing norms the Russian Federation always vouched for a treaty since the late 1990s, however the United States of America (US) and Western states have taken the position that none is needed. [13]

China, the Russian Federation, Tajikistan, and Uzbekistan proposed an International Information Security Code of Conduct in September 2011 but this had a wider ambit and its focus was not restricted to Warfare. They further adopted the framework of the Shanghai Cooperation Organisation in 2009. [14]This document was observed by India, the Islamic Republic of Iran, Mongolia, and Pakistan. An unofficial English translation of this agreement consists concepts of ‘war’ and ‘weapon’ beyond their traditional meaning in international humanitarian law (IHL**).** [15]

There is also a debate on the applicability of International Humanitarian Law and different standpoints and stances are given by several states on this position. Even Though the US, United Kingdom, Northern Ireland, and Australia, have stated that IHL applies to cyber warfare there is no clarity regarding implications, definitions, and threshold. China also opposes Militarization of cyberspace.

However, the paper would conclude that there is a clear - cut necessity for bringing in a treaty governing cyberwarfare with a wider paradigm when compared with IHL to face the challenges posed by the threat. This is necessary due to the reasons for coping with the growing technology, having a clarity of attribution, protecting the infrastructure that is beyond the scope of Geneva Law and finally setting rules for state behaviour and conduct. This would help maintain stability at the International level, give security, and prevent escalation of conflicts.

5. Conclusion

To conclude, it can be precisely said that this research is a collaborative study of International law in a specific realm of Cyber Warfare. The wide methodologies used in the paper examines the various dilemmas posed due to the paradigm shift from physical borders to cyberspace. The complexities involved in cyber warfare such as anonymity, terrorism, the legal frameworks of the Tallinn Manual, and the ripe necessity of collective efforts from the International community for regulating the digital realm, predominantly form the structure of the research. At length, the research proposes the international community to take the responsibility of establishing conventions to face the challenges posed by cyber warfare and thus envisaging the scope of International Humanitarian Law to adapt itself to stay relevant with the proliferating technology.

[12] Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross

[13] **D**raft resolution submitted by the Russian Federation to the General Assembly First Committee in 1998, letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Secretary-General, UN Doc. A/C.1/53/3, 30 September 1998)

[14] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc. A/66/359 of 14 September 2011 & Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security

[15] http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf