ASSESSING LEGAL FRAMEWORK FOR CYBER ESPIONAGE IN INTERNATIONAL LAW

Nayan Chandra Mishra*

ABSTRACT

This paper analyzes the legal aspects of cyber espionage in international law. It aims to build a framework that can tackle the lacunas in international law for cyberespionage. Through both primary and secondary sources, this paper looks into several arguments both in favor and against cyber espionage to reach a reasonable conclusion.

INTRODUCTION

With the advent of the internet and globalization, the world is interconnected as never before. Cyberspace has grown into a place where millions of different transactions take place every day. Global financial markets have witnessed a tremendous upsurge in the number of transactions and cloud computing has made the recording of data easier and accessible for both the governments and the common masses. This enormous boom in the dot com world has also spurred debate among experts on the security and vulnerability of cyberspace. In recent years, there has been an upsurge in the number of cyberattacks on the governments, businesses, and common people affecting privacy, trade secrets, confidential information, ransom, private data, etc.

In 2018, there were 80,000 cyber-attacks per day (over 30 million attacks per year). 812.67 million Malware infections were recorded in 2018, almost double the figure recorded since 2015(425 million). Every day 230,000 new malware are created and the figure is growing every year. There has been a 350% rise in the cases of ransomware (2018), which is estimated to cost $3 trillion to the world economy by 2021. About 27% (1.2 billion) of the breaches recorded were against the governments. In 2017, the average number of breached records by country was 24,089, with 53% of the breaches caused by cybercriminals.[1] According to the report published by IBM and Ponemon Institute in 2020, the average cost of a single data breach in

*FIRST YEAR, BA LLB, DR. RAM MANOHAR LOHIYA NATIONAL LAW UNIVERSITY, LUCKNOW.

[1] "2021 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends." n.d. Purples <https://purplesec.us/resources/cyber-security-statistics/> accessed January 21, 2022.

the business sector was $3.86 million. Recent cyber-attacks on critical infrastructure, including confidential data of the state and the companies, have led to a spur of debates on the implementation of efficient regulation, not just domestically, but also internationally. For example, a data breach on the Accellio file transfer application affected 100 companies, government agencies, organizations, and universities around the world. Another cyber-attack on the Pulse Secure VPN resulted in the leakage of confidential information of Fortune 500 companies and several undisclosed defense firms and government agencies located in the USA and Europe.

CYBER ESPIONAGE

Cyber espionage is one of the components of cybercrimes. It involves a wide range of issues such as surveillance, stealing confidential data, privacy, subversion, and manipulation. The concept of cyber espionage is not new and is a facet of traditional espionage. But it came to light in the early 2010s when Edward Snowden, former defense contractor of the Central Intelligence Agency, made a monumental revelation concerning the cyber-surveillance by the USA, both on citizens and non-citizens, including heads of several nation-states. It caused a severe shock wave around the world. Since then, the issue has been constantly in the news relating to espionage, hacking, recruitment of terrorists, data breach, privacy, fake news, etc.

Both state and non-state actors can indulge in cyber espionage. In the case of the former, several government departments and agencies play a critical role in the hacking of the system, especially for confidential data or damaging the critical infrastructure of rival states and foreign companies. In the case of the latter, illegal hacking groups, terrorist organizations, state-sponsored organizations, or any individual who can hack can be looked at. A leading and famous instance of digital cyber-attack by any state occurred in 2008-09 when the USA and Israel jointly destroyed the nuclear program of Iran by sending a malware, Stuxnet, into the pen drive of one of the nuclear engineers, leading to overloading and subsequent destruction of centrifuges used for uranium enrichment. Another cyber-attack was orchestrated by Russia on Estonia and Georgia, which came into headlines in 2007 and 2008, respectively. Subsequently, the news of cyber-attacks on critical infrastructure came every year. Recently, in 2021, a cyberattack on the USA's colonial pipeline and the Mumbai power grid made headlines. There are several issues ranging from building better infrastructure to the creation

of a dedicated cybersecurity roadmap that has been in discussion since the early 2000s. But we will hold on to the legal aspects of cyber espionage in the domain of international law.

LEGAL DEFINITION

There is no legal definition of cyber espionage that we can adhere to in figuring out what it means. But for our understanding purposes relating to the subject of our discussion, we can take the following definition - "*Cyber espionage is a process of remotely stealing confidential and sensitive data of the state without its explicit consent using cyberspace*."

The legal aspects of Cyber Espionage are associated with the stealing, processing, and subsequently using the stolen information to affect the rights of an individual and the sovereignty of the state. For instance, when Russia interfered in the US elections by using the citizens' data (through Cambridge Analytica), it endangered the right of individuals to make an independent choice by subverting the consciousness of citizens through fake news. Moreover, it also hurts the sovereignty and authority of the state to conduct free and fair elections. Another example of cyber espionage leading to subversion of people's independent choice was at the time of BREXIT (2016) and the Scottish referendum (2014) when Russia was alleged to use the British citizen's personal information to "selectively affect their choice through fake news on social media.

THE STEPS TAKEN

A crucial step was taken in 2001 when several countries came together and signed the Council of Europe's (Coe) Cybercrime Convention, also known as the Budapest convention on cybercrime. It is the only legally binding multilateral treaty that coordinates cybercrime investigations between nation-states and criminalizes certain cybercrimes. But there are many countries, including India, China, and Russia, that declined to sign the convention on grounds that data sharing with foreign investigative agencies will hurt their sovereignty. Many provisions of the convention do not fit with the domestic policies and laws of several nation-states, thus causing hindrance in cooperation and coordination among them. For instance, Article 32b of the Budapest convention allows for transborder access to data which affects the sovereignty of the state and also domestic laws of several nation-states. Another concern for the state stems from the nature of the treaty. The convention is a criminal justice treaty that does not include state actors, thus leaving a broad cleavage for state-sponsored cybercrimes.

This problem becomes more acute for countries like India that suffer most from state-sponsored cyberattacks. Apart from the Budapest convention, UN Congress on Crime Prevention and Criminal Justice in 1990 (Havana), UN Crime Congresses (in 2005, 2010, and 2015), and annual UN Crime Commissions also subsequently tried to pass a regulation on cybercrimes and cyber surveillance, but given the differences among the states, a consensus could not be reached.

THE ROADMAP TO EFFECTIVE REGULATION

The first and foremost step would be to define what is cyber espionage and under what circumstances it can be regarded as espionage. As we know, the world of cyberspace is very broad and includes several aspects affecting the rights of individuals, companies, states, and even animals! Secondly, there are different types of espionage -political (governments and state), economic (Companies and International financial institutions), and social (citizens and society)- concerning the number of rights of different entities. So how can we solve the problem of definition and circumstances? In this essay, we will narrow down the infinite boundary of cyber espionage and make the issue revolving around the state to understand legal aspects in the international arena.

The next step will be to cover some common factors before taking into account the legal aspects to help us establish the uniformity of the issue across the nations. Some of them are:

1. State Actors
2. Confidential Information
3. Stealing of Information
4. Non-consensual
5. Affecting sovereignty
6. Transmission through cyberspace

Now we can move on to describe whether the act of cyber espionage is a war against the state or is it just indirect meddling in the state's affairs. From the UN Charter, war is used in consonance with the use of force, which cannot be applied to cyber espionage or cyber warfare because there is little or no physical interaction between the states, unlike a war.[2]

[2] "*Chapter VII,* UN Charter", "UN Charter." n.d. Law of War. http://lawofwar.org/u.n.%20charter.htm.

Several conventions indirectly affect the cyber domain in terms of warfare, privacy, human rights, civilian protection, peace agreements, consular and diplomatic conventions, etc. The book was written by Russell Buchan, "Cyber Espionage and International Law"[3], has explicitly mentioned the concept of general international law such as mutual non-intervention, territorial sovereignty, and mutual-non aggression relevant to the arena of cyber espionage. Moreover, he also wrote about the specialized international regimes covering international human rights, diplomatic and consular privilege (Vienna Convention on diplomatic relations[4] and Consular Relations[5]), and the rules of the World Trade Organization in addressing cyber espionage. For example, WTO's Dispute Settlement Body (DSB) exercises its authority according to the WTO's Understanding on Rules and Procedures Governing the Settlement of Disputes, which is entrusted with resolving disputes, including economic cyber espionage, that arises between WTO members and all WTO members are under the DSB's jurisdiction. Another example relates to Vienna conventions on diplomatic and consular relations. Both the conventions provide several legal protections that enable diplomatic missions and consular posts to maintain confidentiality over their information and communications such as "Inviolability of documents and archives of diplomatic missions and consular posts" under Article 24 of VCDR[6] and "inviolability of consular premises" under Article 31(1) of VCCR[7]. We can also identify Cyber espionage through customary international laws and conventions such as the UN charter. Article 2(4) of the Charter specifically bans the use of force against other states by saying, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or any other manner inconsistent with the Purposes of the United Nations." Furthermore, Article 2(1) recognizes the "principle of sovereign equality" among UN members implying the principle of "non-interference" in the internal affairs of the state that may endanger the state's ability to maintain effective control over its territory. But the Charter also allows for certain exceptions to article 2(4) in Article 51 that talks about the "Inherent right of individual or collective self-defense if an armed attack occurs against a member of the United Nations until the Security Council has taken the

[3] Buchan, Russell. 2019. Cyber Espionage and International Law. Oxford; New York: Hart.
[4] "Vienna Convention on Diplomatic Relations, 1961", n.d. Office of Legal Affairs https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf
[5] "Vienna Convention on Consular Relations, 1963", n.d. Office of Legal affairs https://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf
[6] "Vienna Convention on Diplomatic Relations, 1961", n.d. Office of Legal Affairs https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf
[7] "Vienna Convention on Consular Relations, 1963", n.d. Office of Legal affairs https://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf

measures necessary to maintain international peace and security."[8] Taking a liberal interpretation, it certainly inculcates the state's self-defense from a high level of cyber-attack that can lead to armed insurgencies and killings, thus, affecting its sovereignty. But there is a lot of space that has to be filled, especially in the case of cyber espionage because it does not directly lead to the use of force. Regarding that, the International Court of Justice in the Nicaragua vs the USA case (1986) defined, any act, overt or covert, if harms the sovereignty of the state by intermeddling in the internal affairs affecting the territorial integrity and legitimacy of the government is illegal and violates the article 2(1) of the UN charter and international customary law. The judgment gave an impetus to deciding whether only using force by a state can hurt another state's sovereignty or not. While the judgment concluded "organizing or encouraging the organization of irregular forces or armed bands for incursion into the territory of another State" and "participating in acts of civil strife . . . in another State" does make up an impermissible use of force, but at the same time, it also ruled that "the mere supply of funds to the contras . . . does not in itself amount to a use of force", thus, leaving a wide gap in interpreting the fine line of incursion.

The Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by the Independent Group of Experts (IGE) convened by NATO, while analyzing the ICJ judgment, acknowledged the use of cyber espionage as a coercive element, but at the same time, rejected the applicability of other interpretations such as using cyber espionage as a tool of economic and political pressure. The manual's interpretation was just limited to the usage of cyber espionage as a "means" to cause the use of force or armed struggle. It observed that "actions such as disabling cyber security mechanisms to monitor keystrokes would, despite their invasiveness, be unlikely to be seen as a use of force."

USE OF FORCE

Now the question arises whether cyber espionage should only be limited to kinetic or coercive interpretations or include the issues such as privacy, human rights, and surveillance that can have a long-term impact on the state. Ted Koppel, in his book, "Lights out: A Cyberattack, A

[8] "Chapter VII: Article 51 — Charter of the United Nations — Repertory of Practice of United Nations Organs — Codification Division Publications", n.d. United Nations - Office of Legal Affairs https://legal.un.org/repertory/art51.shtml

Nation Unprepared, Surviving the Aftermath"[9], has illustrated how the vulnerability of critical infrastructure can bring chaos into the entire nation. In the book, he described how the archaic American electricity grid can easily be hacked by cybercriminals located anywhere in the world to bring chaos into the most powerful country by simply cutting the electricity in just one state. As mentioned by him, it would take years to just find from where the cyberattack happened, let alone knowing the actual perpetrators. He reiterated the fact that the list of cyberattacks (both state and non-state hackers) is much more than the list of nuclear-powered countries. Now, if we don't have any accused, then how can we identify the culprit? An entire nation can be shut down in just a few days without knowing who the real culprit is. Therefore, it becomes imperative for the international community to define the standards and proper regulation for cybercrimes involving non-usage of force too.

THE CASE FOR DOMESTIC LAWS

Some experts argue that domestic laws penalizing espionage activities are an effective way to tackle this big problem. Many countries have laws that restrict their citizens from using cyberspace for surveillance or stealing of data. Furthermore, Article 38(1) of the Statute of the International Court of Justice (ICJ Statute)[10] also acknowledges those principles of national law that apply to inter-state relations at the level of international law. But the fundamental problem lies in the narrowness of these laws which is individual-centric and does not implicate responsibility of the state and non-state actors.

Another problem in extracting the principle of the illegality of espionage, pointed out by Ella Shoshan is, "issues of inter-state political relations are found within the sphere of International relations and not within municipal law." Therefore, domestic laws cannot be taken into consideration as a principle for international law in the prohibition of cyber espionage. Other reasons stem from the increase in dependence on the internet and its vulnerability in the recent decade. But the laws of many nations are still archaic, thus creating a huge loophole in the Legal system to tackle this problem. Additionally, the spectrum of cyberspace is so diverse that many laws could not inculcate every aspect of cybercrime. Some argue that excessive regulation might affect the growth of the internet and AI-based industry. The problem arises in

[9] Koppel, Ted. 2015. Book Club Kit. Lights out: A Cyberattack, a Nation Unprepared, Surviving the Aftermath. New York, New York: Crown Publishers, an Imprint of the Crown Publishing Group.
[10] Statute of the Court | International Court of Justice https://www.icj-cij.org/en/statute

interpreting what is excessive and what is not. Therefore, the case for domestic laws does not fit in the international scenario.

EXPLORING LEGALITY OF CYBER ESPIONAGE

There are plenty of arguments on both sides but the crack is so wide open, it cannot be filled just by assessing one side of the coin. Here comes the applicability of "the Lotus principle" derived from the judgment of the Permanent Court of International Justice (PCIJ) in 1927, while assessing the legality of cyber espionage. The court said:

"International law governs relations between independent States. The rules of law binding upon States, therefore, emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot, therefore, be presumed."[11] Therefore, in short, if the international law does not prohibit cyber espionage, then it is permissible under international law.[12] Following are the arguments to support the legality of cyber espionage.

ESPIONAGE AS A SELF DEFENCE

Those who favour cyber espionage argue that it is a self-defence tactic of the state. As per Article 51 of the UN Charter, any act in furtherance of self-defense is permissible. But it is only valid at the time of conflict, not peace. Thus, the scope of cyber espionage as self-defense gets contracted. Second, this also gives an excuse to the state for employing the tactic as a move towards "anticipatory self-defense", thus protecting it from the legal framework. Espionage is a legitimate function of the state. Preserving national security and sovereignty is one of the essential functions of the state and cyber espionage is one facet that helps in the furtherance of its function. The argument holds water when it covers the defensive approach, but if the sole motive of espionage is aggression, then it is not permissible.

[11] The Case of the S.S. 'Lotus' (France v Turkey) (Judgment) [1927] PCIJ Rep Series A No 10, 18., https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf
[12] paras 46-47; North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) (Judgment) [1969] ICJ Rep 54, para 77. Cf. the Statute of the ICJ Art 38 on applicable law

Essential functions also come under international custom, which legitimizes the “general practice of the states" as law. For Hart, the development of customary law is a slow process ‘whereby courses of conduct once thought optional become first habitual or usual, and then obligatory’. However, the state can develop it instantaneously without waiting for a long period, provided that the state believes ‘conduct is required by law’. Therefore, if the state proves cyber espionage as an essential function of the state required by law, it can be recognized under the International customary law. But according to Article 38(1)(b) of the ICJ statute, reiterated in the Nicaragua case, two conditions must be fulfilled for any act to become a well-established function: first, the act must lead to generally uniform and consistent state practice. Second, there must be a belief that the action must be permitted under international law – described in the notion of "opinion Juris save necessitates”.[13]

But here is the catch, does the state refer to this activity as its necessary function, and does it acknowledge the cyberattacks/espionage that happened on them or conducted by them? Furthermore, does the state without uniformly accepting a certain phenomenon can make something customary? For example, in “The Moonlight Gaze” cyberattacks in 1989 (by Russia) and the “Titan Rain” incident (by China) several US departments have never been acknowledged by the US government. Other examples include the joint cyber espionage of the US National Security Agency and UK government communications headquarters to tap the communication of other members of the UN Security Council and UN Secretary-general. As mentioned by Ted Koppel in his book, it is highly improbable to find the actual penetrator and it even takes years to identify the real culprit. Therefore, “Official comments providing an opinion Juris on cyber espionage are scarce” and there is “no uniformity in the statements made by the states regarding espionage and its necessity under the law” which is also echoed in the International Law Commission’s “Third Report on Identification of Customary International Law. Thus, it does not fulfill the second condition prescribed above to make cyber espionage an international custom.

[13] See for example: North Sea Continental Shelf (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) (Judgment) [1969] ICJ Rep 54, para 77.

THE WAY AHEAD

When Kai-Fu Lee, in his book AI Superpower: China, Silicon Valley, and the New World Order[14], mentioned that the future is Artificial Intelligence, he also pointed out the importance of its legitimate use for human development. He mentioned several new artificial technologies that will revolutionize human civilization in the future and, at the same time, the increase in "disruptive technologies" at the hand of state and non-state actors will cause a huge problem in the future for the world. Therefore, it becomes more urgent for the countries to address the issues of cyber security to tackle future problems. Apart from that, Author C Forces in his book, "Spies without borders: International Law and Intelligence"[15], emphasized that cyber espionage should not only be limited to the debate of legality or illegality but also the "assessment of the method, locations and other relevant factors of the alleged espionage activities". Thus, the legality of cyber espionage is not just limited to only one aspect, but the overall assessment of cyber threats that a nation can face. In this essay, we tried to cover some aspects of cyber espionage from a legal perspective. The importance of legal provisions is increasing with the technological development happening around the world. The governments must ensure that the rights of the people and the sovereignty of the state are preserved in this age of new technology. Therefore, the need of the hour is that the world needs an international legal mechanism that can holistically and efficiently cover the major, if not all, facets of cyber espionage.

[14] Lee, K. AI Superpower: China, Silicon Valley, and the New World Order. (2018)
[15] Forces C, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 J Nat'l Sec L & Pol'y 179, 181