CYBER ATTACKS: GOVERNANCE, CHALLENGES AND FUTURE

By Shashank Chadda*

ABSTRACT

Cyber Attacks have been a crucial concern for many nations across the globe now. Cyber Attacks or warfare, reflects an image of national concern, wherein, important infrastructures of a country are placed under a threat of information warfare. The basic premise of such attacks is that major infrastructures which have been duly identified in this essay, are dependent on information technology. Pertinent questions of thought arise in mind, how does it takes place? How can it be regulated? Much of the literature on cyber attacks assume that the threat of national infrastructures and vulnerability of information networks are the same, however, the laws governing these two are not the same, which is clearly established in this essay. This essay discusses various scenarios of the Cyber Attacks. The theme of the essay is placed on the governance of cyber attacks under International Law, and reassesses the fundamentals of cyber attacks and attempts to rejuvenate a thought process to be pondered upon this neglected area.

* 2nd Year, National Law Institute University, Bhopal

I. INTRODUCTION

Past years have witnessed a warfare between countries involving in Cyber Attacks, which has raised international concern that an unfriendly or an antagonistic country may launch an attack in the cyber domain on critical infrastructures of a country such as defense system, or telecommunications, etc. One of the major examples is the attack on Estonia in 2007. The cyber attacks in Estonia shut down various national websites, resulting into distress, and even lead to violent protests claiming lives of people.[1] Even small scale exercises involving surveillance can disrupt a country's national or regional system. Modernism has made people and in fact, national governments of countries to rely on the computer based programmes that any hostile damage can be meted out by obstructing its connectivity systems, etc.

The Information Warfare is one of the crucial aspects of such cyber attacks. Definitions and conceptualisation in relation to Information Warfare are too complex to be defined in an unambiguous manner but necessarily entails preserving one's information and informational technology, at the same time, disrupting another's.[2] It may also include, defensive measure taken in response to such situations of exploitation.[3] Any such attacks against a country pregnant with Information Technology raises national concern, and it is a unanimous say that, most of the banking and other economic related activities are regulated by Information Technology.[4]

Information Technology is omnipresent and western countries have devoted years on researching and developing such technology. Increasing connectivity between people across the globe has even prolonged the vulnerability of information networks. [5] Accordingly, there is a host of many problems concerning with both, launching and defending of cyber activities, pertinently relating to state's responsibility to cyber attacks.

---

[1] Golnaz Esfandiari, *Putin Warns Against Belittling War Effort*, RADIO FREE EUROPE, May 9, 2007, *available at* http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-b140457a85d3.html .(last visited, 10 July, 2015).

[2] Herbert Lin, *Policy Consequences and Legal/Ethical Implications of Offensive Information Operations and Cyber Attack, in* NATIONAL ACADS. (2007).

[3] Ibid.

[4] *id.*, NATIONAL RES. COUNCIL, *Cyber Security Today and Tomorrow : Pay Now or Pay Later* (2002).

[5] SYSTEM SECURITY STUDY COMMISSION, *Computers at Risk: Safe Computing at the Information Age.* (1991).

II. CYBER ATTACKS UNDER INTERNATIONAL LAW

What more has been contentious than the nature of Cyber Attacks has been the classification of the Information Warfare and its characteristics. This warfare results in complete upheaval in cyber domain and that too by unconventional means, which result in 'non-combat' deaths.[6] technologically advanced countries and the big powers such as the U.S.A. and the Russia, have theorised Cyber Attacks by drawing an analogy with Nuclear attacks. Since, there is no presence of a comprehensive treaty to cover the varying aspects of cyber attacks, other International Conventions must be given due consideration. Given the hurdles of non-proliferation, what can be said to be the best suited analogy for Information Warfare in International Law? Can the Information Warfare be illegalised by the I.C.J.?[7] As has been mentioned earlier, a new and comprehensive convention is required for redressal of cyber attacks. What follow are implantable suggestions.

Banning or illegalising Cyber Tools in international domain cannot be equated with that of banning biological, or nuclear weapons. This difficulty arises from the complexity that computer based codes that are employed because they are indistinguishable from innocent computer codes.[8] In an extent to ban such weapons, this essay proceeds with cogenerating with treaty systems, that may have been a viable option, pertinently relating to Space Law and the Antarctic Treaty System.

It is relevant here to venture upon the authorities, treaties, etc., for controlling nuclear weapons, for instance, in the year 1994, the United Nations General Assembly submitted a request to the International Court of Justice (hereinafter "the ICJ") to deliver an opinion on the issue of legality of the use of nuclear weapons by hostile countries. [9] The Court was of the opinion that "such use of nuclear weapons shall be detrimental for the International Law as applicable against the armed conflict and in particular reference with International Humanitarian Law".[10] As had already been mentioned, the disastrous effects of the nuclear weapons can be similar to that of a cyber attack and has the potential to overlap

[6] Joyner & Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework,* 38 EUROPEAN JOURNAL OF INTERNATIONAL LAW. 844-45 (2001).

[7] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8).

[8] Herbert Lin, *supra* note 2, at 23.

[9] Charles J. Moxley, Jr., *The Unlawfulness of the Use and Threat of Nuclear Weapons* (2000), *available at*http://www.nuclearweaponslaw.com/Moxley_ILA_wkend.pdf. (last visited, July 22, 2015).

[10] Legality of Nuclear Weapons, *supra* note 7.

the settled mechanism of information technology and could destroy critical domains of national interest.[11]

III. THE LAW AND CYBER ATTACK

Although the term "cyber attack" has become a part of common references, few scholars have aimed to determine its scope that might be governed under a law. This section of the essay deals with an area where a cyber attack fills the gap and becomes an armed conflict under the *jus ad bellum*, which then can be termed as Cyber Warfare.

It is worth mentioning here that at the outset, the present laws on cyber attack and their framework are not apt.[12] Such laws were created in the wake of World War II. One particular challenge is that how to address attacks which don't have an existence in physical realm. The physical consequences related to anything do not occur directly from such attack instead such attacks wave out kinetic attacks, which is why most states have disclaimed the notion that a cyber attack constitutes an armed attack, disclaiming their liability under Article 51 of the U.N. Charter. The fact that such attacks are increasing in numbers, calls out for a need for states to constitute a consensus as to when a cyber attack can be said as an armed attack.[13] We now turn on to the Question of *jus ad bellum*. The best way to conclude on the question as to when does a cyber attack constitute an armed attack is to ponder upon whether a cyber attack results in physical destruction, which may also be referred to as kinetic effect, which is comparable to a conventional armed conflict.

IV. SCENARIOS OF CYBER ATTACKS

A comprehensive examination of the weapons that may be employed by cyber terrorists, on critical systems of a country will help in defining the exact scope of cyber attacks in terms of national security. The most vulnerable infrastructures, for instance,

---

[11] DICKON ROSS, *Electronic Pearl Harbour*, GUARDIAN (LONDON), Feb. 20, 2003.

[12] A Handbook on Navy, Coast Guard, Marine states that "legal analysis of wartime targets may call for references to be made to traditional law of war" Dep't of the Navy, The Commander's Handbook on the Law of Naval Operations, § 8.11.1 (2007). However, some noted scholars argue that "the law of war for military targeting, unnecessary suffering, etc., govern all uses of force, irrespective of the means they employ." Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. J. 391, 425 (2010); *Computer Network Attack and International Law,* 187, 195 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); Major Eric Talbot Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 INTERNATIONAL REVIEW. 1145 (2003) (arguing that no new legal framework is necessary) (arguing that no such separate framework is required for cyber attacks).

[13] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW. 1023, 1042 (2007).

include the power supply and damns which are wholly controlled by information technology. For example, in the United States, the water supply and electric supply is often termed as the most lucrative target for cyber attack. The reason is due to the fact that, around 56000 water supply systems of the U.S. and out of these, eighty-one percent of the water system runs on information technology to serve the residents of the country.[14] This increases the vulnerability of the events of multiplicity of such incidents because of the inter-connection that is involved in the intricate network of technology, that can interrupt the whole mechanism of water supply, for instance. Recently, in June 2013, mobile devices saw attacks involving a program called Android Defender that displays fake alerts in an effort to trick the user into paying for a "full version" of the program. In 2014, more attacks emerged, including Oleg Pliss, an attack on Apple's iCloud that locked victims' phones using the Find My iPhone functionality.[15]

The other one, electricity supply, is also vulnerable. According to a survey,[16] it was found that the power companies are primary targets and that such companies have, once in a while, suffered an attack in their transmission system leading to system failure. However, the Global Information Assurance Task Force had concluded its report by determining that, even after such minor attacks to the power companies, physical interruption still constitutes a major chunk of the disruptions, however, attacks involving electronic infusion of cyber viruses are emerging and may pose threat in coming years.[17]

Further, attacks that leverage social engineering have become increasingly popular, with 67 percent of cyber espionage starting with a phishing e-mail, according to the Verizon 2014 Data Breach Investigations Report.[18]

Disruption of the Aero-Systems is another scenario of cyber attacks. Attacks involving shut down of the signal transmission between the nearest airport and a flight, can seriously cost many lives, which is one of the reasons through which, the hijacking of flights

---

[14] Barton Gellman, *Cyber attacks by al Qaeda feared: Experts: Terrorists at threshold of using Web as deadly tool*, The Washington Post, June 27, 2002

[15] Emerging Cyber Threats Report 2015, Georgia Institute of Technology, Georgia Tech Cyber Security Summit 2014.

[16] Riptech Internet Security Threat Report (2002), *available at* http://www.securitystats.com/reports/RiptechInternet_Security_Threat_Report_vII.20020708.pdf (last visited, July 13, 2015).

[17] Information Assurance Task Force Report (2012), *available at* http://www.aci.net/kalliste/electric.htm (last visited, July 13, 2015).

[18] "2014 Data Breach Investigations Report," Verizon, 22 April 2014, *available at* http://www.verizonenterprise.com/DBIR/2014/ (last visited, 06.04.2016).

take place. However, no country is totally dependent on technological transmission and signal trafficking due to high possibility of cyber threats, due to which, the requirement of an extremely efficient pilot is called for. Airlines and passengers are anyway accustomed to disruptions that may happen due to bad weather, storm, etc., however, there must be a surety that any airline and the Aviation Department of a country must not be totally dependent on internet and technological transmission.

V. LEGAL PRINCIPLES

The U.N. Charter under Article 2(4) provides:

> "member states shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[19]

There is an additional customary international law to complement such prohibition as stipulated in the U.N. Charter, which restrains a state to interfere into the matters of internal affairs of another state. [20] The ICJ has also opined on the field wherein it has held that where an interference takes the form of a usage of any threat or force, it shall be conclusive to implement the customary international law of non-intervention via Article 2(4).[21] However, the general consensus till date has been that the scope of Article 2(4) of the U.N. Charter is limited to armed conflict.[22] Comprehensive discussions of cyber attacks are likely to rejuvenate the debate over the scope of Article 2(4). A decipherable opinion, one may think, is that, the costs that are involved in structuring and excreting out a plan of a conventional armed attack are much more than a cyber attack, and which is why, the countries who are weak in that respect mount cyber attacks over the countries that are technologically advanced. This opinion could have been a part of the debate over the scope of Article 2(4). Wealthier nations may start to focus on giving or arguing for giving a more

[19] U.N. Charter, art. 2, para. 4.

[20] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in accordance with the Charter of the United Nation, G.A. Res. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).

[21] Military and Paramilitary Activities In and Against Nicargua (Nicar v. U.S.), 1986 I.C.J. 14, (June 27), para. 209. ("Acts constituting a breach of the customary principle of non-intervention, will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations.").

[22] Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, *supra* note 12.

liberal interpretive approach to the Article prohibiting coercive use of force by hostile countries.

One must note that Article 2(4) is limited by two exceptions, *firstly,* collective security and *secondly,* self-defense. Article 39 of the U.N. Charter provides:

> "determine the existence of any threat to the peace, breach of the peace, or act of aggression, and to make recommendations, or decide what measures shall be taken (...) to maintain or restore international peace and security."[23]

The aforesaid Article authorises the Security Council of the U.N. to sanction such use of force against other country in retaliation to self-defense.[24] This stance may look politically motivated, however, there is an easy outlook to judge a situation being lawfully collective security measures. Secondly, the Article relating to self-defense under the U.N. Charter i.e. Article 51 states:

> "(...) nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs."[25]

Lawful measures under International Law are hard to be make out, due to the fact that, in an armed conflict, the involving states will claim the disclaimer under Article 51, thereby claiming to have acted in self-defense, which consequently shifts the focus of the debates on factual premises rather than on legal framework. The ICJ has opined further in case of attacks which involve cross border infiltration may be classified as frontier incidents and not armed attacks.[26] However, one may note that even if such attacks constitute as "minor incursions", but this does not in any manner stop the other state to respond and claiming the defence under Article 51 of the U.N. Charter. To this alignment, cyber attacks which cannot be termed as an "armed attack" will still be responded by countermeasures which will then be formulated as cyber attacks.

i. INTERNATIONAL TELECOMMUNICATION LAW

Cyber attacks may involve wires and radio transmissions, which will then be subject to International Telecommunication Law. The International Telecommunication Union of

[23] U.N. Charter, art. 39.
[24] *Id.,* art. 41.
[25] *Id.,* art. 51.
[26] (Nicar. v. U.S.), 1986 ICJ 14, para. 195 (June 27) *supra* note 18.

the United Nations establishes transnational benchmarks and lays down standards for information technology. As stated in its Convention:

> "The purpose and aim of the International Telecommunication Union (hereinafter "the Union") is the preservation of peace and the social and economic development of all countries (...) by means of efficient telecommunications services." [27]

The regulations formulated by the Union apply to cyber attacks that use electromagnetic network. Broadcasting radio between two nations is regulated by the standards of the Union.[28] The Member states may at anytime, snap the network spectrum with any other member state for security purposes.[29] However, such restrictions don't regulate, in their substance, cyber attacks. This is because, these regulations do not expressly talk about cyber attacks and military activities relating to information technology and telecommunications. The Union's regulations does prohibit for harmful interference[30] but it permits the member states for military and paramilitary activates involving telecommunication networks.

ii. INTERNATIONAL SPACE LAW

Cyber attacks could be infiltrated through satellites and the like networking systems, which are an integral part of the routine services of a country, for instance, weather, military purposes, etc. It is relevant to note that the 1967 Outer Space Treaty regulates exploration of outer space but restricts such exploration in case of use of mass destruction tools.[31] Cyber attacks, as has been discussed in various preceding paragraphs , are rarely classified as weapons of mass destruction or physical threat, therefore, it is almost unlikely that the issue of cyber attacks will be covered under the ambit of the Space Law in International Law.

---

[27] Constitution of the International Telecommunications Union, Dec. 22, 1992, *available at* http://itu.int/net/about/basic- texts/index.aspx (last visited, July 20, 2015); International Telecommunications Convention, U.N. Doc. 26559, Nov. 6, 1982.

[28] Constitution of the International Telecommunications Union, *supra* note 24, art. 45.

[29] *Id.,* art. 34.

[30] *Id.,* art. 48.

[31] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205.

VI. COMPREHENSIVE LAW AND RECOMMENDATIONS

Cyber attacks are a potentially advanced and an "emerging" threat for countries at the International level, however, there is no particular law which "specifically" talks or govern cyber attacks. The Law of War (*jus ad bellum*), i.e. to say, the reasons for engaging into a war, by a country, does govern cyber attacks but only to the extent that an attack can be covered under the ambit of "physical attack". Other legal principles only discuss the outer wall of cyber attacks because of the non-analogous nature of cyber attacks with armed conflict. Therefore, this essay now proceeds with recommendations for developing a new and a comprehensive treaty for tackling cyber attacks. A glaring example of such a treaty is Council of Europe Convention on Cybercrime[32] which regulated cyber activities, but only in Europe. The Council of Europe's Convention on Cybercrime was created to address the jurisdictional issues posed by the evolution of the Internet.[33] Its solution was to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cyber criminals.[34]This was effected by successful reorganisation of the existing cyber laws, and to put across a uniform criminal policy for the said purpose. This accomplishment rests on the erstwhile absence of procedural norms, lack of jurisdictions, and ineffective implementation of the inadequate statutes.

Pursuing this, it is submitted that there should be two vital themes of a treaty that should be developed at the International level which can be:

Firstly, Defining cyber attacks related definitions, such as cyber terrorists, information warfare, etc. This definition should also set the standards as to when an attack shall be termed as a cyber attack and when shall it be termed as a attack taking shape of an armed attack. It should be defined to elevate it to a level of a conventional conflict, the proportionality of harm caused and the intensity of the damages that may have been caused due to a cyber attack must also be included in the treaty on cyber attacks. In any resolution at

---

[32] Convention on Cybercrime, *Chart of Signatures and Ratifications*, COUNCIL OF EUROPE, *available at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.(last visited, July 24, 2015).

[33] See Recommendation No. R. (89) 9 Of the Committee of Ministers to Member States on Computer-related Crime, *available at* http://www.cm.coe.int/ta/rec/l989/89r9. htm (Sept. 13, 1989) (last visited, 05.04.2016).

[34] Amalie M. Weber, *The Council of Europe 's Convention on Cybercrime, Article 28,* Berkeley Technology Law Journal Vol. 18 Issue 1, *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1416&context=btlj (last visited, 05.04.2016); *See* William New, "Privacy agenda in 2002 has international flavor," National Journal Technology Daily, January 23, 2002; "Under antiterror law, government can use U.S. standards to nab foreign hackers," AP, November 21, 2001.

the Security Council, the member states must take into consideration that no other member state dissent and there must be a consensus between everyone, to make the provisions effective. One of the major issues in International Law is the variety of opinions, and therefore, to evict every room of ambiguity, it must also provide the standards and methodology for "self-defense", as has been observed in the preceding sections, such ambiguity is often used to cover one's violation under the veil of self-defense.

Secondly, such treaty should lay special emphasis on the negotiation and dispute settlement mechanism along with a co-operative structure wherein member states may join hands to cooperate for collection of evidences, and prosecutions, etc. Such methodology has been followed in the Bribery Convention[35], wherein the convention defines bribery and it integrates all the member states to co-operate for criminalisation and prosecution of bribery.

VII. CONCLUSION

Cyber attacks, on central infrastructures of a country are on the verge of being rampant across the globe. While the intensity of such growth in last few years has been humongous, however, the response received by nations across the globe is not in proportion. The essay has highlighted critical points of cyber attacks and the lack of a comprehensive treaty to tackle such attacks. The nations still rely on embryonic international laws, which are only limited to armed attacks. It is high time that there should be a discussion at an international level between the states furthered by the United Nations, to come up with a treaty, "directly" tackling cyber attacks. This global situation will only be addressed by a global mechanism involving cooperation and commitment.

———

[35] Organisation for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 18, 1997, 37 I.L.M. 1 (1998) [hereinafter "the Convention"].