EQ. CITATION: BNWJ-0720-015

1. Legal Regime Governing Cyber Warfare: Comparative Analysis of Indian and International Legislations

By: K.S. Aravind

Pg. No: 1-14

EQ. CITATION: BNWJ-0720-015

i. Abstract

The world today is going through its second revolution, one involving information technology. All aspects of a person's day to day life involves the use of technology and it is an indisputable fact that information technology has made human life easier. Computers are replacing humans; they have taken over the mundane tasks. Computers are not only common today to assist in the execution of economic and industrial tasks in society, but also to carry out certain roles that rely on human life. This is used not only by people but also by governments to store sensitive information.

Cyberwarfare is a potential weapon waiting to strike at the right opportunity if cyber architecture is not well defended. It is the fifth and latest area of warfare after ground, water, air, and space. Any states have shown these aspects of cybercrime, along with militant groups, and have shown their technological capabilities. The usage of computer technology by terrorist organizations and individuals may be described as cyberterrorism to achieve their objectives. This involves usage of IT for the coordination and execution of attacks on networks, operating systems and telecommunications infrastructure, and the sharing of intelligence and cyber threats. The laws governing cyberspace as of now is in the developing stage if we look at international laws. The major issue we face when looking at laws relating to cyber warfare in international law is that most of the law has not been revised to accommodate cyber warfare. It does not conform to the usual norms of war and hence we can only make connections by pondering on the same. This research paper will be analyzing current laws that deal with cyber warfare in Internationally as well as in India.

EQ. CITATION: BNWJ-0720-015

Table of Contents

EQ. CITATION: BNWJ-0720-015

ii. Introduction

The world today is going through its second revolution, one involving information technology. All aspects of a person's day to day life involves the use of technology and it is an indisputable fact that information technology has made human life easier. Computers are replacing humans; they have taken over the mundane tasks. Computers are used not only extensively to assist in the execution of industrial and economic functions in society, but also to perform other functions that rely on human life itself. It is used to store confidential material by not just individuals but also governments.

Cyberwarfare is a potential weapon waiting to strike at the right opportunity if the cyber architecture is not well defended. It is the fifth and new domain of warfare after land, sea, air, and space. Some countries, along with terrorist outfits, have already demonstrated these facets of cybercrimes, displaying their cyber prowess. "*The cyber terrorism can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This may include the use of information technology to organize and execute attacks against networks, computer systems, and telecommunications infrastructure, and to exchange information and perform electronic threat*".[1] The laws governing cyberspace as of now are also in the developing stage, if we look at international laws, it can be seen that it has not been revised to address this new form of terrorism. The only applicable laws are the respective national laws of each country. If we look to India, IT Act,2000, and the upcoming Data Privacy Bill though does not directly address cyber warfare is a potential counter against the same.

iii. Research Methodology

The methodology to be used to meet the objectives of this research would be preliminarily doctrinal and will be based on various research papers, articles, and books by the academicians. The research paper has been divided into chapters. Chapter I will be dealing with the Introduction of what cyber Warfare is. Chapter II will focus on different cyber warfare related

[1]P. Madhava Soma Sundaram, K. Jaishankar, *Cyber Terrorism: Problems, Perspectives, and Prescription*, Manonmaniam Sundaranar University, India

EQ. CITATION: BNWJ-0720-015

International legal provisions and Chapter III will deal with Indian law concerning Cyber-attacks and suggestions.

iv. Research Object

To analyze whether there are sufficient legal provisions in International Law as well as Indian Law to counter or control the ever-increasing cyberattacks which are developing into cyber warfare and terrorism.

v. Research Hypothesis

Even though there has been an increase in cyberattacks between nations or by non-state actors against nation and the concept of cyber warfare and cyber terrorism has been recognized, there is no proper legislation to govern the same either in International Law or Indian Law.

Chapter I: Cyber Warfare

Cyberwarfare is the use of cyberspace to conduct or instigate a war. Internet development has demonstrated that the cyber-space platform is being exploited by people, countries, and organizations alike to attack governments across the world and terrorize civilians. Here the word ‘war’ cannot be construed in its common meaning of armed conflict but two or more groups using the cyberspace to “attack” each other. The major question that rises with term Cyber Warfare itself is that what laws will apply regarding the same as at a glance it has nothing to do with the traditional definition of “war” but still a link can be made with the use of ‘force’ under international law. Cyberwar has been given many definitions, one of the most used one

is by cybersecurity expert Richard A Clarke "*actions by a nation-state to penetrate another nation's computers or networks to cause damage or disruption*."[2]

Cyberwarfare also includes Cyber Terrorism. Cyber-terrorism is the convergence of terrorism and cyber-space. "*The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives through the exploitation of systems deployed by the target*"[3]

Around the world, different forms of cyber-attacks are taking place by one nation against another this can be seen in the attack of Iran in 2010 by a computer worm known as STUXNET which put the whole nuclear power plant to stop. The next example is of the massive distributive denial of service also known as DDOS in Burma which made the internet service standstill.[4]

Cyber Warfare always constitutes a cyber-attack and cybercrime while it is not vice versa. This covers attacks in the sense of an ongoing armed conflict that compromise the operation of a computer network for the object of political or national security, infringe criminal law (e.g. war crimes), and have been committed through a computer system or network. Secondly, this covers attacks that generate results similar to traditional armed attacks, disrupt the operati on of a computer network for political or national security purposes, and are infringements of criminal law conducted through a computer system or network.

I.I. Types of Cyber Attacks

The computer infrastructure attacks or techniques can be classified into three:

a. Physical Attack: Computer infrastructure with standard techniques is destroyed.

---

[2] As Cited in: Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, *The Law of Cyber-Attack,* California Law Review, Vol. 100, No. 4 (August 2012), pp. 817-885 https://www.jstor.org/stable/23249823 Accessed: 04-10-2019 13:14 UTC

[3] ICFAI Journal o f Cyber Law (2002).

[4] BBC NEWS (Nov 4, 2010), *Burma Hit by Massive Net Attack Ahead of Election*, https://www.bbc.com/news/technology-11693214

b. Syntactic Attack: Computer infrastructures are destroyed by changing the system's logic to delay or render the system unpredictable computer viruses and trojans are used in this type of attacks.

c. Semantic Attack: This is more damaging where the user 's confidence in the system is taken advantage of. During this assault, the information keyed in the program is changed without the awareness of a user when accessing and exiting the network.

I.II. Some common attacks used in cyber warfare:

1. Distributive denial of service attack: This type of attack has been the most common kind of cyber-attack in recent years. These attacks involve a computer network being hijacked by worms or viruses and shutting down the whole network. In many a case this will be just an inconvenience but in the DDOS attack on the republic of Estonia in 2007 saw the emergency line for ambulance and fire force rendered useless for an hour, this may have life-threatening consequences.

2. Misinformation: This is a form of semantic attack where inaccurate information is planted by another party in the victim computer network. This makes the computer appear normal even though it has been compromised making the whole situation more dangerous. These attacks are especially dangerous in the current era where heavy reliance is given to information received in computer networks for military purposes. One such example can be how in Syria, the radars were fed with wrong information of clear skies which allowed Israeli planes to land.[5]

Both of these are done through infiltrating a secured computer network.

[5] As Cited in: Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, *The Law of Cyber-Attack,* California Law Review, Vol. 100, No. 4 (August 2012), pp. 817-885 https://www.jstor.org/stable/23249823 Accessed: 04-10-2019 13:14 UTC

Chapter II: International Laws and Cyber Warfare

The major issue we face when looking at laws relating to cyber warfare in international law is that most of the law has not been revised to accommodate cyber warfare. It does not conform to the usual norms of war and hence we can only make connections by pondering on the same. "*We conclude that while the law of war provides useful guidelines for addressing some of the most dangerous forms of cyber-attack, the law of war framework ultimately addresses only a small slice of the full range of cyber-attack*."[6] The Geneva Convention has been last revised during World War II and it doesn't deal with attacks that don't cause direct physical damage. It is still deliberated upon by scholars whether cyber warfare falls under the ambit of "armed conflict" or not.

II.I. Jus ad Bellum and Jus in Bellum

UN Charter Article 2 states all members of the UN should refrain from the threat or use of force against the territorial or political integrity of a state or any other manner that does not conform to UN's purposes.[7]

The exact nature of the global risk or use of force prohibition has been the subject of intense international and academic discussion scholars have argued that Article 2(4) specifically forbids the use of armed force as well as political and economic exploitation or coercion but it is widely accepted that it only covers armed conflict.[8] This raises the question of whether cyber-attack can be considered as "force" or "armed attack" and the means for the same can be considered as a "weapon". A weapon may be construed to include anything used to gain a tactical, strategic, material, or mental advantage over an adversary or enemy target. If we go by this definition usage of worm, viruses or any other means can be considered as a weapon as it gives an advantage over another nation, hence can be considered as an armed attack.

---

[6] Ibid
[7] U.N. Charter art. 2, "*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 in any other manner inconsistent with the Purposes of the United Nations*."
[8] Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter,* Computer Network Attack, and International law 73, 80-82

"Most cyber-attacks, such as halting automated production systems or "blinding" the radar and air defense of another country, do not include direct damage, harm, or death. On the other hand, they can be considered highly inflammatory and dangerous, and thus contrary to the aims of the UN Charter to preserve international peace and security. It is a separate matter whether they constitute an "armed attack" and whether a state can use force against the same."[9]This attracts Article 51 of the UN charter which allows for the right to self-defense. These all come into picture only if any cyber-attack is taken as a "force".

In the end, the researcher suggests taking an effect-based approach when it comes to Cyberattack. If the cyber-attack has caused such an effect that has result in civilian causalities or a serious compromising of the security of a nation. It should be considered as an act of war and the technical means used should be considered as a weapon. While minor incidents can be compared with the ICJ decision with respect to armed use of force where it can be considered as frontier incidents instead of an armed attack.[10]

In response to a cyber-attack, the use of armed force by a government must not only be compliant with U.N. The use of armed force is forbidden by the Charter and customary international law, but in compliance with customary international law, it must also comply with the standards of necessity and proportionality. The rule of necessity demands that violence should only be used as a last resort.

Proportionality expands this principle, banning violence if the total extent and strength of the force in relation to the real or imminent danger of the state is unreasonable. The United State s has acknowledged that these principles apply to cyber-attack military responses."[11]

If a war breakout, the attacking nations should follow the rules of war of distinction between military and civilians. The attack must not affect civilian life by the law of war but when it comes to cyber-warfare no precise targeting can be ensured. Moreover, the nation should be sure the state they are attacking is the one that made the cyber-attack as in many a case it may just appear it originated from the state while it did not.

---

[9] Ziyad Hayatli, *Cyber Warfare in International Law*, http://newjurist.com/cyber-warfare-in-international-law.html.

[10] "*It indicated that cross-border incursions that are minor in their "scale and effects" may be classified as mere "frontier incident[s]" rather than "armed attacks."* Charles J. Dunlap Jr, Military and Paramilitary Activities in and Against Nicaragua, *Perspectives for Cyber Strategists on Law for Cyberwar.*

[11] Ibid.

II.II. Others

These laws are the general concept of governing war other than that when it comes to the law that directly regulates cybercrimes and attacks there are only the laws drafted by the council of Europe. The 2001 Council of Europe Convention on Cybercrime ("Cybercrime Convention") promoted "General criminal policy with a view to protecting society from cybercrime," mainly through legislation and international cooperation which was ratified by the US . The laws are mainly against illegal access, data, and system interference but the same is not made applicable to the government, this shows that the law has been made keeping in mind the necessity of cyber-attacks. For these reasons, only a portion of the overall threat is addressed by the Convention the most established international legal structure specifically governing cyber-attacks. In general, it is limited both by its inability to control the majority of state parties ' attacks and by its predominantly regional membership. Nevertheless, it offers a starting point for the creation of a robust global regulatory framework.

Chapter III: Cyber Warfare and India

III.I. India’s Position

For the past several years, India has been pushing over digitalization. In many public sectors such as Income Tax, Passport Service, Bank, Visa, etc., India began using information technology in terms of e-governance. It should be practiced by industries such as police and judiciary. The travel industry also relies heavily on this. Total computerization has also been introduced to the concept of e-commerce in this field.

India has both strengths in cyberspace, a specific online identity, and a relatively high Internet user base (estimated at over 400 million), but also peer-to-peer drawbacks, lack of infrastructure, and weak Internet speeds. L As other developing countries, India's cyberspace issues represent both the 'pull' of economic growth (the advantage of free data flow) and the 'pressure' of national security (the problem of ever-increasing cyber-attacks). This makes India

a legitimate representative to shape the new cyber norms and their global governance. According to the United Nations survey, India ranks 23rd among 165 nations in the Cyber Security Index and is placed in the class of 'maturing'.

In the year 2018 India had nearly 6.9 lakh cyber-attacks from US, Russia, China, and the Netherlands, According to a lawyer at the Supreme Court and leading cyber law expert Pavan Duggal, while the risk of cyber-attacks remains "imminent," the country lacks the cyber army's institutional framework to counter the threat. He also said cyber warfare is not protected by Indian cyber laws as a phenomenon. India has seen a growing number of cyber assaults over the past few years.

III.II. Challenges to India's National Security

Most discourses about cyber terrorism in India are inspired by the US-launched 'Global War Against Terrorism' campaigns. The Critical Information Infrastructure is very vulnerable in India.

China can be considered as the greatest threat to India's National Security due to its proximity and its sweeping technology in Cyber Warfare. China has an openly declared Cyber Warfare Strategy and Hacker army for the same following military code. These also have a task-oriented structure, which means that in particular, multiple groups and professional individuals work against different goals." The opponents associated with this problem are successful because for extended periods they can preserve a presence on a targeted network. The Chinese have an advanced ability to attack the network of the opponent that could seriously threaten the national and another network-dependent civil operation of that country, and India is not an exception to this.

III.III. Case Studies

1. In 1998, the Bhabha Atomic Research Center (BARC) website at Trombay was hacked. The attacker obtained access to the computer network of the BARC and

collected digital information

2. Numerous prominent Indian websites were defaced in 2002, particularly that of Mumbai's Cyber Crime Investigation Cell.
3. The new computer hacking incident is "Ghostnet." This was a massive digital surveillance campaign from China that breached computers and stole information from hundreds of government and private offices throughout the globe, including those from the U.S. Indian embassy, Dalai Lama offices, and Tibetan refugee centers.

III.IV. Legal Provisions

In India, the Indian Parliament has passed its Information Technology Act, 2000 followed by Amendments in 2006 and 2008 and Information Technology (Intermediaries guidelines) Rules, 2011to rectify the loopholes in the previous law. The IT Act covers punishment and fine in the areas of e-commerce, e-governance, e-banking, and cybercrime enforcement.

The provisions provided are in Section 66F which lists out Cyber Warfare as well as distributed among different crimes in the Information Technology Act,2000. Cyber Warfare in the end falls under the umbrella of cybercrime. From the instances earlier it can be seen that most cyber terrorism attack involves Denial of service, Data stealing, or alteration. This falls under the sections of Cyber Crime against property. The sections governing under the same are:

Section 66F,[12] deals with punishment for Cyber terrorism and it has listed out three major actions as cyber terrorism:

i. Denial of Service Attack
ii. Accessing or attempting to enter computer resource without authentication
iii. Introducing Contaminant.

According to the section, these acts have to be done with a motive to threaten the sovereignty, security, integrity, and unity or to cause fear in people. This section according to the researcher's opinion has covered the main possible action that can result from a cyber-terrorist attack, the problem with section though is that it is vague and can be used arbitrarily. This vagueness is beneficial also if we look it from a national security perspective as a wide range

[12] 66F. Punishment for cyber terrorism, Information Technology Act, 2000.

of attacks can be put under the term of Cyber Warfare as it one way or another falls under the three categories given. The concept of "intention" should be present can be a buffer to the potential arbitrariness of the section. If the acts were done without intention to affect the mass, then it may not attract this section and will fall under the different crimes given under IPC and IT Act 2000.

Cyberwarfare can also be caused by implanting misinformation which can result in certain acts that may cause death, affecting life or affecting the relationship of one country with another. Even though data stealing is covered under this section, Data alteration is not expressly covered by the same. This may be connected to Section 66C which covers punishment for identity theft. Where a password, electronic signature, or any other unique identification of another person is used dishonestly or fraudulently, Misinformation can be sent by stealing the identity of a person in power and then using the identity to misuse the power to give wrong information. Hence a provision should be put for greater punishment is identity theft is used for cyber terrorism activities.

In R.K. Dalmia v Delhi Administration,[13] "The Supreme Court holds that, in the I.P.C, the word ' property' is used in a much broader sense than the expression ' movable property.' There is no valid reason to limit the meaning of the word "property" strictly to mobile property when used without qualification. Whether the offense given in a specific section of the IPC can be applied with reference to any specific type of property, by this case IPC also will be attracted to the stealing of Data, as Data may also be considered as a property.

Chapter IV: Conclusion

Cyber Warfare even though the term has become common, it can be seen that there is no common international law to govern the same. The laws that present especially with regard to the law of war have not been revised to accommodate this new emerging type of war. As cyber-attacks don't have any direct effect it becomes difficult to accommodate them in "armed attack" or "force" under international law. But it can be seen that if an effect-based approach is used

[13] AIR 1962 SC 1821.

to determine a cyberattack, it is easier to accommodate them in the ambit of international law. Depending on the graveness of the effect it may be viewed as unauthorized use of force. Cyberwarfare is also governed by the principles of war Jus ad Bellum and Jus in Bellum. The only international law that directly deals with the cyberattacks is the council of Europe. The others are either in discussion or no treaty has been formed for the same. Hence when it comes to international law, it can be concluded that there is still a vacancy for proper cyber-attack legal framework, and this can be established only through revising the UN charter and Geneva Convention to accommodate Cyber Warfare.

For the past few years, India has been developing as an IT frontier and with more than millions of network users, India is especially susceptible to Cyber Attack. IT Act 2000 governs all the cyber-related crimes in India and by amendment the act has included 66F which gives punishment for Cyber Terrorism. Though Cyber Warfare has not been expressly mentioned, this section can be used to cover Cyber warfare also as the three components that are punishable under the section are what happens during cyber-attack by another nation also. These are Denial of Service Attack, Accessing, or attempting to enter computer resources without authentication, Introducing Contaminant. Still much stronger laws are required which directly addresses the issue of Cyber-attack by another nation.

It is concluded that it is imperative not just for India but for the whole world to make a proper legislation to govern the various cyberattacks of large scale like Cyber Terrorism and Cyber Warfare to understand when to retaliate and when not to as well as to develop an effective mechanism or treaty to prevent the same as in the end the civilians are the ones who suffer.