ISSN No:-2456-2165

Threshold for the use of Force in Cyberspace – Position in India

Pratishtha Majumdar

Abstract:- The concept of cyber warfare, cyber crimes, use of force and cognate issues are evolving and open to sundry discussions and further criticisms. The terms have not been defined in a way that could be adopted internationally but have been interpreted by various experts on the basis of certain categories like intention and gravity.

The concept of use of force is partly clear as per some provisions mentioned in the UN Charter and other Manuals, but when do cyber crimes enter the ambit of use of force is still obscure.

The paper examines the Tallinn Manual in detail as to its operations in the cyber space, the various criticisms made and its applicability around the world, especially India. Special focus has been given to the Indian scenario, which is not very good in terms of cyber activities. Suggestions have been made to ameliorate the same and how the things could be dealt with.

The paper is going to deal with the contemporary issues of Cyber crime, cyber warfare and use of force in detail. It will also discuss whether cyber warfare is a use of force and some concepts embodied in the Tallinn Manual which deals with cyber conflicts.

I. INTRODUCTION TO THE TOPIC

Cyber warfare is a virtual conflict on an enemy's computer and information systems. These attacks are intended to incapacitate financial and organizational systems by glomming or altering the data to undermine networks, websites and services. Cyber warfare is a component of Cyber attack and is considered as a cyber crime. Cyber-crime can be defined as "any crime that is facilitated or committed using a computer, network, or hardware device." It is defined by its means— that is, a computer system or network and are generally committed by individuals, not states.

Use of force is a controversial issue and an undetermined topic. The United Nations Charter has a provision that controls the use of force by member states.

Cyber attacks constitute to use of force. Wingfield mentions, 'It should be immaterial whether a power transmission sub-station is destroyed by a 2000-lb bomb or by a line of malicious code inserted into the sub-station's master control program because the amount of damage is equivalent.'The Tallinn Manual is a non-binding study expounding how international law (especially *the jus ad bellum* and *jus in bello*) applies to cyber conflicts. The focus of the Manual is on the most destructive cyber operations that qualify as 'armed attacks' and also allow the states to respond in self-defense.

II. CYBER WARFARE : ITS DEFINITION, PROVISIONS AND EXAMPLES

- *What is Cyber Warfare ?*

Cyber warfare (also known as cyber war), waged via the internet, is a conflict between two states initiated to attack on an enemy's online data. The motive is to disable every possible system by purloining or altering the data in websites.

In other words, it is the activity of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies which in result can destabilize financial systems, the telephone system and the energy grid. Hence, it is the utilization of computers and other devices to attack an enemy's information systems.

Cyber warfare, rudimentally, involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service (DoS) attacks.

The term "cyber warfare", in itself, is a war of words and has got no proper definition that could be adopted internationally.

- Richard A.Clarke has defined it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".
- Martin Libicki defines the term by its types, namely: strategic and operational. Strategic being "a campaign of cyber attacks one entity carries out on another", while operational cyber warfare "involves the use of cyber attacks on the other side's military in the context of a physical war."

Other definitions include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.

There is no licit definition of the term and this was made evident on June 12, 2015, when the U.S. Department of Defense released the Law of War Manual (LOWM). It covers all topics pertaining to wartime actions (such as classes of persons and their treatment under the laws of war, conduct of hostilities, weapons, prisoners of war, naval warfare, air and space warfare, etc.), as well as explains "war as a legal

ISSN No:-2456-2165

concept." The LOWM has discussed "war" and includes a section entitled 'Cyber Operations' but the terms "cyber war" or "Cyber warfare" have not been used anywhere in the Manual. The DoD states : "precisely how the law of war applies to cyber operations is not well-settled ..."

Through LOWM defines "cyberspace" as *"a global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."* [1]

However the LOWM fails to explain what kind of war-like acts in cyberspace can come under cyber war. The LOWM further recognizes that aspects of cyberspace are likely to develop in future.

The Tallinn Manual on The International Law Applicable to Cyber Warfare also does not define "cyber war" or "cyber warfare." And neither has any provision to deal with these areas.

In Cyber Espionage or Cyber War, International Law, Domestic Law, and Self-Protective Measures, Professor Christopher S. Yoo explains "the threshold determination for the applicability of *jus ad bellum* (right to war) and *jus in bello* (limits to acceptable wartime conduct) in cyber war. Yoo has analyzed the applicability of the concepts of cyber operations, in particular as applied in the Tallinn Manual. Yoo has also reviewed what kind of cyber actions that the international community would limpidly recognize as uses of force, though the concept is said to cover "all conduct that rises to the level of armed attack and acts that injure or kill persons or damage or ravage objects."

III. WHAT IS CYBER CRIME

The computers through internet have grown in importance and their abuse has given birth to new ambit and a series of new age crimes that have been recognized by the Information Technology Act, 2000.

Cybercrime (denoted as 'computer crime') is, fundamentally, the use of a computer as an instrument to further illicit ends, such as committing fraud, stealing identities, trafficking in child pornography, violating privacy, intellectual property issues etc.

The main distinction between cybercrime and traditional criminal activity is the use of the digital computer, but technology alone is insufficient to deal with the realms of criminal activity.

Mainly, cybercrime is an attack on individual, corporation, or government related information and today in the digital age our virtual identities are essential making the centrality of networked computers in our lives very paramount.

An important feature of cyber crime is its non-local character which means that actions can occur in various jurisdictions which further leads to various quandaries for the enforcement of law since, at the present scenario, local crimes also require international cooperation. Ergo, the Internet offers criminals multiple hiding places in the real world as well as in the network, however, cyber criminals, despite of their best efforts, fail to hide clues which as a result pave way to their location and identity.

IV. IS CYBER CRIME AN ACT OF CYBER WARFARE

New technologies engender new criminal opportunities, like cyber crime and cyber warfare, but Cyber war should not be befuddled with the terrorist use of cyberspace/ cyber espionage/ cybercrime even though similar tactics are used in all the types of activities. Some states that have engaged in cyber war may also have engaged in disruptive activities such as cyber espionage, but such activities in themselves do not constitute cyber war.

The difference between the two can be understood as :

Cyber crimes are Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm their reputation or to cause somatic or noetic harm to them using modern telecommunication networks which includes traffic in child pornography and intellectual property, stealing identity, or breaching someone's privacy.

Whereas Cyber warfare refer to politically motivated attacks that may eradicate data or even cause physical damage to infrastructure of a specific country, for example the cyber attacks against Estonia and Georgia that took place in 2007.

For example, when country A conducts a targeted attack against several companies in country B, does it count as cyber war, or cybercrime? The answer depends on the intent.

Cyber war, as Raimund Genes also said in his 2013 predictions, refers to politically motivated attacks that may destroy data or cause severe physical damage to infrastructure of the intended country. Hence, it can be concluded that if the goal of the attack is to destroy the companies' data or their infrastructure with a political intent, it may be considered an act of cyber war.

However, if the attack is conducted to steal information from the companies with a pure financial intent, then it should be considered a form of cyber crime.

ISSN No:-2456-2165

The cyber crime schemes have now transmuted from affecting individuals to finding bigger and better target in companies.

A clear overlap between the two can be discerned (i.e. gathering of information) though the cessation goals are different. For example, obtaining internal information in order to gain money is the goal of cybercrime, but in cyber war, the same scheme can be just part of reconnaissance for a bigger operation. Hence, the structures, techniques and implements used can be the same, but the ending can be entirely different.

V. USE OF FORCE

The principle of use of force has an international customary law recognition.

Article 2(4) of the UN Charter prohibits the threat or use of force and calls on all members to respect the sovereignty, territorial integrity and political independence of other States. It states that : "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."

The rule embodied in Article 2(4) is a formal treaty obligation and has been ratified by all the members, although the states may withdraw their consent to be bound by the treaty obligations, but may not simply walk away from them. Scholars have interpreted this article to be banning the use of force as in "territorial integrity or political independence of states". Chapter VII of the Security Council embodies "self defence" as an exception to the rule and Article 51 states that, "Nothing in the present Charter shall impair the inherent right to individual or collective self-defense if an armed attack occurs against a state."

The major development in international law is the prohibition of use of threat together with the use of force itself, "threat or danger from aggression" is prohibited by the League of Nations Council as well (Article 10).

VI. IS CYBER WAR A USE OF FORCE

Introduction

Cyber warfare acts as a novel weapon that has the potential to alter the way state and non-state actors conduct modern war. The unique nature of the threat and the ability for cyber war practitioners to inflict injury, death, and physical destruction via cyberspace strains traditional definitions of the use of force.

Whether cyber warfare constitutes a use of force giving rise to the right of self-defense raises an significant question in international law. Modern law on the use of force is predicated on article 2(4) of the United Nations Charter ; however, the precise definition of what constitutes the use of force is unclear. Analysis of the acceptability under the *jus ad bellum*, the body of international law governing the use of force as an instrument of national policy, of cyber warfare centers on the Charter's prohibition of the use of force in Article 2(4), its Chapter VII security scheme, the inherent right to self-defense codified in article 51, and customary international law as established by the behavior of states. The application of use of force in cyberspace is not always obvious and many questions emanate on how international law relates to cyber warfare. After a brief look at the history of cyber warfare, this comment initially seeks to answer a threshold question: what constitutes a use of force in cyberspace ? Conclusions express that cyber warfare will require either an expansion of the application of the article 2(4) definition of the use of force or the development of new means of addressing the threat.

Cyber warfare and International Law on the Use of Force

When a state conducts cyber warfare, the question arises that whether the cyber attacks, both offensive and retaliatory, constituted a wrongful use of force, or threat thereof, in contravention with international law. In order to define cyber warfare adequately, the international community must take into consideration the penumbra of the Charter, specifically Article 2(4) regulating the use of force, and Article 51, which outlines the right of self-defense.

A precise definition of what constitutes the use of force is unclear, though some of the parameters are well-defined. For instance, conventional weapons attacks are included within the ambit of article 2(4). Cyber attacks are intended to directly cause physical damage to tangible property or injury or death to human beings and they can be characterized as a use of armed force and, therefore, encompassed in the prohibition. The dilemma lies in classifying cyber attacks that do not cause physical damage, or do so indirectly, vis-á-vis the proscription on the use of force.

Two exceptions to the prohibition on the use of force have been mentioned in the Charter: Security Council action pursuant to article 42, and individual or collective self-defense under article 51. There have been disagreements on the current state of customary international law as it relates to the use of force in self-defense and the proper interpretation of article 51.

As defined by Daniel Webster in the *Caroline case*, this point in time occurs when the "necessity of that self defense is instant, overwhelming and leaving no choice of means, and no moment for deliberation." Under the *jus ad bellum* paradigm, a state response to an armed attack must meet.

Three conditions to qualify as self-defense

- necessity,
- proportionality, and
- immediacy.

ISSN No:-2456-2165

To fulfill the principle of necessity the state must attribute the attack to a source, characterize the intent of the attack, and conclude that the state must use force in response. The principle of proportionality requires that the use of force in the response be proportional to the original attack. The requisite of immediacy prohibits a response from occurring after enormous time has passed. For immediacy, no requirement exists for defensive action to be exercised.

To address the unique nature of cyber warfare, international law should afford protection for states who initiate attack in respect of good-faith, thus acting in cyber self-defense. State survival may depend on an immediate and truculent response; consequently international law should not impose an inflexible requirement on states to fully appease the traditional necessity requirements when acting in self-defense of vital state interests. The law should evolve to apperceive a state's inherent right to self-defense in response to a cyber attack, especially when the attack targets critical national infrastructure. So basically, States can use force in self defence, as well as in good faith, as and when needed.

The proposals for solving the question of cyber operations and the threshold of force may be divided to three main approaches:

- effects based,
- target based, and
- instrument based

The instrument-based approach acts as the determining factor

A cyber operation may qualify as force if the weapon used sufficiently resembles the conventionally used ones. The target-based approach treats any operation targeting critical infrastructure as an armed attack (and thus, also, as force). The effects-based approach uses the overall effects of the operation as the determining factor. None of these approaches is without issues, but the most prevalent of the approaches seems to be the effects-based one, also adopted by the Tallinn Manual.

VII. THE TALLINN MANUAL

The Tallinn Manual (originally entitled, Tallinn Manual on the International Law Applicable to Cyber Warfare) is a non-binding study and a comprehensive analysis on how international law (especially, the jus ad bellum jus in bello) applies to cyber conflicts and cyber warfare. The drafting of the Tallinn Manual 2.0 was facilitated by the NATO Cooperative Cyber Defense Centre of Excellence. The Tallinn Manual research is led by Michael Schmitt.

The focus of the original Tallinn Manual was on the most rigorous cyber operations that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict. Tallinn Manual 2.0 adds a legal analysis of the most common and prevailing cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict.

"Tallinn Manual 2.0 adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict." [2]

Tallinn, "*covers a full spectrum of international law applicable to cyber operations ranging from peacetime legal regimes to the law of armed conflict, covering a wide array of international law principles and regimes that regulate events in cyberspace. Some pertain to general international law, such as the principle of sovereignty and the various bases for the exercise of jurisdiction. The law of state responsibility, which includes the legal standards for attribution, is examined at length. Additionally, numerous specialized regimes of international law, including human rights law, air and space law, the law of the sea, and diplomatic and consular law, are examined in the context of cyber operations.*"

Due to lack of a proper definition of the term "use of force", the International Group of Experts have offered a list of eight indicative criteria that States will take into account to test whether a particular cyber operation has reached the use of force threshold. These factors include severity, directness, military character, etc. The majority of International Group of Experts contended that countermeasures may not involve the threat or use of force, thereby agreeing with Article 50(1)(a) of the Articles. A minority of the experts said that a limited degree of military force in countermeasures is permissible once the use of force threshold has been crossed so long as they are proportionate.[3]

VIII. CRITICISMS

While there are many reasons that indicate that the Tallinn Manual is a well-drafted document worthy of international recognition, there are some concerns with the Manual's contents that will confound legal scholars and policymakers.

- The definition of cyber-attack in the manual has been criticized for its narrow understanding. The manual fails to clarify the implications of attacks that cause harm, impair functionality without causing physical damage and target physical infrastructure that relies on computer systems. The question arises about the difference between cyber warfare and lawful self defense. It is also difficult to 'attribute' wrongful acts. Nicaragua case that decided issues of attribution and state responsibility to cyberspace is uncertain over its applicability.

[2] https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

[3] ICJ's Oil Platform Judgment

ISSN No:-2456-2165

- There is no regulation in cyberspace due to the absence of an international cyberspace law or a cyber security treaty. As a result, the Tallinn manual has been criticized for being premature and undesirable when no universally acceptable cyber security norms exist.

- The manual is non-empirical. There are no laws mentioned and only lists the conclusion of group of experts. The Manual is a collection of ninety-five case holdings with explanations and consists no survey of the evidence.

- The Manual does tread upon contentious issues but doesnot resolve them. The opinions of the group of experts are worthless for scholars and researchers. The Manual speaks in terms of "some," "many," or "all" when referencing the Group of Experts' opinions on various issues.
- The Manual reads as if unsure of its audience. Rule Thirteen leaves the reader with as many questions as a first-year law student leaving a complex contracts class. In this regard, the Manual seems to be less of a Manual and more of a treatise, a voluminous work that sets out roughly crafted rules that need revision and refinement.
- The question whether a cyber operation of a non-destructive nature that doesnot cause extensive negative consequence can reach the armed attack threshold is left unanswered in the Manual.

In short, the Manual should have incorporated some guiding principles for practitioners based on the international law. Customary international law remains unclear & there is no useful norm at all, like there is nothing different or unique about the situations posed by cyber warfare. The very reason the Tallinn Manual should exist is to guide governments and organizations like NATO in a new world of warfare. Thus, if there ever was a chance to show what an ideal law should look like, drafting the Tallinn Manual was that chance. But the Manual is hesitant and conservative.

IX. APPLICABILITY OF TALLINN MANUAL IN INDIA

It is not difficult to visualize a scenario of cyber attacks against the critical infrastructures of the smart cities that are run by ICT and technology. Such a cyber attack can disable or deform the entire smart city if properly executed. Critical infrastructure protection in India is still at its beginning. The national cyber security policy of India 2013 is also quite weak and has not been implemented by the Indian government, along with The Cyber Security Policy of India 2015 which remains missing. Other cyber projects like National Cyber Coordination Centre (NCCC) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, Grid Security Expert System (GSES) of India, National Counter Terrorism Centre (NCTC) of India, Cyber Attacks Crisis Management Plan of India, Crisis Management Plan Of India For Cyber Attacks And Cyber Terrorism, Cyber Command For Armed Forces Of India, Tri Service Cyber Command for Armed Forces of India, Central Monitoring System (CMS) Project of India, National Intelligence Grid (Natgrid) Project of India, Internet Spy System Network And Traffic Analysis System (NETRA) of India, Crime and Criminal Tracking Network and Systems (CCTNS) Project of India, etc have still not been implemented successfully by Indian government There is a lack of well settled and globally acceptable international legal rules and regulations that could deal with international issues of cyber attacks and govern relationship between various countries and on the other hand, taking about India, a tenacious cyber security infrastructure of India is need of the hour. It becomes important to resolve such issues by various government and non government stakeholders. The cyber security related projects in India must be accelerated and successfully implemented as anon as possible.

X. SUGGESTIONS

Though India is lagging behind the technological firepower, yet it can be the pioneer of the cyberspace diplomacy. Rules of engagement on the Internet by governments and non-state actors are yet to be articulated. The strategic environment in cyberspace is highly volatile. Currently, the only source of international guidelines on "cyber warfare" is the Tallinn Manual but it does not focus on the difficulties in attributing cyber attack to a state. Questions such as what constitutes an "attack" have been evaluated on the basis of certain parameters. For instance, the Tallinn Manual does not classify the gathering of information by hacking into a database as an attack, but as an act of "espionage", although the damage could potentially be irreversible.

There is a dire need for a code of conduct in cyberspace, and India has suggested three modest ways:

- First, a country should host an international conference to build on, and replace, the Tallinn Manual with a binding treaty on the law of cyber warfare. Participating states can include technical experts, businesses, and academia in their delegations.

- Second, the country must think of having international courts (with the jurisdiction to try both state and non-state actors) to prosecute transnational cyber crimes.

- Last, the Indian government should make attempts to create an international data protection law which would facilitate quick information-sharing with MNCs which do not host domestic servers. New Delhi has suggested this recently in the annual session of the UN Commission on Science and Technology for Development in Geneva. India's Internet diplomacy will be keenly watched.

India currently has some great agencies which are performing cyber operations like the National Technical Research Organization, the National Intelligence Grid, and the National Information Board, and many others along with the ministries who perform governance functions. The Ministries of Defense, Home, External Affairs and IT should be part of a policy wing and India's intelligence agencies should separately provide their consolidated inputs to aid the operations of the NCSA.

India must work to involve the development of software which would be specially designed to intrude, intercept and exploit digital networks. The deployment of cyber weapons is not a low-cost affair. India's cyber command should be the primary agency, responsible for the creation and deployment of such weapons, which would also have political or parliamentary oversight and must be guided and supervised by a legal framework.

The truth is, a fully operational cyber command will take years to complete, though it is the need of the hour. India is an active participant in the discussions of Tallinn Manual. At the discussion in the UN forum, India should underline the basic premise that it is impossible to impede all cyber attacks. Secondly, the government should draft recruitment guidelines to hire and train the cyber specialists. Magnetizing such officers may require high pay scales and other benefits but they would bring in India's best minds. If India's cyberspace has built-in vulnerabilities, it also has a highly skilled IT workforce, which should be harnessed by the regime for strategic use.

XI. CONCLUSION

Cyber warfare, basically, is an attack on a government by another, via hackers with a warlike intention. It takes place through penetration of another nation's computers or networks for causing damage or disruption.

The exclusive right of using force is given only in the UN Security Council and nothing impairs the inherent right of individual and collective self-defense in case of an armed attack against any member state of the UN until the Security Council takes the necessary measures for restoring international peace and security. Regional organizations like NATO, OSCE, etc. must be mandated by the UN Security Council for the use of force.

The U.N. Charter was indited before the internet existed and, therefore, there are various challenges relating to cyber warfare and use of force. Talking of applicability in India, there is a little predicament in determining as to how Indian government would ensure cyber security of smart cities. The challenges in cyberspace with special regard to cyber security would increase in future and India must be cyber prepared for it. India needs a dedicated cyber security law keeping in mind the contemporary cyber threats. The awareness for the need of such laws and regulations relating cyber security must be improved so that various stakeholders can contribute to the growth and implementation of cyber security initiatives by the Indian government.

REFERENCES

Web sources :

[1]. http://searchsecurity.techtarget.com/definition/cyberwarfare

[2]. https://www.scmagazineuk.com/tallinn-cyber-warfare-manual-20-refines-definition-of-cyber-warfare/article/637924/

[3]. https://www.forbes.com/sites/adp/2018/02/16/why-social-media-should-be-part-of-recruiting-but-just-a-part/#726af1d05ca1

[4]. https://www.techopedia.com/definition/13600/cyberwarfare

[5]. https://www.businessinsider.in/What-constitutes-a-act-of-cyber-war-One-senator-wants-to-figure-that-out/articleshow/52787937.cms

[6]. https://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare/

[7]. https://law.yale.edu/system/files/documents/pdf/cglc/LawOfCyberAttack.pdf

[8]. https://en.wikipedia.org/wiki/Cyberwarfare#Definition

[9]. https://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/2/#4da0742a5a93

[10]. http://perry4law.co.in/cyber_security/?p=77

[11]. http://www.thehindu.com/opinion/columns/stepping-up-to-cyberspace/article7342980.ece

[12]. http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece

[13]. https://www.lawfareblog.com/warning-about-tallinn-20-…-whatever-it-says

[14]. https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=3849&context=clevstlrev

[15]. https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/