LEGALFOXES LAW TIMES

APPLICATION OF PRINCIPLES OF INTERNATIONAL HUMANITARIAN LAW IN A CYBER-WARFARE

BY SAHANA S AND ANUROOPA D

CHAPTER 1

1. INTRODUCTION:

International Humanitarian law (IHL) or earlier known as law of War, governs the armed conflict and the conduct of hostilities. International Humanitarian Law is derived from customary law as well as conventional laws like Hague regulations. There were series of conventions passed with regard to conduct of hostilities and treatment of sick and wounded and these conventions were later replaced by Four Geneva Conventions. The Geneva Conventions dealt with the protection of sick & wounded, prisoners of War, shipwrecked people and civilians. The main objective of the Geneva Convention is to ensure humane treatment of persons not engaged in armed conflict by distinguishing the combatants and the civilians. Two additional protocols to the Geneva Conventions, 1949, which mainly reflected customary rules, were adopted in 1977.

Under International Law, use of force against any State is prohibited[1] unless if it is for self-defense[2] or if there is any threat to peace and it is necessary to resort to use of force[3]. The situation of armed conflict involving use of force is governed by principles like conduct of hostilities and law enforcement. The conduct of hostilities is derived from International Humanitarian Law. In other words, International Humanitarian Law is a set of rules which govern the armed conflict being international or non- international in character.

Cyber-warfare refers to cyber operations constituting an armed conflict. Cyber-operation, which involves development and dispatch of the computer code from one or more computers to target

[1]UN Charter, Article 2(4)
[2]Id, Article 51
[3]Id, Article 39

computers, can be aimed at either infiltrated a computer system to collect, export, destroy, encrypt data, tripper alter or otherwise manipulate processes. [4]Application of International Humanitarian Law in a cyber-warfare will be discussed further in the paper.

2. RESEARCH QUESTIONS:

- Whether the principles of International Humanitarian Law are applicable to cyber-warfare?
- What are the issues pertaining to application of International Humanitarian Law in a cyber-warfare?

3. SCOPE AND SIGNIFICANCE OF THE STUDY:

The paper seeks to analyze the issues pertaining to the application of International Humanitarian Law in a cyber-conflict. It also discusses the aspect of cyber-warfare constituting an armed conflict under the law. It is significant to address this issue since cyber-warfare and cyber-terrorism is a pressing concern. All laws require reforms according to the societal changes and technological advancements. The Geneva Conventions were reforms made to address the lacunas that existed in pervious Conventions. Similarly it is important to address modern means and methods of warfare like cyber-warfare to avoid ambiguity.

4. RESEARCH METHODOLOGY:

The researcher had followed doctrinal method to accomplish the project. The paper is more of a theoretical research. Primary sources like the statute as well as secondary sources like articles and websites have been relied upon for accomplishment of this paper.

CHAPTER 2:

5. CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW:

The International humanitarian law applies to an armed conflict. The issue raised recently is whether cyber-attack falls within the ambit of armed conflict.

The condition precedent for an application of principles of International humanitarian law to cyber operations is existence of an armed conflict. The Geneva Conventions of 1949 shall apply

[4] Cordula Droege (2012), Get off my cloud: Cyber-warfare, International Humanitarian Law, and the protection of civilians, International Review of the Red Cross, Volume 94, Number 886, P. 533, 538.

to all the cases of declared war or any armed conflict arising between high contracting States even if state of war is not recognized by one of them.[5] Prior to the implementation of Geneva Conventions, the law of war applies only on the existence of a state of legal war. But this rule was changed and the common article 2 applies even if the state of war is not recognized. The ICTY opined that an armed conflict exists when there is a resort to armed forces between the States.[6]

There are two types of armed conflicts under International Humanitarian Law- International Armed conflicts (IAC) & Non- International Armed Conflicts (NIAC). In case of an IAC, it is pertinent to analyze whether 'Use of force' under Article 2(4) of the UN Charter, includes cyber-attacks within its meaning. There are conflicting opinions among experts with regard to this. But an ambiguous provision in a treaty should be interpreted inaccordance with the object and purpose of the treaty in question.[7] The object of the UN Charter is to maintain peace and security and so the scope of Article 2(4) could be expanded by including cyber-warfare within its meaning. It would also help the State (Victim State) to invoke the right to self defence[8] in case of a cyber-attack. There is no question of applicability of Article 2(4), if the effects of cyber-warfare are similar or comparable to that of effects of conventional warfare. However, in case of a NIAC, it is difficult to categorize a cyber-attack as an armed conflict. Unlike in IAC, maximum violence is the threshold limit for NIAC. Therefore singular, unorganized cyber-attack enforceable by domestic laws will not be treated as an armed conflict.

It is established that existence of armed conflict is a prerequisite to application of International Humanitarian Law. But not all cyber operations during an armed conflict will be subjected to the principles of the said law. For example, cyber operations by a private individual during an armed conflict which is totally unrelated to armed conflict will not be governed by the International Humanitarian Law. There is no express provision for cyber warfare under Geneva Conventions or Hague Conventions. But reliance can be made on the Martens Clause which states that the civilians and combatants can seek protection under principles of humanity and

[5]Common Article 2
[6] ICTY, The Prosecutor v. Dusko Tadic, IT-94-1-A, 2 October 1995, para. 70
[7]Vienna Convention on Law of Treaties, Article 31
[8]UN Charter, Article 51

from dictates of public conscience for the cases not covered by the Convention/ Regulation.[9] Therefore International Humanitarian Law could be applied to cyber warfare through Martens Clause.It is contended by many scholars that International Humanitarian Law applies to cyber operations that are ancillary to the kinetic operations undertaken in an armed conflict.

6. ISSUE PERTAINING TO THE APPLICATION OF INTERNATIONAL HUMANITARIAN LAWIN A CYBER-WARFARE:

- **DISTINCTION BETWEEN COMBATANTS AND CIVILIANS :**

  Principle of Distinction is one of the most significant rules in International Humanitarian Law. In fact it act as a basis for application of International Humanitarian Law, since the core objective is to protect the non- combatants. Armed forces refer to organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. The members of the armed forces(except medical personnel and chaplains) are combatants and they have the right to take part in the hostilities[10], and these combatants if captured or falls under the power of adverse party, will be treated as prisoners of war, except spies and mercenaries[11]. The combatants, under Article 44 (3) of the AP I, have an obligation to distinguish themselves from the civilians by carrying arms openly during an attack, etc. during a military engagement. However the application of this provision in a cyber-warfare in difficult. A hacker or any person undertaking the cyber operations might not satisfy the above mentioned essentials, thereby making it difficult to establish such person as a combatant.

- In case of an International Armed conflict, the meaning of attack is ambiguous to apply in a cyber-warfare. Attack is defined as an act of violence against the adversary.[12]If a hostile act is solely committed through cyber operation, the application of this provision is insignificant. Absence of specific threshold with respect to cyber-attacks constituting armed conflict is an existing issue which requires clarification. However, the core customary principles reflected in AP I apply to operations not falling within the meaning of attack. It is a generally accepted that the term violence under Article 49 refers to the

[9]Article 1(2), AP I acknowledges martens clause
[10]AP I, Article 43
[11]Id, Article 47
[12]Id, Article 49

consequence of the operations and not the means of conducting it. Cyber-attack is a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to a person or damage or destruction of property.[13] The issue pertaining to this definition is that it restricts its scope only to physical destructions. Absence of threshold make it difficult to categorize a cyber- operation as an 'attack', because it would be unreasonable if cyber operations disrupting a critical infrastructure causing harm to many people are not regarded as an 'attack' and at the same time it would also be illogical to maintain that a mere inference with computer system would constitute an 'attack'.[14] Therefore there exists a controversy with regard to application of rules for conduct of hostilities (provided in Geneva Conventions) in a cyber-warfare.

- **APPLICATION OF CUSTOMARY INTERNATIONAL HUMANITARIAN LAW:**

Rule 14 of Customary International Humanitarian Law, prohibits an attack which is expected to cause incidental civilian harm in excess of anticipated military advantage. In an armed conflict, either IAC or NIAC, if one party is resorting to cyber-attacks and the other party uses conventional warfare techniques, the existing compliance mechanism isinsufficient as it is difficult to ascertain the military advantage and proportionality in such case.

If both civilians and armed forces use the same cyberspace, there is no regulation to govern the incidental damage caused to civilians through a cyber-attack on military objectives. It is difficult to measure military advantage if almost everything with respect to cyberspace where both civilians and armed forces are users is interconnected or inseparable. Also it is difficult to apply doctrine of distinction in such case because generally dual use objects are treated as military objectives due to the military purpose they serve.[15] But applying this principle would be absurd since it would classify all the elements of cyber infrastructure as military objectives. Also according to Rule 16 of customary International Humanitarian Law, each party to a conflict should verify that the

[13]Rule 30, Tallinn Manual on International Law applicable to Cyber Warfare. It is a non-binding study on application of International Humanitarian Law in a cyber-conflict. It was written by a group of experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence.
[14]Etian Diamond, Application of International Humanitarian Law to cyber-warfare
[15]Rule 39, supra 10

targets are military objectives. However it is highly impossible to completely differentiate military objects and civilians in case of cyber infrastructure having dual purpose. Therefore it is difficult to apply core principles like distinction, proportionality, precaution etc. in a cyber-warfare.

Therefore it can be concluded that there exists an issue with respect to application of principles of International Humanitarian Law in a cyber-warfare.

CHAPTER 3:

7. CONCLUSION:

Cyber-Warfare is an evolving threat and various Countries started addressing to issue of cyber-warfare and cyber-terrorism. A group of experts drafted a non-binding material with regard to application of International Humanitarian Law in a cyber-conflict.[16] It addresses almost all the issues pertaining to the application and serves as guiding manual. There is no question of applicability of International Humanitarian Law in a cyber-warfare. The issue that exists is with regard to the how it is to be applied. This is because, the means and methods of this kind of warfare is completely different from those that are addressed in International Humanitarian Law. Lack of threshold test and clarities with respect to application of rules to cyber operations are few concerns which require clarification. It is significant to address the challenges that arise due to implementation of the principles, in order to ensure effective protection of civilians and civilian objects since that is one of the main objectives of humanitarian law. Therefore it is necessary to address the lacunas and interpret the existing rules pertaining to means and methods of warfare so as to include aspects like cyber-operations. This will improve the compliance mechanism and solve the issues pertaining to the application of International Humanitarian Law.

8. BIBLIOGRAPHY

Statute or Conventions

1. Geneva Conventions Of 1949

[16]Supra 10

2. Additional Protocols To Geneva Conventions, 1977
3. UN Charter, 1945
4. Vienna Convention On Law Of Treaties, 1969

Articles and Manuals:

1. Tallinn Manual On International Law Applicable To Cyber Warfare
2. Applying International Humanitarian Law To Cyber Warfare, Eitan Diamond
3. The Challenges Of Cyber-Warfare : The Application Of International Humanitarian Law (IHL): A Critical Examination Of IHL Rules In Addressing Those Challenges, Addisu Genet, International Law Journal, Volume 4, 2018