Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 7, 2887-2895

Approaches Towards Applicability Of International Humanitarian Law On Cyber Attacks: A Critical Appraisal

Muhammad Siraj Khan[1] , Naghma Farid[2] , Noman Gul[3] , Asim Niaz Khan[4] , Dr. Azmat Ali Shah[5]

[1]Nawab Allah Nawaz Khan Law College Gomal University DI. Khan
[2]Nawab Allah Nawaz Khan Law College Gomal University DI. Khan
[3]Nawab Allah Nawaz Khan Law College Gomal University DI. Khan
[4]Department of Political Science Qurtuba University DI.Khan
[5]Department of Political Science Gomal University D.I.Khan

ABSTRACT

The recent decades have seen greater reliance of individuals as well as states on the computer networks. These networks are used for military and civilian purposes alike that ranges from online shopping to the regulation of radars, satellites and nuclear facilities and installations. For this reason, the computer network system of any country gets a special significance from military point of view during a conflict. The use of computer technology during an armed conflict to gain military advantage poses special challenges to the International Humanitarian Law (IHL) in terms of its applicability as it is qualitatively different from other means and methods of warfare. Many legal experts appreciate the fact that military operations conducted through cyber means during an armed conflict may cause harm of grievous nature.However, they differ over the interpretation and applicability of the relevant law. Schmidt (2014) has noted that there exist, at least, two approaches towards the applicability of IHL over cyber warfare that he calls the 'permissive' and the 'restrictive' approaches[1]. After appraising both these approaches, this article suggests that in order to apply the IHL to a cyber-operation during an armed conflict, it is the impact and consequences of such an operation over the civilian population that should play the decisive role. The main argument it puts forth is that it is the protection of civilians that lies at heart of the IHL.

KEY WORDS: Modern Means and Methods of Warfare, Cyber Attack, International Humanitarian Law.

Introduction

Wars are as old as men. As humans progressed in every field, the art of war is no exception to it and has gone through the process of sophistication and refinement. The training of soldiers, strategies of fighting, methods and techniques of

warfare, sophistication in weapons, the conduct of warfare, in short every aspect related to war has evolved and progressed during the course of time. The use of novel means and methods in warfare has always affected its governing rules and norms. The international law of conflicts has two categories; each comprises its own set of laws and cover distinct aspects of conflicts. The first set is called the jus ad bellum[2]that determines the legality of an armed conflict per se.In other words, it is related to the use of force by a state in an armed conflict and describes conditions, prohibitions and exceptions thereto. The jus in bello[3]on the other hand, deals with the conduct of hostilities during war. It governs the hostile acts of parties during an armed conflict, the manner in which attack is conducted, differentiates between civilians and combatants and between civilian objects and military objectives. There is yet another difference between the two; the subject of jus ad bellum are states and is applied only to international armed conflicts where as the jus in bello applies to non-international armed conflicts as well.

The use of computer technology in military operations is one of challenges that the legal experts have been debating over since early 90s. Computers are used by individuals, corporations as well as governments. They are used in maintenance of services and supplies, management of air-traffic control, railways, banks, industries, dams, and in regulating the nuclear facilities and installments. For that reason, the computer network system of any country gets a special significance from military point of view in an armed conflict.

As a matter of practice, wars are fought in battlefields on land, water or in air. With the development in fields of computers and network systems and growing military reliance of governments over them, a new space of battle has come into existence that is called the 'cyber space'. Experts have defined it as "the environment formed by physical and non-physical components, characterized by the use of computers and electromagnetic spectrum, to store, modify and exchange data using computer networks".[4] This particular space of warfare is elusive and cannot be seen but may have detrimental consequences like those of a conventional war fought with kinetic weapons. This has posed challenges to the legal regime that applies to armed conflict whether that is the jus ad bellum or the jus in bello.

This paper aims at the problem of applying IHL over cyber operations conducted to get military advantage over the adversary during an armed conflict. The Geneva Conventions of 1949 and the Additional Protocols to them of 1977 do not specifically mention terms like cyber operations or cyber attacks as they were drafted at times when wars were fought with 'kinetic weapons'. The cyber warfare is, however, quite different from other methods and techniques of warfare and, therefore, remained a debatable subject till this day. The cyber conflict is not fought in the conventional battle field or spaces like air, water or land. It is fought in the cyber space. Its 'weaponry' is qualitatively different than that of the conventional wars. The implications of the terms like conflict, armed attack, use of force, military and civilian objects etc change all together when we try to apply the rules of IHL over the cyber warfare. Therefore, the need to expound the IHL and its application over the subject area becomes more important.

Applicability of IHL to Cyber Attacks

Many legal experts appreciate the kind of hostilities that may be conducted through the use

of computer network for gaining military advantage during a conflict. They, however, differ over the applicability of law to such operations. When does a cyber operation become prohibited by the IHL? Does IHL apply to each and every cyber operation that is conducted during an armed conflict? In order to respond to this question the debate would mainly revolve around the concept of 'attack' under the IHL as the civilian population and the civilian objects have been granted protection against 'attacks'. So, the same question may precisely be rephrased as when would a cyber-operation qualify to be termed as an' attack' in the meaning of the relevant law?

The principle of distinction lies at the core heart of the International Humanitarian Law. It has been mentioned earlier that the purpose of IHL is to minimize the havoc of war in terms of human losses as well as property, infrastructure and facilities over which the human life depends to sustain. The issue becomes crucial in case of cyber operations after they are assigned the meaning of 'armed attacks' in relevance of the IHL. The principle of distinction attracts automatically and the IHL has, relatively, greater strictness about it.

As to protection of civilians during an armed conflict, Articles 48-58 of the AP-Iare most instructive. There is a difference of opinion about the applicability of these provisions over the cyber operations. Article 48 of the AP-I binds the parties to a conflict to distinguish between the civilian population and combatants and between civilian objects and military objectives at all times. It asserts the parties to 'direct their operations only against military objectives.'[5]This controversy is more sharpened when one looks at article 51 of the AP-I that reads in its first clause that: "The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations."[6]This clause confers blanket protection to each and every person who qualifies to be a 'civilian' in the meaning of Article 50 of AP-I against 'dangers arising from military operations'. The phrase 'dangers arising from military operations' in general and its last portion 'military operations' specifically have stirred controversial debate among legal experts. As the term 'military operations' is very general and wide and, if applied vigorously, may restrict each and every operation that is related to the activities of armed forces during a conflict. This term, in its restrictive sense of application, would also apply to each and every 'cyber operation' that is related to the activities of armed forces to a conflict. Likewise, the term 'dangers arise from' is also subject to interpretation before its application. A danger may be referred to a mere apprehension or a threat and it may also mean casualties and destruction on a large scale.

Having said that, it is interesting to note that the succeeding clauses of same Article 51 of the AP-I, while instructing the parties to an armed conflict about protecting civilians, use the term 'attack' instead of military operations. This controversy is the basis for the evolution of the two approaches, the permissive and the restrictive approach, towards the application of IHL over the cyber operations.

The Permissive Approach

Schmitt, the pioneering champion of this approach, considers it to be called 'permissive' because it 'allows a wider range of cyber operations against the civilian population'.[7]He argues that IHL becomes applicable as soon as an armed conflict is initiated. What does constitute an armed conflict? In response to this question he

.

concludes that, (an) "armed conflict occurs when a group takes measures that injure, kill, damage or destroy.The term also includes actions intended to cause such results or which are the foreseeable consequences thereof".[8]This view, as shall become clearer, sets the basic criteria for the proponents of this approach as to when IHL would apply to cyber operations. His arguments are based upon articles 51 and 52 of the AP-I wherein protection is granted to the civilian population and objects specifically to 'attacks 'during an armed conflict. It is argued that word 'attacks', for the purpose of IHL, has been defined by article 49 of the AP-I as "acts of violence against the adversary, whether in offence or defense".[9] Hence, only those 'military operations' that constitute an 'act of violence' may be termed as 'attacks' and, therefore, shall be regarded as prohibited under the IHL.

This argument faces us with a problem when we try to apply IHL to cyber operations as they are not normally 'violent' in the first place. Schmitt puts this dilemma as, "although clear with respect to classic kinetic operations, Article 48′s plain text and the Commentary's reference to the use of violence might seem problematic when applied to cyber operations since they are not violent per se".[10] While responding to this issue, he opines that "although the principle of distinction is framed in terms of 'military operations', it is clear that not all military operations are contemplated by the norm".[11]To support his opinion, he mentions that in practice, the operations of espionage, propaganda or dropping of leaflets have not been contemplated as 'violent' by states to an armed conflict. Thus, he infers that the relevant article would 'encompass all acts having violent consequences'.[12] Hence, cyber operations that result in death or injury to civilians' person or cause physical damage or destruction to their property would qualify to be an 'attack' under IHL and, therefore, prohibited. On the other hand, cyber operations which do not physically harm the person and/or property of civilian population would fall short of the definition of 'attack' and would not cause the attraction of the relevant provisions of the AP-I.

The Restrictive Approach

Along with the permissive approach, some experts adopted a different approach, more restrictive regarding the applicability of the rules of IHL to the cyber operations. The proponents of restrictive approach are of the view that it is not the nature of military operation alone that decides whether IHL principles would be attracted to it or not. Rather, it is the protection of civilians that has been contemplated by the framers of the protocols. They declare the fact that whether a cyber-operation would result in the destruction of an object or not is altogether irrelevant.

Dörmann says that whether a cyber operation results in the destruction of a targeted object or not is altogether irrelevant. He refers to article 52 (2) of the AP-I which holds only those objects, which make effective contribution to military action or whose total or partial destruction or neutralization would give a certain military advantage over the adversary as valid targets of attacks. According to him, the term neutralization in the said article contemplates that for the purpose of an operation to qualify as an attack, it is irrelevant whether the targeted object is disabled through destruction or otherwise.[13]

Droege disagrees with the permissive approach on different grounds. She is of the view that the principle of distinction binds the conflicting parties to distinguish between civilians and combatants and between civilian objects and

military objectives because it seeks the protection of the civilians in the first place. The relevant provision (article 48 of the AP-I) requires them to direct their operations only against military objects. Thus, by virtue of this provision, any operation that is aimed at or directed against a civilian person or object shall be deemed as violation of the IHL. Responding to Schmitt that some operations, for example propaganda or other psychological operation may be directed towards civilians is an argument that is based on misunderstanding of the 'military operations'.[14]She argues as to responding the permissive approach that considering an attack to be necessarily an act of violence would mean to restrict it to kinetic means of warfare. A military operation that is not violent per se but which result in violent consequences would also qualify as an attack. She gives the example of chemical and biological weapons whose use does not involve physical force but the consequences are dreadful and would, therefore, constitute an attack. In other words, it is not the violent means but violent consequences that would confer a military operation the status of an attack. She further argues that Schmitt has overlooked the fact"that 'neutralization' was meant to encompass an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it".[15] For example, any cyber interference with the computer system of enemy's air defense that disables it for a certain span of time would come under the definition of 'neutralization' and would, therefore, constitute an 'attack' within the meaning of IHL even if no harm has occurred to the physical infrastructure.[16]

Critical Analysis of the Permissive and Restrictive Approaches

The whole theme of IHL is to strike a balance between military necessity during warfare on one hand and the protection of civilians from hostilities on the other. Thus, the protection of civilians and civilian objects lie at the heart of IHL. In order to keep this balance, the IHL provides for the principle of distinction that is required to be strictly observed by the conflicting parties at all time. Article 48 of the AP-I establish the principle of distinction and firmly assert the parties to a conflict to 'direct their operations only against military objectives'.[17] The term 'operations' used in the said article is general and would encompass every operation carried out by the conflicting parties during a warfare to get military advantage. The advocates of permissive approach, as mentioned earlier, asserts that the proceeding articles use word 'attacks' instead of 'operations' and, therefore, only a cyber operation that qualifies to be called as an 'attack' would attract the provisions of IHL. They rely upon the definition of 'attacks' as mentioned in article 49 of AP-I.

As for as Article 48 is concerned, it underlies the principle of distinction and offers general protection to civilians and civilian objects during an armed conflict. This protection is not only general but is also permanent as the parties to the conflict are bound to distinguish between military objectives and civilian objects at all times during the conflict. The protection of civilians lie at heart of the IHL, therefore, they are granted protection against all kinds of military operations that are aimed at or intended against them. The same approach would be adopted in case of cyber operations and the parties would be bound to strictly observe the principle of distinction at all times when such operations are conducted in warfare.

Responding to the dichotomy of words 'operations' used in article 48 and 'attacks' in some of the succeeding articles, this author has

observed that the provisions which mention the term ‘attacks’ are prohibiting certain acts of the conflicting parties. Such acts, as per definition of words attacks, are conducted to get military advantage over the adversary which is a military objective, through violence. These provisions bind the attacking party that while conducting an attack, no compromise could be made over the protection that has been offered to civilians. It is so because the IHL does not prohibit an armed conflict per se and allows the parties to take military advantage over the adversary but regulates the conduct of hostilities, thus, restricting the rights of the parties to a combat. In other words, the provisions which, by establishing the principle of distinction, offer protection (which is general and to be respected at all times) to civilians, word ‘operations’ has been used which, too, carries more general and wider sense than ‘attacks’.

On the other hand, while addressing the conflicting parties, thereby restricting their right to combat, word ‘attack’ has been used that carries the meaning of a targeted and specific kind of operation that is intended to gain military advantage through violence.

The notion that ‘acts of violence’ necessarily means to kill, injure, damage or destroy needs to be ponder upon. Droege and Dörmann[18] have responded to such notion by suggesting that term ‘neutralization’ used in article 52 (2) does not necessarily mean total or partial damage or destruction of an object. According to them if an object is made disabled to be used by the enemy whether temporarily or permanently to gain military advantage, it comes within the meaning of ‘neutralization’ even if no physical damage has been made to it. So, if a cyber operation is conducted to attack at a computer system that impairs its working or cause denial of a service would be termed as neutralization of such system. Whether it amounts to an ‘attack’ or not would depend on its impact and consequences over the civilians. It is not necessary that the same operation may cause death or injury to a person or physically damages or destroys a civilian object. If we accept the position taken by the advocates of the permissive approach, such an opinion, in words of Droege, “would lead to the conclusion that the destruction of one house by bombing would be an attack, but the disruption of an electrical grid supplying thousands or millions of people would not”.[19]

The IHL guarantees protection to civilians as well as civilian objects. The word ‘object’ also stirs a controversy among the experts as to whether data stored in a computer or hard disk may be treated as an ‘object’ or not. And in case if the resident data in a computer is attacked through cyber means, whether damage or destruction of the same would amount to an ‘attack on civilian object’ in the meaning of Article 52 of the AP I?

The proponents of permissive approach hold the view that the word ‘object’ has not been defined in the AP I but a dictionary meaning of the word is something that is visible and tangible. Since ‘data’ is neither of them, therefore, it does not qualify to be an ‘object’ under IHL[20].

Some experts hold an opinion contrary to that of the advocates of the ‘permissive approach’. They argue from Article 48 of the AP I which provides blanket immunity to civilians and civilian objects against all kinds of military operations. They argue that if the former opinion is accepted, it would restrict the relevant law and would pose potential threats to civilian datasets and information no matter how much valuable and important they may be. Such a stance would also contradict the customary premise of law that

offers general protection to the civilians and civilian objects[21].

As an observation during this study, a point may be raised here that Article 51 (2) limits military objectives to 'those objects which by their nature, location, purpose or use make an effective contribution to military action'. It further holds that if the total/partial destruction, capture or neutralization may result in military advantage during the circumstances[22]. In this article the words 'nature, location, purpose or use' are important. Since the 'nature' of computer data is different from other tangible objects and could only be 'useful and purposeful' if it is 'located' in its proper place i.e. a disk or any device where it is stored. Therefore, if a resident data which is used for civilian purposes only is attacked during an armed conflict in such a manner which renders it useless either by wiping it out of the storage place or corrupting it, affecting the civilian population e.g. interruption in electricity or disturb the air traffic control, it would in violation of the general protection guaranteed to the civilian by AP I.

A thorough analysis of both these approaches in the light of the principles of distinction suggests that it is not the violent means through which an act is conducted and, therefore, qualifies it be an "attack" in the meaning of IHL but it is rather the impact and violent consequences that it generates or is capable to generate over the civilian population. As and if such consequences are caused by a cyber means of warfare, it would fairly attract the relevant provisions of IHL.

Conclusions

Human advancements in every field pose challenges to the norms whether social or legal. Laws have to pace up with the advancements of modern era. Modern means, methods and techniques of warfare have raised many questions about the applicability of IHL to them. In recent few decades, we have witnessed an exponential development in field of computer network systems and both the civilian and military installments and infrastructure are, to a greater extent, dependent upon them. The use of cyber means during an armed conflict in order to get military advantage over the adversary party has stirred a controversy about the applicability of the relevant laws of warfare. They can potentially result in drastic consequences if used against civilian population and civilian objects.

Although there exists a group of experts who believe that the existing legal regime is not compatible to the developments in cyber technology and a new convention is ultimately needed to provide answers to the questions that rise in case of cyber attacks[23]. Such proposals may seem closer to an 'ideal' to some but in practice is quite lengthy process and may take many years or several decades. Whereas the advancements in the field of computer technology are rapid and fast tracked, hence, challenges, too, are growing rapidly. This would only mean to leave the entire mankind vulnerable to the dangers arising out of cyber attacks during conflicts.

This is one of the reasons that the majority experts, organizations are busy in deliberations upon the issue so as to the existing legal regime is explored and exploited to its maximum by way of interpretation. Moreover, International law is robust and flexible enough to be applied to new situations and circumstances through proper interpretation. There is an agreement among majority expert that international law is sufficiently vigorous and dynamic to be applied over them. They have difference of opinion, however, over the question as how should it be

applied to them. During the course of debates for more than a decade over the issue, two approaches have been evolved namely the permissive and restrictive approach. The former allows a wider range of cyber operations to be conducted during an armed conflict against the civilian population whereas the later puts restrictions on them. One of the he main controversy among the experts revolve around the question as to when a cyber operation may qualify to become an 'attack' in the meaning of the IHL and thereby attracting its relevant provisions. The two approaches that have been evolved during this debate have their own strengths and weaknesses as to justify their arguments.

It is important to mention here that during the ongoing debate, focus shall remain over the core principles of the IHL e.g. principles of distinction, precaution, proportionality etc and shall be applied uniformly to all kinds of hostilities during an armed conflict irrespective of the means and method induced.

Recommendations

Cyber means of warfare are under the process of development and therefore deemed to have been under ruled. There is very less evidence of state practice that has evolved regarding the issue. The experts have been, however, debating over the application of the principles and provisions of the IHL over the cyber warfare. There is a need to look at the purpose of IHL which is the protection of those human who are not participating in the acts of hostilities during an armed conflict. Therefore, their protection from wrath of war shall be the object of every approach adopted towards the applicability of IHL over cyber attacks.

Secondly, efforts should be made to separate, as for as possible, the military computer network system shall be separated from the civilian as currently both of them share a common system. Both the civilian and military installations rely on the same computer network system which causes difficulty in establishing the principle of distinction.

It has been made clear via detailed debate in this thesis that cyber attacks may qualify to be 'use of force' (Art 2 of UN Charter), 'armed attack' (Art 51 of UN Charter) and an 'attack' (in the meaning of AP I) in given circumstances. It is suggested that for purpose of application of IHL to a cyber attack, the impact and consequences which result in such an operation shall be regarded as the decisive factor. When a cyber attack produces consequences in the 'outer world', it poses a serious concern and if the impact and consequences may prove to be dreadful to the civilian, it will be in violation of Art 48 of AP I.

For the purpose of the applicability of IHL over cyber attacks, it is irrelevant whether it has been conducted through a violent means or not. Looking from the angle of the general protection offered to the civilians at all times, it is the impact and consequences of such attacks upon the civilians that shall play a decisive role. If a cyber attack is aimed and targeted at the civilian or civilian objects, it shall stand prohibited under the law. If the consequences of a cyber attack during an armed conflict are likely to have dreadful consequences for the civilians, it shall also be prohibited. A cyber attack can be conducted during an armed conflict only to target a military objective, and not the civilians, in order to get a certain military advantage over the enemy. Moreover, all the provisions of IHL shall equally apply to an attack that is conducted through cyber means.

The general protection shall be available to civilians against cyber attacks in the same manner as it is available against other means of warfare. Cyber operations that are aimed at civilians shall be prohibited under the IHL. The principle of

proportionality shall apply to the cyber attacks as well and the attacking party must calculate the proportion of military advantage that it wishes to gain and the likelihood of collateral damage in result of such attacks.

At present stage, it seems difficult to answer each and every question regarding the applicability of IHL over cyber warfare. However, appreciating the flexibility of time tested principles of IHL, the state practice that may be hoped to evolve during due course of time regarding the use of cyber means and methods of warfare, and through a deliberate, healthy and objective debate over the legal and technical issues involved, one can be optimistic that we would feel more comfortable in applying laws over cyber warfare in the coming future.

References

Treaties

Icrc.org. (2018). Protocols additional to the Geneva Conventions of 12 August 1949. [online] Available at: https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf [Accessed 10 July 2018].

Manuals

Schmitt, Michael. N. (Ed.). Tallin Manual on the International Law Applicable to Cyber Warfare. Cambridge, NY: Cambridge University Press. Retrieved July, 10, 2017 from https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Articles

1. Dörmann, Knut. “Applicability of the Additional Protocols to Computer Network Attacks”. [online] Available at https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf [Accessed on September 16, 2018].
2. Droege, Cardula. “Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians”. International Review of the Red Cross 94, No. 886 (2012): 533-578.
3. Schmitt, M. N. “Wired Warfare: Computer Network Attack and jus in bello”. International Review of the Red Cross 84,No. 846 (2002): 365-398.
4. Schmitt, M. N. “Attack” as a Term of Art in International Law: The Cyber Operations Context”. 4th International Conference on Cyber Conflict. Eds. Czosseck & Ziolkowski. Tallin: NATO CCD COE Publications (2012).
5. Schmitt, M. N. “Rewired Warfare: Rethinking the Law of Cyber Attack”. International Review of the Red Cross 96, No. 893 (2014): 189-206.