International Journal for Multidisciplinary Research (IJFMR)
E-ISSN : 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law

Rohit Bokil

Assistant Professor, ILS Law College, Pune

INTRODUCTION

The use of the internet has become so extensive today that a historical fact is easily forgotten, i.e., internet was originally used only for military purposes and it took several years before it became available to civilians. With the development of electronics and telecommunications, military's reliance on computer systems and networks has increased exponentially, thus opening a "fifth" domain of war-fighting next to the traditionally recognized domains of land, sea, air and outer space (Melzer 2011). Initially, it was not recognized that the internet or the cyberspace could prove a battlefield and internet can be used to attack nations. But now it has become a reality. Cyber warfare is basically an attack using computers or networks to affect the networks or computers of other nations. In simple words it can be described as a war fought with computers and networks.

The development of computers and internet has happened so fast that the existing laws relating to warfare have proved to be inadequate in regulating them. This trend raises the question: To what extent could the existing International Humanitarian Law (IHL) be transposed to the cyber domain? Applying pre-existing legal rules, concepts and terminology to a new technology may entail certain difficulties in view of the specific characteristics of the technology in question.

International Humanitarian Law (IHL) applies exclusively in the situations of armed conflict. IHL comprises of a large number of international treaties which have been developed over the period of 150 years, starting with the Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field in1864. The major part of modern IHL is based on four Geneva Conventions of 1949 and two Additional Protocols of 1977 and a third Additional Protocol of 2005. These are as follows: (a) Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GC I), (b) Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GC II), (c) Convention relative to the Treatment of Prisoners of War (GC III) and (d) Convention related to the Protection of Civilian Persons in Time of War (GC IV). The three Protocols are:(a) Protocol Additional to the Geneva Conventions of 1949, and relating to the Protection of Victims of International Armed Conflicts (AP I), 1977, (b) Protocol Additional to the Geneva Conventions of 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), 1977 and Protocol Additional to the Geneva Conventions of 1949, and (c) relating to the Adoption of an Additional Distinctive Emblem (AP III), 2005.

As IHL regulates the conduct of hostilities between the belligerent parties, as well as the protection and treatment of those having fallen into the power of the enemy, it would be natural to expect the application of IHL in the cases of cyber warfare or cyber-attacks. But there are several issues and problematic areas, which are discussed in this paper.

CYBERSPACE AND THE CONCEPT OF ARMED CONFLICT

One way to understand the concept of cyberspace is to understand its contents. The Cyberspace includes (a) the infrastructure which includes hardware parts such as integrated circuits, storage devices, fiber optic cables etc. (b) software programs and (c) data which is created by machines and which is in a stored form.

One of the most difficult issues in IHL is the classification and definition of 'conflict'. The notion of cyberspace makes it further complicated. Conflict in cyberspace shares certain similarities with the traditional concept of armed conflict. There are certain evident differences between traditional kinetic conflict (TKC) and cyber conflict which should be grasped at the outset.

In TKC, military operations happen between military forces and civilian population is not involved. In cyber conflicts the space where the conflict takes place is shared by civilian population. In TKC, offensive technologies and defensive technologies are often in rough balance. In cyber conflicts the offence is inherently advanced to the defense because the offence needs to be successful only once, whereas the defense needs to succeed every time (Lin 2012: 521). In traditional conflicts the activities are carried out by the military forces which are presumed to be under the command of national government. No such presumption exists in cyber conflicts. In TKC, the effects that are produced are generally a function of the number of military personnel and since such numbers tend to be smaller for non-state actors than those available to states. In cyber conflicts, non-state actors can leverage the capabilities of IT to produce some of the large-scale effects that can be achieved by large-scale actors (Lin 2012: 521). In conventional conflicts, violations of national borders are significant and important. But in cyber-conflicts the distance is immaterial and breach of national borders for offence and defence occur routinely and without being noticed.

WHAT IS CYBER WARFARE?

The International Committee of the Red Cross (ICRC) has defined cyber warfare as "A means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL". As per this definition, the cyber warfare basically consist cyber operations which are carried out during an armed conflict, as defined under IHL. This means that any cyber operation carried during an armed conflict could be treated as the cyber warfare. The problem with this definition is that it is too general. It does not specifically define which cyber operations constitute cyber warfare. IHL basically defines conflicts in two types: international armed conflicts (IACs) and non-international armed conflicts (NIACs). Hence, defining every cyber operation in IACs or NIACs as cyber warfare becomes problematic.

Cyber warfare is also defined as "Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in

response to a perceived threat against a nation's security." (Shakarian et al 2013:2) This definition of cyber war is basically a policy by one nation state which involves actions taken in cyberspace and which causes serious threats to national security of another nation state. Even though this is a narrow definition, it attributes to one of the most important features of any war that is 'a war should pose a threat to national security'.

Even though the current IHL does not specifically mention cyber warfare, the Martens Clause, that is associated with accepted principles of IHL, says that whenever a state of affairs is not covered by a global agreement, "civilians and combatants stay below the protection and authority of the principles of jurisprudence derived from established custom, from the principles of humanity, and from the dictates of public conscience." Basically, this clause states that in situations wherein there are no concrete rules regarding the law of armed conflict, the combatants and civilians are still protected under the customary rules of international law. The same clause can be made applicable to cyber warfare till concrete rules governing the cyber warfare are not devised.

Cyber warfare came into light after the attacks of 11th September, 2001 in the United States of America. Cyber-attacks were carried out during the massive cyber operations by hackers against Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008. Other cyber operations include the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010. These examples show that the threats of cyber warfare are not hypothetical but real. As the critical infrastructure of nations becomes more reliant on networks and cyberspace, the possible targets for cyber-attacks greatly increases. The major challenge which states face in the cyber environment is that the scope and manner of international law's application to cyber operations, whether in offence or in defense, is not determined.
As cyber warfare is closely related with cyber-attacks it is necessary to understand the term cyber-attacks. One definition is: "A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose" (Hathaway et al 2012: 822). This definition appears comprehensive but needs analysis to bring out the exact meaning of 'action'. A cyber-attack may include hacking, bombing or cutting of networks. The objective of such operation should be to undermine the functioning of a computer network.

Tallinn Manual under Rule 30, defines a cyber-attack as "a cyber operation whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." (Schmitt 2013: 106). The requirements of this definition are same as compared to any conventional attack. Such cyber-attack should cause injury, death to humans or damage or destruction to objects. This definition is simple but it aptly describes what a cyber-attack is and it includes both, offensive and defensive capability of a cyber-attack.

As any warfare involves weapons and methods of warfare, it is necessary to look what are means and methods of cyber warfare. Means of warfare consist of all weapons, weapons platforms and associated equipment used directly during conflicts. If this description is applied to cyber weapons then the pertinent question is how a potential cyber capability can be described as an offensive capability? In such a scenario the destructive nature of that potential cyber capability makes it a cyber weapon. Therefore, a cyber

weapon would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects (Boothby 2013: 389). It can be deduced from the above cited text that, computers and computer systems that are capable of causing effect on the data in the targeted computer or can affect the service the target computer provides, on an opponent in the conflict are capable of being a cyber weapon.

There are three customary principles of use of weapons as far as IHL is concerned. The first is that the right of the parties to an armed conflict to choose methods or means of warfare is not unlimited which means that those engaged in cyber operations during an armed conflict have a duty to respect the rules of law applicable during an armed conflict as mentioned in Article35(1) of AP I. As per Article 35(2) of AP I, it is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous or unnecessary suffering. In applying this rule, the legitimacy of a cyber weapon must be assessed "by comparing the nature and scale of the generic military advantage to be anticipated from the weapon in the application for which it is designed to be used with the pattern of injury and suffering associated with the normal, intended use of the weapon." (Fenrick 1990: 500). Article 51(4) of the AP I provides that it is prohibited to employ weapons, means or methods of warfare, including cyber weapons to cause indiscriminate attacks.

CYBER WARFARE AND INTERNATIONAL LAW

As far as applicability of international law to cyber warfare is concerned, it has two components: customary international law and *jus ad bellum* which is state's right to resort to force.

Customary international law with respect to cyber warfare suffers from certain problems. As the notion of cyber warfare is new, the state practice is not sufficiently developed to deal the situation. Instances of cyber-attacks have shown that even the victim states are hesitant to acknowledge cyber-attacks. It is also very difficult to gather enough evidence as to make a state liable for cyber-attacks. As cyber operations are not visible, it is very difficult to determine a state's cyber practice. These factors make crystallization of customary principles with respect to cyber warfare a difficult task. The application of customary law to cyber warfare should be based on the interpretation of existing customary norms.

Jus ad bellum has two components: (a) resort to use force as given under Article 2(4) of the UN Charter and (b) right of self-defence as given under Article 51 of the UN Charter. But as the "force" is not defined under the UN Charter this task has been kept open for interpretation by the International Court of Justice (ICJ). ICJ has given contradictory opinions with respect to use of force which has resulted in confusion at the global level, whether use of force includes cyber-attacks. Whether cyber-attacks can be used in self-defense is also a debatable issue.

Attribution of cyber-attacks to a state is also a difficult task due to the anonymity in the cyberspace. It is very hard to find out the origin of a cyber-attack. Often effects of cyber-attacks are not visible enough to attribute such attack to any particular state. Difficulties in gathering evidence, also makes this work further problematic. Indirect support from state to non-state actors for cyber-attacks is not sufficient to hold the state liable for cyber-attacks.

APPLYING INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE

The issues of cyber warfare and cyber security have gained much attention recently because of the humanitarian concern. The risk that civilians and civilian objects will come to harm as a result of cyber warfare is heightened by the high level of interconnectivity and interdependence between civilian and military computer infrastructures which makes it very difficult to differentiate between them. In view of these risks it is clear why there is a humanitarian need for the law to regulate cyber warfare. But at the same time many questions remain open about how existing legal frameworks might be applied to this relatively new phenomenon.

Cyber warfare does not occur in a legal void. To be sure, cyber operations are governed by international law, and when amounting to or occurring in the context of an armed conflict they are regulated by IHL. However, even while there is no question that IHL applies to cyber warfare, when considering *how* it is to be applied many questions emerge that have yet to be given comprehensive and satisfactory answers. The nexus between IHL and cyber warfare is interwoven and interconnected. IHL deals with the rules that militaries must follow when participating in a war. These laws of war describe what actions may or may not be taken against non-combatants, soldiers and unlawful combatants. A key point of IHL is that civilians and non-combatants may not be killed or treated inhumanly during times of war.

Cyber warfare challenges some of the basic assumptions of IHL. First, IHL presupposes that the parties to conflict are identifiable. However, in the cyber operations, anonymity is the rule. If the perpetrator of a given operation and link of such given operation to an armed conflict cannot be established it is extremely difficult to determine whether IHL is applicable. Secondly, IHL is based on the presumption that means and methods of warfare will have effects in the physical world. Many cyber operations may have effects which may be disruptive but may not be immediately seen. Thirdly, the principle of distinction is based on the assumption that civilian objects and military objects are distinguishable. In the cyber theatre most cyber infrastructures serve for both military and civilian communications (Droege 2012: 541).
Once a state has entered into a conflict, the use of force is governed by *jus in bello*. Under jus in bello, even states that have the lawful right to use force still have limitations in how they use it. Jus in bello is largely derived from the Hague Conventions, the Geneva Conventions, and the associated protocols, much of which is considered customary international law. In the words of the Saint Petersburg Declaration of 1868, the aim of the laws of war is to "alleviate as much as possible the calamities of war." (Gervais 2012: 562-563)

Some of the fundamental principles of jus in bello are military necessity, principle of distinction, ban on perfidious conduct, neutrality and proportionality. As with the UN Charter, the Geneva Conventions are silent on cyber-attack as a modality of conflict, and the question of how to apply the above mentioned principles in any instance involving cyber conflict may be problematic.

MILITARY NECESSITY

When a cyber attacker is a party to a conflict, international humanitarian law restricts the use of force to targets that will accomplish valid military objectives. Article 52 of the AP I limits lawful targets to "those objects which by their nature, location, purpose or use make an effective contribution to military action

and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage." Similarly, Article 23 of the Fourth Hague Convention forbids destruction or seizure of property "unless such destruction or seizure be imperatively demanded by the necessities of war." Violating the principle of military necessity is considered a "war crime" in the Rome Statute of the International Criminal Court under Article 8(2)(a)(iv).

A cyber-attack that targets an adversary's military computer systems satisfies the condition of military necessity by virtue of their exclusive military association. But whether a target creates a "definite military advantage" is a complicated issue. The complexity involved in cyber operations makes it difficult to ascertain military advantage. It is possible, that many cyber-attackers would not know the possible effects of cyber-attacks. For example, cyber attacker that penetrates into the computer systems of an electrical generator *might* gain a military advantage, but the system may have unforeseen layers that prevent such an advantage from occurring. In these circumstances, the military advantage is not definite enough to satisfy the condition of military necessity. As far as cyber-attacks are concerned, it is very hard to tell beforehand whether the successful cyber-attack will create a definite military advantage. Military advantage of a cyber-attack can only be determined once it is carried out (Gervais 2012: 564).

PRINCIPLE OF DISTINCTION

The principle of distinction requires that parties to a conflict distinguish at all times between civilians and combatants and civilian objects and military objects and objectives which in enshrined in Articles 48, 51 and 52 of the AP I. This means that, in planning and carrying out cyber operations, the only targets permissible under IHL are military objectives, such as computer and computer networks that make effective contribution to military operations. Attacks via cyberspace may not be directed against computers used in civilian sector.

Under IHL, civilian objects are all those objects that are not serving military objectives. Military objectives are defined under Article 52(2) of AP I as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage" This provision makes it clear that there should be a nexus between the potential target and military action. The term 'military action' denotes the enemy's war-fighting capabilities. This nexus is established through the criteria of nature, location, purpose and use.

Additionally, Article 51 (3) of AP I indicates that civilians who take part in hostilities will be targetable if "for such time as they take a direct part in hostilities." This raises a possibility that a non-state actor, or hacker would be targetable while he or she is launching an attack. Then after conclusion of that attack would become an un-targetable civilian, thus complicating when a non-state actor may be targeted (Pool 2013: 314). Another problem associated with cyber warfare is that certain attacks potentially bring into fray zombie computers that are owned by civilian who have no idea their machines are being used for such attacks. This act could be comparable to the use of "human shields" a known tactic in warfare that is prohibited under the Fourth Geneva Convention (Gervais 2012: 567).

The dual-use objects are those used for both civilian and military purposes. Due to their use for military purposes, they become military objectives under Article 52(2) of AP I and legitimate targets of attack. According to present view, an object cannot be civilian and a military object at the same time. The moment it is used for military action it becomes a military objective in its entirety. It is generally considered today that the object becomes a military objective even if its military use is only marginal compared to civilian use (Droege 2012: 566). It is clear that, in cyberspace the principle of distinction appears to hold a little promise for the protection of civilian cyber infrastructure and all civilian infrastructures that rely on it.

PERFIDIOUS CONDUCT

Another rule of jus in bello is the ban on perfidious conduct, which is in place to facilitate a short period of violence and a quick restoration of peace. The Hague Convention IV Article 23(b) states that "to kill or wound treacherously individuals belonging to the hostile nation or army" is against the laws of war. Perfidy is a form of deception, in which one side insists that it is acting in good faith in conducting hostilities but, once an opportunity presents itself, deliberately acts in bad faith. Such unlawful conduct is prohibited under AP I, which states that "[a]cts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law in armed conflict, with intent to betray that confidence, shall constitute perfidy." Perfidious conduct is prohibited under the law of armed conflict because it undermines the ability to restore peace.

Cyber warfare is enticing for those who wish to indulge in perfidious conduct. Cyber attackers will find bountiful opportunities to influence or mislead adversaries because most sophisticated cyber-attacks involve some level of concealment. Cyber warfare presents additional complexities in that cyber-attacks can deceive targeted states into believing an attack originated from another source, whether the source is a non-combatant or a third party. Under Article 37(1)(c) of the AP I, "the feigning of civilian, non-combatant status," is an example of prohibited perfidious conduct. Cyber attackers that trick adversaries into thinking the attack originated from a non-combatant or a civilian violate the laws of war. But this provision applies only to actions directed against adversaries in armed conflict; thus, an action that tricks third parties to act against adversaries remains a grey area (Gervais 2012: 574). Cyber attackers benefit from the failure of targeted states to detect cyber-attacks or attribute the same to a particular state. Sophisticated cyber attackers are able to operate in ways that make tracing attacks impossible. This is especially true if tracing an attack requires the cooperation of states with strong domestic privacy laws. The result is that military commanders face less accountability and have more incentives to use cyber weapons (Gervais 2012: 574).

NEUTRALITY

The principle of neutrality permits a state to declare itself neutral to a conflict and thereby protects it from attack or trespass by belligerents. The principle of neutrality is derived primarily from the Hague Conventions. The Hague Convention (V) of 1907 in Article 3 outlines the rights of neutral states and their obligation not to participate in the conflict, and the obligation of belligerents to respect the inviolability of neutral states. The Hague conventions allow a neutral state to allow belligerents access to their telephone lines for communicating purposes but when dealing with cyber-attacks, this portion of the Hague

Conventions needs revising if a state is to maintain neutrality and still allow belligerents access to its telephone lines (Pool 2013: 314).

There is a debate among legal scholars as to the liability of a neutral state in cyberspace dealing with a cyber-attack that originated even unintentionally from within its borders. Some argue that because of the packet switching system of electronic information that is the foundation of transmission, and its subsequent unpredictable pathways that information will take to reach its destination, no one can predict the path that a cyber-attack could follow on its way to its target. So the servers used for transmitting the attack are not targetable. Some say that if a state is either unable or unwilling to stop an unlawful cyber-attack then the servers enabling the attack are targetable irrespective of home country's declared neutrality (Pool 2013: 316).

It is unrealistic to require the neutral state to prevent a cyber-attack from originating in its territory because of the complex Internet infrastructure involved in perpetrating, as well as preventing, a cyber-attack. Cyber battlefields do not exist in a concentrated area. The internet infrastructure is disparate and extends globally. It is important to maintain the principle of neutrality to prevent warfare from spreading. The infrastructure of the Internet presents practical problems for a state attempting to be neutral under the current IHL framework. A re-interpretation of neutrality that permits a state to maintain its neutrality despite its cyberspace infrastructure "facilitating" attacks is necessary to preserve the spirit of neutrality.

PROPORTIONALITY

Under the principle of proportionality, an attack is prohibited if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" as stated in Article 51(5)(b) of AP I. Article 57 of AP I similarly requires that attackers "refrain from deciding to launch an attack which may be expected to cause incidental [but] excessive [losses] in relation to the concrete and direct military advantage anticipated." The Rome Statute incorporates proportionality within its enumeration of particular crimes. Article 8(2)(a)(iv) references "extensive destruction not justified by military necessity" and Article 8(2)(b)(iv) states that "intentionally launching an attack in the knowledge that such attack will cause incidental loss or damage would be clearly excessive in relation to the concrete and direct overall military advantage anticipated."

Proportionality applies to the indirect effects of an attack as well. For instance, a cyber-attack is responsible for the indirect effects on a civilian population caused by an attack on the control system of an electrical generator. Some attacks have such dangerous indirect effects that they are prohibited (Gervais 2012: 572). As stated in Article 56 of AP I, "works or installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations, shall not be the object of an attack, even where those objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."

There are challenges, of course, in determining whether a cyber-attack can meet the necessary requirements to be considered lawful. For example, without a mechanism to reverse an attack, cyber-

attacks do not allow a target to surrender. Unlike an attack that uses a human operator who can assess changed conditions, a cyber-attack that is unleashed into the cyber environment without the ability for recall cannot take into account a targeted state's desire to surrender (Gervais 2012: 572).

OTHER PRINCIPLES OF IHL

The relationship between IHL and cyber warfare is not limited to the core principles of IHL which have been discussed above. There are other principles of IHL which are necessary to be made applicable to cyber warfare.

As far as persons are concerned, legitimate military targets include combatants, members of organized armed groups and civilians directly participating in hostilities. Civilians, medical and religious personnel, and combatants *hors de combat*—due to wounds, sickness, capture, surrender or any other reason—must be spared and protected. As far as persons in cyber space are concerned there are certain key issues. For example, how does the obligation of combatants "to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack" play in cyberspace ? Does it mean that hackers or non-state actors have to wear a uniform even they are not on a battlefield ? It is clear that these and other questions need urgent clarification if civilians exposed to cyber warfare are to receive the protection they are entitled to under treaty and customary law. In the meantime, it may have to suffice to recall that, in case of doubt, any person must be presumed to be a civilian and, as such, protected against direct attack as per the Article 50(1) of AP I.

Other cyber-specific problems which need to be addressed include the question of how the computer-controlled systems of medical installations, transports and logistics such as hospitals, ambulances, ships and aircraft could be marked so as to ensure they are respected and appropriately protected from infection with malware and other hostile cyber operations. Similar problems also arise with regard to other specially protected objects (such as works and installations containing dangerous forces, objects indispensable to the survival of the civilian population, cultural objects and of places of worship and the natural environment) and areas (most notably non-defended localities and de-militarized zones).

The term "*levée en masse*" as mentioned in Article 4(6) of GC III refers to the inhabitants of a non-occupied territory who, on the approach of the enemy, spontaneously take up arms to resist the invading forces without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war. In cyber warfare, territory is neither invaded nor occupied, which may significantly prolong the period during which a *levee en masse* can operate. Also, cyber space provides an ideal environment for the instigation and non-hierarchical coordination of spontaneous, collective and unorganized cyber defence action by great numbers of "hacktivists". The only question is, of course, how the requirement to "carry their arms openly" should be interpreted in cyber space.

KEY ISSUES AND CHALLENGES

There are many issues involved in the application of IHL to cyber warfare. The complexity has emerged due to the complex nature of cyberspace and the existing unrevised laws of war.

The cyberspace is shared by military and civilian users, the key challenge is whether it is feasible to ensure that attacks are directed against military targets only and that great care is taken to spare the civilian infrastructure and population. The next issue is with respect to hackers, that is whether hackers are legitimate targets in cyberspace. This is a grey area as far as cyber warfare is concerned. Most hackers are civilians who remain protected by IHL against direct attack but they would remain subject to law enforcement and criminal prosecution depending on their activities violated other branches of law. One possible answer to this question is, if hackers take a direct part in hostilities by way of a cyber-attack in support of one party in an armed conflict then they should be legitimately targeted like other military personnel in an armed conflict.

Another major issue in cyber warfare is of holding people liable for cyber-attacks. War crimes have been defined under international law. War crimes should also be recognized in cyberspace. War crimes in cyberspace should be brought at the same level with the war crimes in traditional conflicts. Commanders and superior military officers should be held criminally responsible for ordering cyber operations that constitute war crimes. The International Criminal Court should extend its jurisdiction to try cyber war crimes. If such commanders and military officers are from the regular armed forces of a state then such state should be held liable for such crimes. Such a state can be made liable to pay compensation if its armed forces commit cyber war crimes. Dedicated International Criminal Tribunals for cyber crimes can be established to try cyber war crimes.

TOWARDS SOLUTIONS

The above mentioned issues will have to be resolved systematically. Ideally there should be a new protocol added to the Geneva Conventions of 1949 with respect to cyber warfare and cyber operations. But as Protocols are optional, it is difficult to say how many states will ratify the protocol and adhere to the same. A new treaty document is one way to regulate the cyber warfare. But such treaty should be comprehensive and exhaustive. The treaty should provide clear definitions of cyber warfare, cyber operations and cyber-attacks. For an applicable legal regime to be drafted in some way, there must first be an agreement between nations about what constitutes a cyber attack. Not until a universally accepted definition has been established, will development towards an international framework to govern cyber warfare be seen. The treaty should provide concrete rules with respect to state responsibility relating to cyber warfare. There should be provisions with respect to neutrality in cyberspace. It is possible with such a dedicated treaty to rectify the lacunas in IHL and international law with respect to cyber warfare. Such a treaty can provide the exact definition of the concept of use of force with respect to cyber warfare. The treaty can be used to lay down prohibitions against use of force, as existing principles of international law with respect to use of force are very complicated and insufficient when it comes to their application to cyber warfare. Instead of making a separate treaty for non-international armed conflict, one single treaty should govern the international and non-international armed conflict with respect to cyber warfare. Status of combatants in cyberspace is a grey area as far as IHL is concerned. Such a treaty could provide definite rules in this respect. It is also needed to protect civilian and civilian infrastructure. The Tallinn Manual can provide good guidelines with respect to drafting of a new cyber warfare treaty.

In the light of the dangers that cyber warfare poses to civilian infrastructure, two solutions can be proposed. The first solution is for states to make declaratory statements about digital safe heavens. These are civilian targets that they will consider off-limits in the conduct of cyber operations just like the demilitarized zones foreseen in Article 60 of AP I. The second solution is to expand the list of 'works and installations containing dangerous forces' in Article. 56 of AP I. This could apply to specific cyber infrastructure components such as major internet exchange nodes of central servers on which millions of important civilian functions depend. They could not be made the object of attack even if they constituted military objectives because of the danger to civilian population would outweigh the military advantage attacking them (Droege 2012: 577).

As far as the core principles of IHL are concerned, cyber warfare should be conducted to serve the principle of military necessity. Combatants should spare civilians and their objects. And as far as objects having dual purpose, effective assessment should be made in light with the principle of proportionality. Another question is how to determine if a cyber-attack has occurred. There needs to be consensus among nations so that there is a definitive answer to when a cyber-attack has occurred and how much damage must occur in order for it to be called as such.

CONCLUSIONS

The main aim of IHL is to regulate warfare as to avoid any harm to civilians and non-combatants. But IHL needs support from the global community in achieving this in the sphere of cyberspace. Cyber-attacks have proved their deadly capacity to be employed as effective weapons and cyber-attacks are here to stay. It is up to the global community and IHL to stop the future generations from the horrors of cyber warfare. Computers and technology will only improve as time progresses, which is why the legal grey area of cyber warfare should be clarified in order to help nations understand and comply with international rules that will limit the potential harm that cyber weapons can have.

REFERENCES

1. Boothby, William H. (2013) "Methods and Means of Cyber Warfare", *International Law Studies,* Vol 89, pp 387-405.

2. Droege, Cordula (2012) "Get off my cloud: cyber warfare, international humanitarian law and the protection of civilians", *International Review of the Red Cross,* Vol 94, No 886, pp 533-578.

3. Fenrick, William J. (1990) "The Conventional Weapons Convention: A Modest but Useful Treaty," *International Review of the Red Cross,* No 279, pp 498-509.

4. Gervais, Michael (2012) "Cyber Attacks and Laws of War", *Berkeley Journal of International Law,* Vol 30, pp 525-579.

5. Hathaway, Oona A and Crootof, Rebecca (2012) "The Law of Cyber-Attack", *California Law Review,* Vol10, pp 817-885.

6. Lin, Herbert (2012) "Cyber Conflict and International Humanitarian Law", *International Review of the Red Cross*, Vol 94, No 886, pp 515-531.

7. Melzer, Nils (2011), *Cyber Warfare and International Law*, <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

8. Pool, Philip (2013) "War of the Cyber World: The Law of Cyber Warfare", *International Lawyer*, Vol 47, pp 299-323. (2013).

9. Schmitt, Michael N. (ed) (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York: Cambridge University Press.

10. Shakarian Paulo, Jana Shakarian and Andrew Ruef, (2013): *Introduction to Cyber Warfare: A Multidisciplinary Approach*, Massachusetts: Elsevier.