INTERNATIONAL CYBER LAW 2019- CYBER WARFARE IN CONTEXT OF INTERNATIONAL HUMANITARIAN LAW

By Vishakha Chaudhary
From UILS, PU

"*Cyber war takes place largely in secret, Unknown to the general public on both sides"*

.Noah Feldmen

In January 2010, inspectors with the International Atomic Energy Agency while visiting the Natanza Uranium Enrichment Plant in Iran noticed that, centrifuges used for enriching the uranium gas were failing at an unprecedented rate. The cause was a mystery, apparently for the Iranian technician. After five months a computer security firm was called to troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. The cause of this was again a mystery, until the researchers found some malicious files in one of the computer systems and discovered the world's first digital weapon Stuxnet.

Stuxnet worm was malicious software designed to infiltrate the factory computers. The virus was extremely effective in delaying the Iran's nuclear program for the development of nuclear weapon. It is said that over fifteen Iranian facilities were attacked and infiltrated. And it all started with a random workers USB drive. It still remains unknown who was behind the Stuxnet attacks[1], although fingers have been pointed to the United States and Israel.[2]

CYBER WARFARE - INTRODUCTION

As far as the definition of Cyber war fare is concerned there are number of definitions but no single definition is widely accepted internationally. Still it is worthy to state the position of International Committee of Red Cross in the context of 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"[3]
Also Richard A Clarke, former special advisor to the National Security Council on cyber issues defines cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[4]

'Cyber-attack' is a wide term which can be referred as computer network attack (CNA)[5],or computer network exploitation (CNE)[6].The nature of cyber attack highly

[1] Tallinn Manual, Commentary to Rule 22, note 14 page 83.
[2] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", New York Times (01 June2012)http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacksagainst-iran.html?
[3] Cyber warfare and international humanitarian law, p. 2 available at http://www.icrc.org/eng/.
[4] www.wikipedia.org/cyber warfare.html last visited 11th june,2018.
[5] See the NATO GLOSSARY OF TERMS AND DEFINITIONS (2013): CNA is defined as 'Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself'.
[6] Ibid. CNE is defined as 'Action taken to make use of a computer or computer network, as well as the

depends upon the various ways it is conducted , their consequences and also the skill of the attacker. Cyber warfare can present a multitude of threats towards a nation. At the most basic level, cyber attacks can be used to support traditional warfare[7]. The attacker can overload a server with an ultimate goal of shutting down the network system, which makes it a Denial of Service Attack or can also send a malware[8] to the system with intent to erase all the information contained in the hardware. Cyber Espionage, not being an act of war can also create serious tension between nations and are usually described as cyber attack.

Cyber Attack is a term with special meaning in International Humanitarian Law, and differs from other branches of law[9].Under Additional Protocol 1 (AP 1)Article 49[10], attacks mean 'acts of violence against the adversary, whether in offence or in defense'. The Tallinn Manual 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'[11]. A cyber operation is defined as 'the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'[12]. The main objectives behind these definitions are to differentiate cyber operation from cyber attack as all the cyber operations cannot be considered as cyber attack. It draws a line between the operations that results in inconvenience, and the ones that harms the target.

CYBER WARFARE AND ITS RELATION WITH INTERNATIONAL HUMANITARIAN LAWS

As increasingly more attacks are conducted by the nations against each other, the cyber warfare has taken the international spotlight, but the most important point is that there is lack of set of International laws which can regulate this new warfare species. Also the countries are perplexed with the questions as to whether follow the International laws of armed conflict to tackle cyber warfare and if so, till what extent these established rules regarding armed conflict can accommodate this new kind of war.

As we know, International Humanitarian Law (IHL) deals 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 inhumanely during times of war[13].

information hosted therein, in order to gain advantage'.

[7] www.wikipedia.org/cyber warfare.html last visited 11th june,2018.

[8]The Tallinn Manual's glossary defines malware as Instructions and data that may be stored in software,
firmware, or hardware that is designed or intended adversely to affect the performance of a computer system.
Page 260.

[9]Knut Dörmann in "Applicability of the Additional Protocols to Computer Network Attacks" page 3.

[10] Additional Protocol 1 OF 1977 – "Protocol Additional to the Geneva Conventions of 12 August 1949"

[11]Rule 30 of "the Tallinn Manual", page 106

[12] Tallinn Manual page 258

[13] Ayalew, Y. E. (2015). "Cyber Warfare: A New Hullaballoo under International Humanitarian Law". Beijing Law Review, 6, 209-223. http://dx.doi.org/10.4236/blr.2015.64021

The International Criminal Court (ICC) was established in 1988 under the Rome Statute with the objective of repressing war crimes and cases related to International Humanitarian Laws. In the 21st century, cyber warfare is also a part of military warfare concept as it can be equally destructive by using network system instead of conventional weapons and satellites providing more information than human spies. No international community has so far accepted publicly that any cyber attack has reached the threshold of armed attack.

There is no treaty that specifically deals with the cyber warfare under the International laws, there a number of sources which can be used like the customary international laws and general principles of law. However the problem is considered and discussed in various summits. The Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) is a nonbinding manual on the law governing cyber warfare. In 2009, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE) invited an 'International Group of Experts' (henceforward 'the experts') to produce a nonbinding manual on the law governing cyber warfare[14].

The experts were legal practitioners, academics and technical experts. Three organizations were invited as observers, NATO's Allied Command Transformation, the US Cyber Command and the International Committee of the Red Cross. The observers could participate in all discussions, but the unanimity that was required for adoption of a Rule was limited to the experts[15]. The manual is not an official document but is considered as a persuasive document.

Besides, as far as dealing with International Humanitarian Laws, it is important to distinguish between jus ad bellum (rules for when states can go on war) and jus in Bello (rules of conduct of war). Article 2(4) and article 51 of the U.N Charter governs the use of force regarding jus ad bellum. According to it no state can resort to the use of force, besides in self defense or when the use of force in authorized by the Security Council. International Humanitarian Law does not consider the cause behind the armed conflict, whether it is just or not, it only limits the sufferings for those involved and the destructive effects of the conflict.

If IHL is to be applied, there has to be an armed conflict. Armed Conflict refers to international and non –international conflict. Various treaties and customary laws will apply depending upon the type of conflict. It means that a cyber attack would have to be deliberate in nature, and should amount to armed conflict.

The experts of the Tallinn Manual agreed that a cyber-attack has the potential to amount to 'armed force'. The applicability of the law of armed conflict to cyber-attacks is expressed in Rule 20 of the Manual which provides that "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict"[16]. ICRC explains Cyber warfare as any hostile measure taken against an enemy designed "to discover, destroy, disrupt, alter, destroy, disrupt or transfer data kept in a computer, which is manipulated through a computer or transmitted through a

[14] Tallinn Manual - page 1

[15] Tallinn Manual pages 6-10.

[16] Tallinn Manual Rule 20 page 75.

computer network"[17]. Simply it is an attack based on networks which is adopted by many countries to reduce their frustration and also to avoid the real war situation. Chinese attack on US, Chinese attack on Google, attack by Ghost net spyware network upon confidential information of more than 100 countries are the examples which introduces the concepts of cyber warfare. Facebook has taught us that some-one is always watching our activities, but it is always acceptable when it is not a big boss[18]

IHL doesn't specifically mention cyber warfare, the Martens clause[19] which is associated with accepted principle of IHL, says that whenever a state of affairs isn't coated 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".

Also it is the work of ICRC to look into the developments that need to be incorporated in IHL. Article 36 of I protocol to the Geneva Conventions provides that, "in the study, development, acquisition or adoption of a brand new weapon, means that or methodology of warfare, a High contracting Party is below associate obligation to see whether or not its employment would, in some or all circumstances, be prohibited by this Protocol or by the other rule of jurisprudence applicable to the High Contracting Party." It means that , through general rules it regulates the legitimacy of all means and strategies of warfare. This rule also shows that general IHL rules apply to new technology.

However, there are still arguments' inclining to the position that IHL provisions do not specifically mention cyber operations. Because of this, and because the exploitation of cyber technology is relatively new and sometimes appears to introduce a complete qualitative change in the means and methods of warfare, it has occasionally been argued that IHL is ill adapted to the cyber realm and cannot be applied to cyber warfare[20]. It is noted that, the absence in IHL of specific references to cyber operations does not mean that such operations are not subject to the rules of IHL. New technologies of all kinds are being developed all the time and IHL is sufficiently broad to accommodate these developments[21]

The Tallinn Manual defines a cyber-attack as a 'cyber operation… that is reasonably expected to cause injury or death to persons or damage or destruction to objects'[22], but it does not describes as what classifies as 'damage' to an object. The majority of the experts were of the view that interference with functionality qualifies as damage if restoration or functionality requires replacement of physical components, but were split over whether the 'damage' requirement is met when functionality can be

[17] Legal Vacuum in Cyber Space, International Committee of the Red Cross, available at http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, last visited 11 june 2018

[18] Geneva Convention III, art. 4A they are entitled to this status as soon as they fall "into the power of the enemy". Id. arts. 4A, 5

[19] see http://en.wikipedia.org/wiki/Martens_Clause

[20] Charles J. Dunlap Jr., "Perspectives For Cyber Strategists On Law For Cyber War", In Strategic Studies Quarterly, Spring 2011, p. 81.

[21] www.wikipedia.org/cyber warfare.html last visited 11th june,2018.

[22] Tallinn Manual Rule 30 page 106

restored by reinstalling the operating system.[23] A few experts suggested that it does not matter how an object is disabled, and that it is the object's loss of usability that qualifies as 'damage'[24]

It is the violent result of a cyber attack that determines whether IHL will be applied or not. For instance, if a cyber operation is conducted on the civilians of a state, and creates inconvenience which is not harmful in nature, will not come under the ambit of cyber attack that triggers the application of IHL. However, if a cyber operation is conducted on the civilians, and the consequences are violent causing damage and injury to the civilians, it will trigger the IHL. The main focus of IHL is to protect the people from any harm who are not the part of conflict, but it does not protect from inconvenience. Also, it is worth noting that most academics point out that the meaning of the legal term may shift over time, and that new treaties, new customary law norms might develop and give new understanding to the meaning of cyber-attacks.[25]

CYBER ATTACK IN CONTEXT OF CIVILIANS

As already mentioned, the main focus of IHL is to limit the sufferings of the civilians who are affected by a armed conflict. IHL prohibits the attack on civilians and civilian objects. The basic rules of IHL distinguish the civilians from combatants. It is considered customary international law that the parties to the conflict must distinguish between civilians and combatants.[26] AP 1 has codified this principle in Articles 48 and 51(2), which state respectively that: "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives".[27] And "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited".[28] Civilian objects shall also not be the object of attack.[29]

According to IHL, attacks can only be directed against military objectives, and civilians shall not be the object of attack.[30] This requirement applies to all the means and methods of warfare. IHL does not guarantees that civilians will be unaffected by the military operation, but also does not excuses the intentionally directing cyber attacks against civilians. It does not matter if the attack has the power to end the ongoing conflict for example by conducting cyber-attacks against a civilian leader's private property and damaging it to pressure him into capitulation.[31] Although protected from being made the object of attack, civilians will lose this protection if they directly participate in hostilities.

[23] Ibid. commentary to Rule 30, note 10, page 108-109..
[24] Ibid. commentary to Rule 30, note 11, page 109.
[25] See for instance Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context page 293, Melzer, Cyberwarfare and International Law page 36.
[26] ICRC Study on Customary International Humanitarian Law, Rule 1
[27] Ibid. Article 48.
[28] Ibid. Article 51(2).
[29] Ibid. Article 52(1).
[30] Additional Protocol 1 Article 48 and 52(2).
[31] Example from the Tallinn Manual, commentary to Rule 31, note 6.

Civilians are protected against attacks by virtue of being a civilian. They are per definition not a member of the armed forces, and are non-combatants.[32] IHL strives to offer them protection, and they are protected from direct attack and against the dangers arising from military operations[33]. IHL does not ban civilians from participating in the armed conflict, but does set out consequences for doing so. If a civilian takes a direct part in the hostilities, he or she will lose their protection for such time as he partakes in the hostilities.[34] Those attempting to be 'farmers by day and fighters by night' lose protection from attack even in the intermediate time-frames punctuating military operations, if they assume a continuous combat function[35]. The same rationale applies if an individual joins an organized armed group that partakes in hostilities, he would lose civilian protection for as long as that membership lasts, and may be targeted, even when not personally linked to any specific hostile act—simply due to his membership in such a group—as long as that membership endures.[36] It means if a civilian joins a group of hackers that conduct cyber attack in armed conflict that will produce harmful effect will loose his protection under IHL.

Geneva Convention 3, Article 4A(6) provides for an exception for situations where a civilian can participate in an armed conflict, and qualify as combatant. That situation is referred to as 'levee en masse' and is considered a 'long-standing rule of customary international law'.[37] A levee en masse exists when "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.[38]

CASES IN A CYBER ATTACK PRESPECTIVE

The real world examples of cyber operation will be helpful to establish more clarity on what can be classified as a cyber attack and whether those attacks trigger the applicability of IHL.

Estonia

At the end of April 2007, riots broke out in Estonia by youth groups of mostly Russian origin, after the government had decided to remove a soviet-era Second World War memorial. Not long after the riots, on April 27 web pages of Estonian government institutions and news portals came under a wave of cyber operations that lasted for more than three weeks.[39]

The means of attack used in the April-May 2007 events included denial of service (DoS) and distributed denial of service (DDoS) attacks, defacement of governmental websites, and large amounts of comments and email spam. Public propaganda, distributed on different Internet forums, and dissemination of attack instructions were

[32] Ibid. Article 52 (1).
[33] Ibid. Article 51 (1) and (2).
[34] Ibid. Article 51(3).
[35] Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts" page 276.
[36] Ibid.
[37] It is also considered customary international law, see ICRC Study on Customary International Humanitarian Law 387.
[38] Geneva Convention 3, Article 4A(6).
[39] E Tikk, K Kaska and L Vihul, "International Cyber Incidents: Legal Considerations" page 15 and 16.

employed to encourage, coordinate and aid in carrying out the attacks.[40]
To prove that the attack was a cyber attack or armed conflict, the attack should be between governmental organization and organized armed group within the state, and the attack must resort to armed violence between states.

There was no proof that the Russian Federation was behind the attack, so on that basis it cannot be an International Armed Conflict. But if it would have been proved it still won't reach the threshold of an armed conflict as the intent of the attack was hostile but defacing of governmental websites, sending of spam emails and distributing propaganda does not fit with the definition of cyber-attacks which requires a certain level of damage. Such attacks did not reach the threshold of the international armed conflict and created inconvenience. The attack was illegal in nature but it did not triggered the applicability of IHL.

Wannacry Ransom ware Attack
On may 2017, a worldwide attack occurred which bought the cyber warfare attack again in the lime light. It was Wannacry Ransom Ware attack, which made the world realize that how much the cyber attack has developed and the magnitude of destruction it can cause.
The Wannacry Ransom Ware attack began on Friday 12 may, 2017, which effected between 2,30,000 to 3,00,000 computers in over 150 countries by encrypting computer files and demanding ransom from users in order to restore it. Later United States, United Kingdom asserted North Korea was behind the attack. For the sake of arguments if it is assumed that the attack was attributable to North Korea, can it trigger the IHL? There are mainly two questions to be dealt with. First being was the attack destructive and injurious and second, did the attack intervene into other states internal and external affairs.

The Wannacry attack falls into a grey zone in which the threshold for violation remains unsettled. It did disrupted many services like health care that could reasonably be viewed as use of force and with respect to sovereignty it did violated the sovereignty of a number of states, particularly in light of the significant disruption of functions like law enforcement.

STATE ATTRIBUTION
For the application of IHL, the degree of state responsibility should be proved. The most difficult task in the cyber warfare is to link an attack to a state. The ICJ and ICTY through various cases have tried to illustrate the different approaches with regard to attribution of state responsibility based on control test.

Effective Control Test
In the Nicaragua case[41] the ICJ dealt with the question of whether Nicaraguan rebels could be considered to be acting on behalf of the United States. The Court held that the financing, organizing, training, supplying and equipping the rebels was not enough. In order for the US to be responsible, the rebels either had to be so completely dependent on them that they had to be considered state organs,[42] or the US had to have held

[40] Ibid. Page 20.
[41] Military and Paramilitary Activities in and against Nicaragua,1986.
[42] Ibid. Para 109.

'effective control of the military or paramilitary operations in the course of which the alleged violations were committed'.[43] Under ICJ's control test, for a State to incur responsibility it would have to exercise control over the non-state actors that launches the cyber-attacks.

Overall Control Test

In Tadic (1999)[44], the ICTY looked at the legal conditions required for when individuals can be considered to act on behalf of a State. According to the ICTY logic dictates that the criteria for ascertaining responsibility is the same in the cases where the court wants to attribute the act of an individual to generate State responsibility, or whether the individuals are acting as de facto State officials, thereby rendering the conflict international and thus setting the necessary precondition for the "grave breaches" regime to apply.[45]

Since there are no specific legal criteria in IHL for when individuals can be said to work on behalf of a State and making it an international armed conflict, reliance must be had on the criteria for State responsibility.[46] The Tribunal did not, however, however find the Nicaragua test of 'effective control' to be persuasive. In its view, it did not hold up to the logic of State responsibility[47], nor with judicial and State practice.[48]

The ICTY distinguishes between the control needed for individuals and organised groups. If an individual is engaged by a State to carry out illegal acts, it is necessary to show that the State has issued specific instructions, or publicly given retroactive approval. A generic authority over the individual would not be sufficient.[49]

Acts of State Organs

It follows from ILC Draft Article 4 on State responsibility that 'A State is responsible for the actions of its organs'.[50] Under Article 7, such responsibility applies even if the organ exceeded their authority, or contravened instructions.[51] This is only logical, as a State is made up by its organs. the act of individuals that lacks the status of State organs may still be attributed to the State under international law. For example, Draft Article 8 states that a person or groups conduct shall be considered an act of a State if they are in fact acting on the instructions of, or under the direction or control of the State carrying out the conduct.[52]

Hacktivists

Hacktivists[53] are usually dealt with under criminal law, and generally are not sponsored by a State. Since a hacktivist would be an individual, it follows from the Tadic case that the State must issue specific instructions or publicly give retroactive approval.[54]

[43] Ibid. Para 115.
[44] Tadic Appeals Chambers 1999.
[45] Ibid. Para 104.
[46] Ibid. Paras 98 and 105.
[47] Ibid. Para 115.
[48] Ibid. Para 116.
[49] Ibid. Para 118.
[50] Draft Articles on State Responsibility Article 4, annexed in UN Res A/56/83.
[51] Ibid. Article 7.
[52] Draft Articles on State Responsibility Article 8, annexed in UN Res A/56/83.
[53] The Tallinn Manual's glossary defines a hacktivist as a person who gains or attempts to gain unauthorized access to hardware and/or software.
[54] "Tadic Appeals Chambers 1999", para 118. It also follows from the Draft Articles on State Responsibility

The Tadic judgment (1999) also talked about 'overall control' over organized groups. Organized groups will normally have a structure, a chain of command and a set of rules as well as the outwards symbols of authority.[55] The hacktivists must be organized in order to be a group. The fact that many hackers are attacking a State individually would not make them organized. If they are working under a leadership structure and operating cooperatively, things might be different.[56] If the hacktivists are organized, 'overall control' will be enough for attributing the conduct to the State. Individual hacktivists, however, require specific instructions to attribute the acts to the State.

CHALLENGES

With the emergence of this new warfare species there a few challenges which have to be dealt with. As cyber war is new and different from the traditional kinetic war the challenges and concerns are also different. The researcher has identified and noted the following critical issues as far as cyber warfare is concerned –

- Countries lack laws against cyber warfare and lack of enforcement coupled with low cost attack allows anyone or any state to initiate cyber-attacks.[57]
- As to the battlefield, there is only one cyberspace, shared by military and civilian users, and everything is interconnected. The key challenge is whether it is feasible to ensure that attacks are directed against military objectives only and that constant care is taken to spare the civilian population and civilian infrastructure.[58]
- Cyber warfare makes the application of the Principle of Distinction difficult.
- One of the biggest challenge of the cyber warfare in that the parties of the attack are not known and are unidentified.
- The other challenge is the inevitable Attitudinal and policy differences between major super powers as to cyber law treaty.
- Finally, there are no centralized monitoring mechanisms to govern cyber warfare so far.

RECOMMENDATIONS

The researches have provided some recommendation regarding the challenges and for the suggestions for the way forward. First of all, there should be comprehensive and well organized International legal machinery by enacting separate treaty document to govern cyber warfare.

And since, most of the hackers would be civilians and remain protected under the IHL against direct attack. It is recommended that the notion of direct participation in hostilities should be on case to case that is if hackers take a direct part in hostilities by way of a cyber-attack in support of one side in an armed conflict. In such a situation, the hackers will be legitimately targeted.

Article 8, which the ICJ deemed reflection of customary international law in the Genocide case, para 398.

[55] Tadic Appeals Chambers 1999, para 120.

[56] Tallinn Manual , Commentary to Rule 23, note 13, page 89.

[57] http://www.techrepublic.com/blog/it-security/cyberwarfare-characteristics-and-challenges/ last visited 12 june 2018.

[58] Ibid. Article 48.

CONCLUSION

The threat of cyber warfare is growing every day and it is important for the states to be aware of their responsibilities under International Humanitarian law, and recognize an established framework and rules applicable to it. Cyber attack has the potential of mass destruction and the states should be well are of it. With time more states are adding cyber attacks to their arsenal, which is leading to the establishment of elaborate and cleaner rules. In future, it is hoped that the sates will ban targeting the innocent civilians from cyber operations with context to International Humanitarian Laws.

*****