Beijing Law Review, 2015, 6, 209-223
Published Online December 2015 in SciRes. http://www.scirp.org/journal/blr
http://dx.doi.org/10.4236/blr.2015.64021

Cyber Warfare: A New Hullaballoo under International Humanitarian Law

Yohannes Eneyew Ayalew

School of Law, Samara University, Samara, Ethiopia
Email: enyewyohannes@gmail.com, yohanneseneyew@su.edu.et

Received 27 August 2015; accepted 12 October 2015; published 15 October 2015

Abstract

Cyber warfare is a new phenomenon and scenario under International Humanitarian law. This paper was basically portrayed the impact of cyber warfare in light with international humanitarian law and assessed the notion of cyber warfare, conduct of hostilities, legal framework, monitoring mechanisms as well as current challenges. Moreover, critical legal analysis is used as principal methodology. Major findings of the research revealed that there are plethora of issues to be underlined save as absence of binding treaty governing the challenging scenarios. Recommendations are made by suggesting points of improvement until the international community has agreed on this cross-cutting contemporary issue.

Keywords

Cyber Warfare, Hackers, Civilians, Combatants, Soft Law, International Humanitarian Law

1. Introduction

To begin with, the concept of cyber warfare is a new phenomenon under International Humanitarian law (here in after "IHL")[1]. Since the era of science and technology, the means and methods of warfare become more sophisticated and very much complex one interalia, the issue of cyber warfare is one of the current debatable issues as far as IHL is concerned[2]. The information revolution has fundamentally changed the way that wars are fought in the 21st C. Needless to say from actors' point of view, the strategies that parties adopted as well as the spread of technology in to all aspects of warfare is pervasive.

By similar fashion, technology now controls our daily lives to an unprecedented level from electricity generation, water supplies, communications and almost every aspect of our globalized world, making it increasingly

[1]The impact of cyber warfare under international humanitarian law; a critical legal analysis by Yohannes Eneyew; a senior essay see my unpublished thesis available at www.abyssinialaw.com/ p. 1.
[2]http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/ihl-new-technologies/index.jsp last visited 12-05-2014.

How to cite this paper: 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

vulnerable to computer attacks and other cyber operations during armed conflicts[3].

From conceptual point of view, cyber warfare is Internet-based attack involving politically motivated missions on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple financial systems…among many other possibilities[4].

On top of that, cyber warfare and its effect began to draw the attention of the international legal community among other things law schools in the late 1990s. Most significantly, in 1999 the United States Naval War College convened the first major legal conference on the subject[5].

In the aftermath of the attacks of 11th of September, 2001, terrorism and the ensuing armed conflicts diverted the attention of the world community from the topic until the massive cyber operations by "hackers" against Estonia in 2007 and against Georgia during its war with the Russian Federation in 2008, as well as cyber incidents like the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010[6].

Needless to mention, one of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defense, have remained unsettled since their advent.

After all, at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal regime[7].

The threshold questions are whether the existing law applies to cyber issues at all, and, if so, then how it could be? Views on the area range from a full application of the law of armed conflict as inferred from the International Court of Justice's[8] pronouncement that it applies to "any use of force, regardless of the weapons employed"[9], to strict application of the Permanent Court of International Justice's pronouncement that acts not forbidden in international law are generally permitted[10]. Of course, the fact that States lack definitive guidance on the subject does not relieve them of their obligation to comply with applicable international law in their cyber operations[11].

Surprisingly, almost all IHL treaties are known by their bad connotation called "one war behind reality" thus, due to that reason there were plenty of sufferings and superfluous injuries occurred in history of mankind[12]. In other words, in the past 150 years all most all IHL treaties were not stipulated in advance before those historically known wars had brought the unforgettable and immeasurable sufferings. Albeit; treaties were so far enacted after the drama of a certain warfare.

For instance, The 1929 Convention on the treatment of prisoners of war (POW Convention) was the result First World War (WWI) incident meaning that the POW Convention was enacted after mass killings of prisoners[13]. Surprisingly even the Four Geneva Conventions of 1949 were enacted after the scourges of Second World War (WWII)[14].

---

[3]Heather A. Harrison Dinniss, (2013) "Participants in Conflict—Cyber Warriors, Patriotic Hackers and the Laws of War" in Dan Saxon (ed) International Humanitarian Law and the Changing Technology of War (Leiden: Martinus Nijhoff), pp. 251-278.

[4]Definition from what Is.com available at http://searchsecurity.techtarget.com/definition/cyberwarfare last visit ed11dec, 2013.

[5]Cited on Tallinn Manual preamble; the proceeding was published as computer network attack and international law, 76 NAVAL WAR COLLEGE INTERNATIONAL LAW STUDIES (Michael N. Schmitt & Brian T. O'Donnell eds., 2002).

[6]ibid.

[7]ibid.

[8]International court of justice (ICJ) was established by UN charter served at world court since 1945 yet permanent court of international Justice (PCIJ) was established under the auspices of league of Nations ceased its service after 1945 glance at http://www.experts123.com/q/what-is-the-difference-between-the-pcij-and-the-present-international-court-of-justice.html last visited 12-05-2014.

[9]Cited on Tallinn Manual preamble Nuclear Weapons Advisory Opinion, para. 39.

[10]The Permanent Court of International Justice famously asserted that "[t]he rules of law binding upon States…emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims." Lotus Case at 18.

[11]For the view that the law of armed conflict applies to cyber warfare, see International Committee of the Red Cross, *International Humanitarian Law and Challenges of Contemporary Armed Conflicts*, ICRC Doc.

[12]Supra note 1.

[13]The number of soldiers imprisoned reached a little over seven million for all the belligerents, of whom around 2,400,000 were held by Germany and also German and Austrian populations literally starve under the British blockade—roughly 800,000 Germans die to starvation and starvation-related disease. Available at http://en.wikipedia.org/wiki/World_War_I_prisoners_of_war_in_Germany last visited 12-05-2014.

[14]The financial cost of World War II is estimated at about a $1.944 trillion US dollars worldwide, making it the most costly war in capital as well as lives. See generally http://en.wikipedia.org/wiki/Effects_of_war last visited 12-05-2014.

On top of that, now a day there is no binding legal framework under international law to govern and deal with cyber warfare. The only authoritative document that may question the above assertion if to be cited is Protocols Additional to The Geneva Conventions relating to the Protection of Victims of International Armed Conflicts (Protocol I) here in after "AP I" have even in this document, one can find only one provision which is phrased with terms of vagueness and more general articulations as it is stated[15].

As a result of this gap, the international community so far witnessed plethora of cyber incidents that could be cited as good indicators of how the issue is becoming a serious concern of the world community coupled with lenient and unregulated law on cyber warfare that is why then this paper intends to critically analyze the impact of this newly emerging threat to the world peace in the absence of organized legal framework under international law even to punish the alleged perpetrators of cyber warfare.

Finally, the researcher believes that the international community should attentively follow the impact of cyber warfare on IHL, and tried to delve in to various cross-cutting issues with regard to cyber warfare and pinpoints the nexus between cyber warfare and IHL.

2. The Notion of Cyber Warfare

As far as the notion of cyber warfare is concerned, it is worthy to reiterate the remarks of ICRC (International Committee of Red Cross) as a base to define cyber warfare[16].

Richard Clarke, former special advisor to National Security Council on cyber security issues and author of the book Cyber War, describes cyber warfare as "*actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.*"[17].

Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage[18]. As one can infer from the above suggested definitions, there is no agreed definition on the term cyber warfare albeit, various literatures opted to define it differently either directly or indirectly via cyber-attack. Similarly such understandings is reaffirmed in The Tallinn Manual[19].

For instance countries have their own standings towards cyber warfare, The United Kingdom outlined four different methods of cyber-attack in its national cyber strategy[20].

On the other hand, The United States also defines Computer Network Attack (CNA) as "*actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves*"[21].

One can make rehearsal of the following recent historical events as indicators that the world is already on the verge of witnessing this kind of warfare[22];

These examples of cyber-attacks show the legitimate threats that can emanate from this new domain. As the critical infrastructure of nations continually becomes more reliant on networks and cyberspace, the possible targets for cyber-attacks greatly increases. The researcher also observes other forms of cyber incidents yet the

[15]Ibid AP I, Arts 36 "In the study, development, acquisition or adoption of a new weapon, means and methods of war fare, a High Contracting party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this protocol or by any other rule of international law applicable to the High Contracting party."

[16]Cyber warfare and international humanitarian law: The ICRC's position "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." p. 2 available at http://www.icrc.org/eng/.

[17]Richard Clarke, Cyber war (HarperCollins, 2010).

[18]www.wikipedia.org/cyber warfare.html last visited 15 January 2014.

[19]Supra note 10, Rule 32 "A cyber-attack is a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."

[20]UK Cabinet Office, The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world: *electronic attack, subversion of supply chain, manipulation of radio spectrum, disruption of unprotected electronics using high power radio frequency* 13-4.

[21]US Joint Chiefs of Staff, Joint Publication 3-13. Information Operations.

[22]See http://searchsecurity.techtarget.com/definition/cyber warfare; In 1998, the United States hacked into Serbia's air defense system to compromise air traffic control and facilitate the bombing of Serbian targets. In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries. Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information. In 2009, a cyber-spy network called "Ghost-Net" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. Ghost-Net was reported to originate in China, although that country denied responsibility and finally in 2013, Germany revealed the existence of their 60-person computer network Operation unit. The German Intelligence agency, BND, announced it was seeking to hire 130 "hackers" for new cyber defense station unit. See also Cyber-warfare: Are we ready? By: Nina Levarskapp 1.

above are critical and officially acknowledged. The irony is that those nations like the United States and its NATO Allies that have the capacity to excel in cyber war as an adjunct to military operations and can achieve information dominance over the Battle field are also those most vulnerable to unrestricted cyber wars. There are, however, measures that can be taken to reduce these vulnerabilities[23].

Cyber warfare is not fundamentally different from conventional, physical warfare. When conducted by a nation state, it is integrated into a defined strategy and doctrine, becomes part of military planning and is implemented within specific parameters. Consequently, it is subject to analysis and warning in much the same way as other military operations. Indeed, there are several ways of reducing vulnerability to cyber war.

These include anticipation and assessment, preventive or deterrent measures, defensive measures and measures for damage mitigation and reconstitution.

Therefore the most sensitive point here is, Cyber warfare took the international spotlight as increasingly more attacks are conducted by countries against one another, whereas there exists no set of international laws of war regulating this new warfare species. Countries are perplexed by the string of questions as to whether this kind of warfare is indeed to be regulated with the established law of armed conflict and, if so, to what extent can these rules—established back in times of considerable old—accommodate this very modern war.

These questions remain paramount on the bucket list of the General Assembly. In the handful of times it addressed the aspects of cyber warfare, not once has the General Assembly spoken in unanimity on how to handle cyber warfare via concerted effort and, most especially, united rules of international law. It is hoped that in this 2015 session the Assembly will be able to sufficiently address these persistent challenges and decide on what is best, as well as what is first, to be solved in the context of cyber warfare[24].

3. The Nexus between Cyber Warfare and International Humanitarian Law (IHL)

To begin with, the nexus between international humanitarian law and cyber warfare now a day is interwoven and interconnected.

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

The International Humanitarian law has banned the use of many weapons, which includes ex-ploding bullets, chemical and biological weapons, blinding laser weapons and anti-personnel mines.

The International Criminal Court (ICC), with the objective of repressing inter alia war crimes, was created by the 1998 Rome Statute to try cases relating to IHL. The ongoing 21st century is the Era where several new military warfare concepts have emerged. The concept of Cyber warfare is one of them. Where computer networks are used for cyber-attacks instead of conventional weapons; and satellites are used for providing images far more detailed than human spies and reconnaissance units have ever offered.

However, as Cyber technology is the new phenomena in the 21st century, IHL faces the new challenge of addressing ethical standards for war in cyber space. Though the obvious wars on land, sea, and air may be claimed as issues covered by the existing rules and customs of warfare, cyberspace is undefined. While cyberspace itself is non-physical, it is a critical infrastructure that can greatly affect the physical world. Logic bombs and computer viruses can disrupt everything from electric grids and the stock market to nuclear power plants and water treatment facilities.

Besides, As far as the nexus between IHL and Cyber warfare is concerned, it is worthy to reiterate the central themes of humanitarian laws; Interalia. *Jus in bello*, conjointly called the law of war, the law of armed conflict (LoAC) or international humanitarian law (IHL)[25] is the section of law of nations handling the protection of persons who are not any longer collaborating within the hostilities which restricts the means and strategies of warfare. It includes written agreement law and customary law, because the latter has been crystallized through-

[23]Ibid p. 3.

[24]UN General Assembly Study Guide; cyber warfare 2013, p. 1

[25]Glance at, The Law of Armed Conflict: Constraints on the Contemporary Use of Military Force By Howard M. Hensel; The Law of Armed Conflict: International Humanitarian Law in War By Gary D. Solis; International law and armed conflict: exploring the fault lines: By Michael N. Schmitt, Jelena Pejic, Yoram Dinstein; The conduct of hostilities under the law of international armed conflict By Yoram-Dinstein; The contemporary law of armed conflict By Leslie Green; The law of war By Ingrid Detter.

out history[26].

Treaty law consists primarily of two sets of IHL legal package: that is Hague Conventions and Geneva Conventions. The first one, Hague Conventions deals with sensible military aspects of the conduct of hostilities, consisting of city rules of 1899 and 1907, plus numerous other conventions and agreements prohibiting the employment of sure weapons and military tactics.

The second one, Geneva Conventions concentrates on the protection of civilians, prisoners of war, wounded and sick toward land and sea, comprising of the four 1949 Geneva Conventions[27].

Further Protocol III was added in 2005 regarding the Adoption of a further Distinctive Emblem[28].

International law is a body of rules and regulations governing the relation between various states and International Humanitarian law is just a part of it, which applies to armed conflict.

It covers two areas:

- The protection of those who are not a part or not a party to conflict.
- Restrictions on the means of warfare—in particular weapons and the methods of warfare, like military tactics.

International Humanitarian Law protects those who are not taking part in the fighting, like civilians and medical and religious military personnel. International Humanitarian Law prohibits all means and methods of warfare which fails to discriminate between those taking part in the fighting and those, such as civilians, the purpose being protecting the civilian population, individual civilians and civilian property;

- Cause injury which results into unnecessary sufferings and;
- Cause severe and permanent damage to the environment[29].

Cyber warfare has been explained 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 computer network"[30]. 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[31].

Contemporary armed conflicts are to be controlled by a body of law by which came in to existence as binding and relatively comprehensive document in the second half of the 20th century and which have not yet become adaptable to contemporary legal as well as practical challenges introduced by new technologies of warfare interalia cyber warfare.

Some scholars like **Cordula Droege**, a legal expert of International committee of Red Cross (ICRC), explain that the existing legal framework is applicable and must be respected even in the cyber realm[32].

The researcher on the other hand argues it is very difficult to apply the existing IHL legal regime to cyber realm because the technicality of the subject matter results in non-compliance.

The following is an overview of weapons that are regulated by IHL treaties[33].

[26]ICRC has contributed with a recent customary IHL database published with the results of research on customary humanitarian law conducted in 2005, available at www.icrc.org/customaryihl.html last visited 15 January, 2014.

[27]Supplementary to earlier Conventions of 1846, 1906 and 1929. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949 [GC I]; see also Jean Pictet (ed.), Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva, 1952; Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949 [GC II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949 [GC III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949 [GC IV]. It's more complemented by the two further Protocols of 1977, regarding the protection of victims of international and non-international armed conflicts. i.e. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977 [AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977 [AP II].

[28]Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem, December 8 2005 [AP III].

[29]WWW.INTERNATIONAL%20HUMANITARIAN%20LAW%20AND%20NEW%20WEAPON%20TECHNOLOGIES%20_%20LAW%20MANTRA.htm Last visited 15 January 2014.

[30]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 15 January 2014.

[31]Supra note 44.

[32]Codula Droega, "Elective affinities? Human rights and humanitarian law", 30-09-2008 Article, International Review of the Red Cross, No 871, published on 30-09-2008.

[33]International humanitarian law contains basic principles and rules governing the choice of weapons and prohibits or restricts the employment of certain weapons. The ICRC plays a leading role in the promotion and development of law regulating the use of certain weapons. See http://www.icrc.org/eng/war-and-law/weapons/overview-weapons.htm last visited16-05-2014.

Weapon	Treaty
Explosive projectiles weighing less than 400 grams	Declaration of Saint Petersburg (1868)
Bullets that expand or flatten in the human body	Hague Declaration (1899)
Poison and poisoned weapons	Hague Regulations (1907)
Chemical weapons	Geneva Protocol (1925)
	Convention on the Prohibition of Chemical Weapons (1993)
Biological weapons	Geneva Protocol (1925)
	Convention on the Prohibition of Biological Weapons (1972)
Weapons that injure by fragments which, in the human body, escape detection by X-rays	Protocol I (1980) to the Convention on Certain Conventional Weapons
Incendiary weapons	Protocol III (1980) to the Convention on Certain Conventional Weapons
Blinding laser weapons	Protocol IV (1995) to the Convention on Certain Conventional Weapons
Mines, booby traps and "other devices"	Protocol II, as amended (1996), to the Convention on Certain Conventional Weapons
Anti-personnel mines	Convention on the Prohibition of Anti-Personnel Mines (Ottawa Treaty) (1997)
Explosive remnants of war	Protocol V (2003) to the Convention on Certain Conventional Weapons
Cluster munitions	Convention on Cluster Munitions (2008)

Even though IHL doesn't specifically mention cyber warfare, the **Martens clause**[34], that 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".

In fact, it is the role of ICRC to look into the valid developments that need to be incorporated in IHL. Generally speaking, it shall be taken for granted that new scenarios of warfare are not far-flung from IHL regulation.

However it also regulates, through its general rules, the legitimacy of all means and strategies of warfare, as well as the employment of all weapons. specifically, 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."

On the far side the precise obligation it imposes on States parties, this rule shows that general IHL rules apply to new technology.

Unless IHL addresses specific guidelines for warring nations to follow in cyberspace, civilians and non-combatants could be seriously endangered in the event of cyber-war[35].

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[36].

But one has to note 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[37].

[34]The clause took its name from a declaration read by **Fyodor Fyodorovich Martens**, the Russian delegate at the Hague Peace Conferences 1899 and was based upon his words: "*Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.*" see http://en.wikipedia.org/wiki/Martens_Clause last visited 21-05-2014.

[35]International Humanitarian Law for Cyber warfare; Max Blumenthal School of International Service The American University 4400 Massachusetts Ave NW Washington, DC 20016.

[36]Charles J. Dunlap Jr., "Perspectives for cyber strategists on law for cyber war", in Strategic Studies Quarterly, Spring 2011, p. 81.

[37]Supra note 15, p. 8.

IHL prohibits or limits the use of certain weapons specifically (for instance, chemical or biological weapons, or anti-personnel mines). Beyond the specific obligation it imposes on states party to Additional Protocol I, this rule shows that IHL rules apply to new technology.

Now the researcher raises the issue that should International Humanitarian Law **in black and white** applies to Cyber warfare or not?

At this juncture it is worthy to reiterate the notion that IHL is only applicable if cyber operations are conducted in the context of and related to an armed conflict. Thus, there is a fast and hard rule that when cyber operations are conducted in the context of an ongoing armed conflict they are governed by the same IHL rules as that conflict: for instance, if in parallel or in addition to a bomb, Airplane or missile attack, a party to the conflict also launches a cyber-attack on the computer systems of its adversary.

However, a number of operations referred to as cyber warfare may not be carried out in the context of armed conflicts at all. Terms like "cyber attacks" or "cyber terrorism" may evoke methods of warfare, but the operations they refer to are not necessarily conducted in an armed conflict. Cyber operations can be and are in fact used in crimes committed in everyday situations that have nothing to do with war[38].

In a nut shell, the researcher argues IHL will apply to cyber operations that are conducted within the framework of an ongoing international or non-international armed conflict in addition to kinetic operations.

4. The Legal Framework

4.1 The Conduct of Cyber Attacks

As we know the customary international law of IHL does not prohibit any civilian from participating in an armed conflict, whether international or non-international. It should be noted that Additional Protocol I[39] provides that "*members of the armed forces of a Party to a conflict* (*other than medical personnel and chaplains covered by Article* 33 *of Geneva Convention III*) *are combatants, that is to say they have the right to participate directly in hostilities*". This provision, applicable in international armed conflict, confirms that combatants enjoy immunity in respect of the acts undertaken a part of the hostilities. It does not prohibit others from engaging in those hostilities.

Besides, the Tallinn Manual with regard of the conduct of hostilities stipulates "*the law of armed conflict does not bar any category of person from participating in cyber operations. However, the legal consequences of participation differ based on the nature of the armed conflict and the category to which an individual belongs*" [40].

Needless to mention, the generally accepted understanding of combatant derives from the Hague Regulations[41]. Geneva Convention III adopts this standard in Article 4A with regard to the entitlement to prisoner of war status[42]. Although Article 4A (1), (2), (3), and (6) is textually applicable only to such status, it is universally understood as reflecting the customary international law criteria for being combatant. The notion of combatant is limited to international armed conflict; there is no non-international armed conflict equivalent of either prisoner of war status or combatant immunity rather those who have participated in non-international armed conflict will face criminal prosecution.

On top of that the soft-law or Tallinn Manual provides vividly in an international armed conflict, *members of the armed forces of a Party to the conflict who, in the course of cyber operations, fail to comply with the requirements of combatant status lose their entitlement to combatant immunity and prisoner of war status*[43].

Moreover, Combatants are entitled to treatment as prisoners of war in accordance with Geneva Convention III upon capture[44]. They are also entitled to combatant immunity, that is, they may not be prosecuted for having engaged in belligerent acts that are lawful under the law of armed conflict[45]. For instance, a combatant who conducts cyber operations that violate domestic criminal law may not be prosecuted for such actions so long as they are carried out in compliance with the law of armed conflict. Combatant immunity is a customary interna-

[38]Ibid p. 542.

[39]Supra note 18, API 43(2).

[40]Supra note 10, rule 25.

[41]Hague Regulations, art. 1.

[42]US COMMANDER'S HANDBOOK, para. 5.4.1.1; AMW MANUAL, Rule 10(b) (i) and accompanying commentary. *But see* ICRC INTERPRETIVE GUIDANCE at 22.

[43]Supra note 10, rule 26.

[44]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.

[45]Cited at Tallinn Manual US COMMANDER'S HANDBOOK, para. 5.4.1.1.

tional law principle recognized in Article 43(2) of Additional Protocol I.

4.1.1. The Impact against Civilians

The term civilian under international humanitarian law is not defined in a very comprehensive way. Albeit, Additional Protocol I[46] defines civilians in negative terms as being all persons who are neither members of the armed forces nor of a *Leve'e en masse*[47]. This approach is implicit in Geneva Conventions III and IV. As a general rule, then, during an international armed conflict, civilians are persons who are not members of the armed forces or of groups assimilated to the armed forces.

The majority of the International Group of Experts agreed that civilians retain civilian status even if they directly participate in cyber hostilities[48]. Meaning they are civilians irrespective of their participation For instance, consider an international armed conflict in which civilian patriotic hackers independently undertake offensive cyber operations against the enemy's forces. Such individuals may be lawfully targeted, and, unless they qualify as participants in a *levée en masse*, lack combatant immunity for their actions.

The right of non-combatant *inter alia* civilians is not absolute right since they owe a duty of refraining from participation in warfare generally and cyber warfare particularly. According to Karma Nabulsi, The right of the non-combatant population to protection…involves…a corresponding duty of abstaining from…hostilities[49].

The researcher observes the impact of cyber warfare on civilians from two dimensions.

First, from protection point of view they should deserve protection from being targets of attacks since the international legal framework in force obliges to do so. For instance, the civilian population and individual civilians shall enjoy general protection against dangers arising from military operations[50]. By the same vein, civilian objects should be protected from attacks[51]. Albeit, Computers, computer networks, and cyber infrastructure may be made the object of attack if they are military objectives. The possible impacts include among other things are humiliating industries, infrastructures, telecommunications, transportation services and financial systems. For example manipulating civilian air traffic control systems. Thus, the researcher opined that the above civilian facilities should be protected from cyber-attacks.

Second, from Participation point of view civilians have no right to participate in the conduct of hostilities yet if they take part on warfare they loss the protection of the law[52].

In Toto, Civilian hackers remain civilians unless they meet the definition of combatants under the law. In the case of states who have signed Additional Protocol I would mean all members of the armed forces and any groups and units etc as defined under the protocol[53]. For those states who are not party to API the older rules set out in the Geneva conventions apply. All other civilian hackers remain civilians—however they lose their protection as civilians for such time as they directly participate in hostilities[54].

4.1.2. The Impact against Combatants

With no doubt Additional Protocol I[55] provide that "*members of the armed forces of a Party to a conflict* (*other than medical personnel and chaplains covered by Article* 33 *of Geneva Convention III*) *are combatants, so that they maintain the right to participate directly in hostilities*".

The Tallinn Manual Commentary reviewed the issue dictating that[56], *although the law of armed conflict contains no prohibition on participation, it does set forth consequences that result from such participation. Three are of particular importance*: *combatant immunity, prisoner of war status, and targetability. Entitlement to combatant immunity and prisoner of war status depend on whether the individual concerned is a combatant in an international armed conflict.*

[46]Supra note 18, Arts 50(1).
[47]Supra note 86, Arts 4A (6).
[48]Supra note 10, rule 29 commentary 3.
[49]Karma Nabulsi, *Evolving Conceptions of Civilians and Belligerents*: *One Hundred Years After the Hague Peace Conferences, in* CIVILIANS IN WAR cited at *Susan W. Brenner* fn 18.
[50]Supranote 18, Arts 51(1).
[51]Ibid, Arts 52.
[52]ibid, Arts 51(3).
[53]Ibid, Arts 43.
[54]Interview with Dr. Harrison International cyber law expert on e-mail on 9 April 2014.
[55]Id.
[56]Id, rule 25 commentary 2.

By the same token, members of the armed forces of a Party to the conflict who, in the course of cyber warfare, fail to comply with the requirements of combatant status lose their entitlement to combatant immunity and prisoner of war status.

In other words, if a person engaged in cyber operations during an armed conflict is a member of an organized armed group not belonging to a Party to the conflict, it does not matter if the group and its members comply with the four criteria of combatancy. That person will not have combatant status and therefore not be entitled to combatant immunity or to be treated as a prisoner of war. Such a person would be an unprivileged belligerent.

According to Dr. Harrison, the term combatant has been used to describe both those persons with a right to take direct part in hostilities but also to describe any person who actually engages in hostile acts in an armed conflict on behalf of a party to conflict, whether or not they are permitted to do so. Thus, in international armed conflicts, combatants may be further distinguished in two viz, members of regular armed forces and any other persons actively participated in hostilities[57].

On the other hand, the researcher argues that the term combatant should be destined to those regular members of armed force[58] otherwise we defeat the very purpose of being combatant.

Still more Unlike civilians, combatants are entitled to directly participate in hostilities and are subsequently immuned from prosecution for acts which are carried out as per the laws of armed conflicts, Given the increasing extent of international and domestic laws prohibiting and criminalizing various forms of computer misuse and network intrusion, the combatant shield is perhaps the most important consequence of being a lawful combatant for cyber operations where combatants are unlikely to face capture and subsequent detention[59].

As mentioned somewhere in this paper, Right now, there is no comprehensive international treaty exists specific to regulate cyber-attacks. Plethora international legal frameworks are not directly aimed at cyber-attacks but however regulate means that may be used in or may be a focus of a cyber-attack. These include particularly, the international law governing telecommunications, aviation, space, and the law of sea.

By similar fashion, these legal regimes were largely formed prior to if not at the infant stage of the emergence of cyber-attacks and therefore and are not comprehensive enough to regulate or prohibit cyber-attacks. Instead, these “means-based” frameworks implicate cyber-attacks only so long as an attack employs the particular means regulated by the agreement.

Thus, the jurisprudence on cyber security has suggested that these bodies of international law can be used to regulate cyber-attacks[60].

However, internationally assessing the legality of new weapons is in the interest of all States, as it will help them ensure that their armed forces act in accordance with their international obligations.

In other words, whenever a state study to use, acquire or adopt new weapon, means and methods including cyber such employment in some or all situations is prohibited by this protocol or international law.

In particular, States party to Additional Protocol I must consider the rules under that treaty, as required by Article 36 whenever cyber operation is conducted. These include:

- Prohibition to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering[61].
- Prohibition to employ methods or means of warfare which are intended, or may be expected to cause widespread, long-term and severe damage to the natural environment[62].
- Prohibition to employ a method or means of warfare which cannot be directed at a specific military objective and consequently, that is of a nature to strike military objectives and civilians or civilian objects without distinction[63].
- Prohibition to employ a method or means of warfare the effects of which cannot be limited as required by Additional Protocol I and consequently, that is of a nature to strike military objectives and civilians or civilian objects without distinction[64].

[57]Supra note 17, p. 141.

[58]Supra note 18, Arts. 43.

[59]Supra note 1, p. 254.

[60]THE LAW OF CYBER-ATTACK by; Oona A. Hathaway, Rebecca Croot of, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel pp. 54 & 55.

[61]Supra note 18, Art. 35(2).

[62]Ibid, Articles 35(3) and 55.

[63]Id, Art. 51(4) (b).

[64]Id, Art. 51(4) (c)). See also, Article 51(4) (b) and (c) and rule of customary international law prohibiting indiscriminate attacks.

- Prohibition of attacks by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects[65].
- Prohibition of attacks which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination there of, which would be excessive in relation to the concrete and direct military advantage anticipated[66].

Is Cyber considered as a weapon? Yes indeed! The researcher glanced at the definition of the term weapon by taking three countries experience[67].

Now after saying that cyber as weapon as well as means and method of warfare, the question is that weather cyber is prohibited under international humanitarian law? The researcher argues cyber is not unlawful. Albeit, A weapon that can be used with due care is going to be used abusively against civilians. In such a case, it is not the cyber per se as a weapon rather as a method or the way in which it is used is prohibited.

However, Cyber operations are not explicitly referred to in existing law of armed conflict treaties. Albeit, in the Nuclear Weapons Advisory Opinion[68], the International Court of Justice affirmed that "the established principles and rules of humanitarian law…apply to all forms of warfare, and to all kinds of weapons, those of the past, those of the present and those of the future."

Finally, the researcher opined that Article 36 of API is backed by ICJ advisory opinion mentioned above on Nuclear Weapons case so that cyber warfare is subject to IHL regulation.

4.2. Customary International Law

To begin with, under international law, custom comprises two elements. These are state practice and *opinion juris sive necessitates*. The first element should be backed by actual practice of states via duration[69], uniformity[70] and generality.

Meanwhile, the second element that is the *opinion juris*, belief that a state activity is legally obligatory, is the factor which turns the usage into a custom and renders it part of the rules of international law. To put it slightly differently, states will behave a certain way because they are convinced it is binding upon them to do so[71].

Still more, the increasing use of computers and computer networks through the 1970s and 1980s was followed swiftly by the rise of the "network of networks" known as the Internet in the mid-1990s[72].

Ultimately, the Internet spawned an entirely new domain of operations referred to as *cyberspace*. It is in and through this virtual space that cyber activities occur. So, not only are the activities in cyber new, *where* cyber actions take place is a unique location[73].

As noted above, customary law does not instantly appear but is developed through state practice and rationale. The cyber practices of states and the thought behind those actions over the past 30 years must be examined to determine if there is customary law in cyberspace[74]. If no principles have been developed, as earlier discussed, cyberspace remains unconstrained under the default customary international regime.

[65]Id, Art. 51(5) (a)

[66]Id, Art. 51(5) (b).

[67]The Australian Instruction Sub-section 3(a) defines the term "weapon" as "an offensive or defensive instrument of combat used to destroy, injure, defeat or threaten. It includes weapon systems, munitions, sub-munitions, ammunition, targeting devices, and other damaging or injuring mechanisms." Whereas the Belgian General Order Subsection 1(a) defines the term "weapon" as "any type of weapon, weapon system, projectile, munitions, powder or explosive, designed to put out of combat persons and/or materiel". The USA Law of War Working Group has proposed standard definitions, pursuant to which the term "weapons" refers to "all arms, munitions, materiel, instruments, mechanisms, or devices that have an intended effect of injuring, damaging, destroying or disabling personnel or property", and the term "weapon system" refers to "the weapon itself and those components required for its operation, including new, advanced or emerging technologies which may lead to development of weapons or weapon systems and which have significant legal and policy implications".

[68]Nuclear Weapons Advisory Opinion, para. 86.

[69]International Court of Justice (ICJ), *North Sea Continental Shelf* cases 1969, dispute between Germany on the one hand and Holland and Denmark on the other over the delimitation of the continental shelf, the IC Jmarked "**Though the time element too short**", state practice, "including that of states whose interests are specially affected", had to be "both extensive and virtually uniform in the sense of the provision invoked".

[70]Ibid, Asylum case 1950; The Court declared that a customary rule must be "in accordance with **a constant and uniform usage** practiced by the States in question".

[71]Malcolm N. Shaw, International law 6th edition, p. 84.

[72]The Customary International Law of Cyberspace by; *Gary Brown, Colonel, USAF Keira Poellet, Major, USAF* p. 4.

[73]ibid.

[74]http://Online.lewisu.edu/miss/resources/the-history-of-cyber-warfare last visited 22-05-2014.

Taking the above explanation in to account, custom as a source of international law is vividly stipulated under the ICJ statute[75]. Thus, the same is true for international humanitarian law in general and Cyber warfare in particular.

Despite the law of armed conflict does not expressly regulate cyber activities, regard should be had to the Martens Clause, found in Hague Convention IV[76], the 1949 Geneva Conventions[77], and Additional Protocol I[78]. The text in Hague Convention IV provides that:

"*Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in Cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public Conscience.*"

Thus, as far as cyber operations are conducted in the course of an armed conflict is concerned, the Martens Clause, which reflects customary international law, should come in to picture to address the scenarios.

At this juncture, the issue worth considering is that cyber warfare is a new phenomenon in the contemporary world due to the advancement of technology. So, instant-customary international law should govern the situations regarding cyber warfare.

4.3. General Principles of International Law

The other issue worth considering is that general principles of law, General principles of IHL help to guide belligerents during an armed-conflict, the following are the most dominant principles under IHL;

1) **Military Necessity:** It is permissible to use those measures not forbidden by international law which are necessary to secure the complete submission of the enemy. In other words, all measures necessary to bring an enemy to complete submission excluding those (as cruelty, torture, poison, perfidy, wanton destruction) that are forbidden by modern laws and customs of war.

By the same vein, the Tallinn manual stipulates that "a use of force involving cyber operations undertaken by a State in the exercise of its right of self-defense must be necessary…"[79].

2) **Humanity:** It is forbidden to inflict suffering, injury or destruction not actually necessary to accomplish a legitimate military purpose. This principle is reaffirmed in St. Petersburg conference of 1868. At the conference the delegates affirmed that the only legitimate object of war should be to weaken the military force of the enemy and not to senselessly cause suffering to innocent millions[80].

3) **Proportionality:** The collateral damage arising from military operations must not be excessive in relation to the direct and concrete military advantage anticipated from such operations. an action is proportional when it does not cause: a) Too many unintended collateral civilian casualties; b) Unintended damage excessive in relation to the expected military advantage. "Proportionality" does not aim to limit casualties among combatants in war; it seeks to minimize non-combatant losses.

Proportionality addresses the issue of how much force, including uses of cyber force, is permissible once force is deemed necessary. The criterion limits the scale, scope, duration, and intensity of the defensive response to that required to end the situation that has given rise to the right to act in self-defense. It does not restrict the amount of force used to that employed in the armed attack since the level of force needed to successfully mount a defense is context dependent; more force may be necessary, or less force may be sufficient, to repel the attack or defeat one that is imminent.

In addition, there is no requirement that the defensive force be of the same nature as that constituting the armed attack.

Therefore, a cyber-use of force may be resorted to in response to a kinetic armed attack, and vice versa[81].

[75]The UN ICJStatute, Arts. 38(1) which reads; the Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states; (b) international custom, as evidence of a **general practice accepted as law** (c) the general principles of law recognized by civilized nations; (d) Subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

[76]Hague Convention IV, preamble.

[77]GC I, Art. 63 GCII, art. 62; GC III, Art. 142; GC IV, art. 158.

[78]Additional Protocol I, art. 1(2).

[79]Supra note 10, rule 14.

[80]See http://en.wikipedia.org/wiki/St_Petersburg_Declaration_of_1868 last visited 22-05-2014.

[81]Supra note 10, commentary 5 on rule 14.

4) **Distinction and Precautions:** Military Commanders must distinguish between legitimate military targets & civilian objects including the civilian population. Pursuant to Additional Protocol I[82] codify the customary international law principle: "*in order to ensure respect for and protection of the civilian population and civilian objects*, 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*".

On the other hand, Precaution is a right hand of distinction principle. Pursuant to first additional protocol[83] which provides in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.

5) **Limitation:** The rights of the belligerents to choose methods and means of warfare are not unlimited. This principle is reaffirmed in the first additional protocol I of Geneva conventions, which stipulates in black and white as; "*In any armed conflict, the right of the parties to the conflict to choose methods or means of warfare is not unlimited*"[84].

By the same fashion, the Tallinn Manual provides that it is prohibited to employ means or methods of cyber warfare that are of a nature to cause superfluous injury or unnecessary suffering[85].

Finally, the researcher strongly argues that the general principles of IHL mutatis mutandis applies to cyber warfare since such principles from times immemorial guide and regulate the conduct of belligerents.

5. Monitoring Organ

Although the UN so far had took limited action on the issue of cyber-security and *on sui generis* cyber warfare yet still there are several UN General Assembly resolutions[86]. In August 1999, the United Nations sponsored an international meeting of experts in Geneva to better grasp the security implications of emerging information technologies[87]. A follow-up General Assembly resolution in 2002 called for further consideration and discussion of "information security"[88].

Finally, although absurd, these recommendations represent real progress in overcoming a long impasse between the United States and Russia over how to address cyber-security issues. The cooperation may even suggest possibilities for a future multilateral treaty under the auspices of the United Nations, which Russia has been advocating for some time. Now a day, however, the role of the United Nations with respect to cyber warfare remains largely limited to discussions and informational sharing since so far there is no binding treaty governing the issue and absence of commitment by international community thereof.

Besides regional moves are encouraging despite cyber plans and capabilities are still emerging and could serve as courage for further actions.

6. Current Challenges

The emergence of cyberspace adds an additional dimension to warfare: with and without clashes of traditional troops and machines of war[89]. Cyber warfare is not consistently defined across national borders. Further many countries lack laws against it and lack of enforcement coupled with low cost attack allows anyone or any state to initiate cyber-attacks[90].

[82]Supra note 18, Arts 48.

[83]ibid, Arts 57.

[84]Id, Arts 35.

[85]id, Rule 42.

[86]"Developments in the field of information and telecommunications in the context of international security". *See*, G. A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Jan. 8, 2008); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Jan. 9, 2009); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Jan. 14, 2010). Available at http://www.un.org/en/ Last visited January 2014.

[87]G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002).

[88]Id, *The resolution called upon Member States to*: *promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field and invited all Member States to continue to inform the Secretary-General of their views and assessments on the following questions*: (*a*) *General appreciation of the issues of information security*; (*b*) *Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources.*

[89]http://www.techrepublic.com/blog/it-security/cyberwarfare-characteristics-and-challenges/ last visited 26-05-2014.

[90]ibid.

The researcher has identified and noted the following critical issues as far as cyber warfare is concerned, needless to say,

- 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[91].
- Are hackers a legitimate target in cyber warfare? Most hackers would be civilians who remain protected by IHL against direct attack—although they would remain subject to law enforcement and possible criminal prosecution depending on whether their activities violated other bodies of law. The researcher argues that if hackers take a direct part in hostilities by way of a cyber-attack in support of one side in an armed conflict, there is no reason to let them free from being legitimately targeted.
- The other challenge is the inevitable Attitudinal and policy differences between major super powers as to cyber law treaty. For instance, the United States has for many years been an opponent of creating an international treaty for cyber-warfare. It has listed enforceability and accountability as two of its primary concerns.

Instead, the US has suggested increasing national cyber-defence technology and increasing the cooperation between law enforcement agencies[92]. Albeit, Russia has been the ardent supporter of an international treaty for cyber-warfare. Beginning in 1998, Russia has been submitting requests to members of the United Nations to back its plan for a global cyber-warfare treaty.

- Finally, there are no centralized monitoring mechanisms to govern cyber warfare so far as the only actors irrespective of the questionable effectiveness are NATO, Council of Europe, Organization of American states and Shanghai Cooperation Organization which are mandated to follow up their respective regions and members.

7. Conclusion

Cyber warfare is a new phenomenon and scenario under International Humanitarian law. There is no agreed definition for cyber warfare albeit for the sake of understanding that it is Internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data and cripple financial systems…among many other possibilities. The cyber incidents coupled with lenient legal framework pave the cyberspace for hackers as a playground. Internationally, there is no comprehensive cyber oriented treaty to address the hazards posed by cyber warfare despite attempts towards codification by a group of experts in Tallinn albeit being as a soft law.

8. Recommendations and the Way Ahead

To solve the above mentioned challenges, the researcher recommends the following suggestions as a way forward;

First and foremost, there should be comprehensive and well organized International legal machinery by enacting separate treaty document to govern cyber warfare.

Secondly, from *jus in bello* point of view since the law of war is based in large part on the provisions of the Geneva Conventions and their customary counterparts so that Some of the fundamental principles underlying law of war are the principle of military necessity (military operations must be intended to assist in the military defeat of the enemy and must serve the intended military purpose) the principle of distinction (military operations may be conducted only against "military objectives" and not against civilian targets), and the principle of proportionality (the expected incidental loss of civilian life, injury to civilians or damage to civilian objects must not be disproportionate to the anticipated military advantage). Thus, the researcher recommends that fore onething, cyber warfare should be conducted to serve military necessity principle fore another thing, even if one cyber dominion, combatants in cyber warfare should spare civilians' and their objects. And with regard to objects having dual purpose that is military as well as civil use effective assessment should be made in light with principle of proportionality.

As to should hackers a legitimate target in cyber warfare? Most hackers would be civilians who remain protected by IHL against direct attack—although they would remain subject to law enforcement and possible criminal prosecution depending on whether their activities violated other bodies of law. The researcher recom-

[91]ibid, Arts 48.

[92]Alter Gary Sharp Sr., "The Past, Present, and Future of Cyber security," *Journal of National Security Law & Policy* 4, no. 1 (2010).

mends the notion of direct participation in hostilities should be on pragmatic way (case by 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.

Finally, from monitoring organ point of view, there are no centralized monitoring mechanisms to govern cyber warfare so far only NATO, Council of Europe, Organization of American states and Shanghai Cooperation Organization follow up their respective regions and members.there should be United Nation Special body for Cyber Affairs to come up with centralized monitoring organ.

References

Clarke, R. (2010). *Cyber War*. New York: HarperCollins.

Dinniss, H. A. H. (2013). Participants in Conflict—Cyber Warriors, Patriotic Hackers and the Laws of War. In D. Saxon (Ed.), *International Humanitarian Law and the Changing Technology of War*. Leiden: Martinus Nijhoff. http://dx.doi.org/10.1163/9789004229495_013

Dinstein, Y. (2010). *The Conduct of Hostilities under the Law of International Armed Conflict.* Cambridge University Press.

Droega, C. (2008). Elective Affinities? Human Rights and Humanitarian Law. *International Review of the Red Cross, 90*.

Hensel, H. M. (2007). *The Law of Armed Conflict: Constraints on the Contemporary Use of Military Force.* Ashgate Pub Co.

Pictet, J. (Ed.) (1952). *Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*. Geneva: ICRC.

Solis, G. D. (2010). *The Law of Armed Conflict: International Humanitarian Law in War*. Cambridge University Press.

Annex I: List of Key Informants

Name of Interviewees	Title and position of Interviewee's	Place and Date of Interview
1) Dr. Heather A. Harrison Dinniss	Professor of International cyber Law at Swedish National Defence College	Addis Ababa, 08 April 2014 10:36 on E-mail
2) Umesh Kadam	Professor, Regional Legal Advisor Nairobi, Kenya	Addis Ababa, 24 April 2014 on E-mail
3) Laurence Brunet-Baldwin	Legal attachée, Forum for the Integration and Promotion of the Law International Committee of the Red Cross (ICRC) 19, avenue de la Paix, 1202 Geneva, Switzerland	Addis Ababa, 23 April 2014 on e-mail
4) Etienne Kuster	ICRC Academic Relation Advisor, Geneva, Switzerland	Addis Ababa, 22 April 2014 on e-mail

Annex II: Interview Questions

Below are questions designed to collect information for my research on Cyber warfare from different experts on the area;

Name of Interviewee: _____
Title/Occupation: _____
Date of Interview: _____
Place of Interview: _____

Q1. What is the impact of cyber warfare on civilians and combatants?
Q2.Do you think that the existing IHL regime applies to cyber space by analogy?
Q3.Do you think that civilian hackers deprived of their status by their participation?