An Appraisal of The Legal Framework for The Protection of Civilians in Cyber-Warfare Under International Humanitarian Law

Adasi, Nsanawaji Igakuboon LLM

Abstract: **This research paper appraises the legal framework for the protection of civilians in cyber warfare under International Humanitarian Law. The paper examines the existing rules of IHL on the protection of civilians in armed conflicts, their applicability or otherwise to cyber warfare, the existing gap in the law, with a view to making recommendations on more effective ways to protect the civilian population in armed conflicts. In doing this, the research methodology adopted is the doctrinal approach. Both primary and secondary sources of information were consulted and utilized in the course of this work. The primary sources include the four Geneva Conventions and their Additional Protocols, the Commentaries on the Geneva Conventions and Additional Protocols, the Rome Statute etc. The secondary sources include textbooks, journals, articles, newspaper, and online material retrieved from the ICRC website and other relevant websites. This paper finds that although International Humanitarian Law provides for robust rules aimed at the protection of civilians in armed conflicts, these rules do not sufficiently afford protection to civilians in cyber warfare as the complexity brought about by these new means and methods of warfare were not captured at the time the rules were made. This work identifies some of the challenges posed to the protection of civilians in cyber warfare and establishes a case for the need for a treaty to specifically regulate cyber warfare and provide for the protection of civilians in cyber warfare. This work also recommends that International policy debates on cyber warfare should be geared towards streamlining the various national views on cyber-attacks.**

I. INTRODUCTION:

Cyber-security has become a growing concern within the national and international polity. The need for protection from the hostile use of the cyber-space is a security concern that is on the front burner for governments, individuals, businesses and the media. The dependence of modern societies and of their armed forces on computer systems renders such systems prime objects of attack, or a choice medium through which to target some linked object or person.[1] While it is fair to say that most of the threats in the cyber-realm are not immediately related to situations of armed conflict but stem, rather, from economic or other espionage, or organized cyber-crime, it is also clear that recourse to cyber-weapons and cyber-operations is playing a growing role in armed conflicts, and because of the growing sense of insecurity among states and other actors, most states are actively preparing for this new development. The impact of cyber-attacks in armed conflict has given it a prominent position in the agenda of policy makers and military leaders around the world.[2]

The cyber-space is a virtual space that provides worldwide interconnectivity regardless of borders. While this feature is of great utility in peacetime, interconnectivity also presupposes porosity. Interconnectivity also means that the effects of an attack may have repercussions on various other systems given that military networks are in many cases dependent on commercial infrastructure.[3]The consequences of cyber-attacks can be quite devastating, particularly when its effect is not limited to the data of the targeted computer system. Most cyber-attacks are intended to have physical effects in the real world, beyond the cyber-space. Cyber-attacks have the potential to disrupt a nation's power grids, transportation links, health care service, emergency response, financial flows among many other venues[4]. Most cyber-operations have significant humanitarian consequences on the civilian population. This is because of the fluid nature of the cyber-space which makes it difficult to distinguish between civilian objects and military objectives.

The focal point of International Humanitarian Law[5] is the reduction of human suffering in armed conflicts. IHL provides a legal framework for the regulation of armed conflicts and the protection of persons who are not or are no longer involved in hostilities. The rules of IHL were only targeted at hostilities in the traditional, kinetic or physical setting, and did not envisage the conduct of hostilities in the cyber-space.[6] Thus, their application to activities in the cyber-space poses a lot of challenges and raises a lot of queries. For instance, 'when does a cyber-attack amount to an attack in the sense of armed conflict?'; or 'how should the most important rules on the conduct of hostilities, namely the principles of distinction,

[1] Boothby, W. 2012. Some Legal Challenges posed by Remote Attack *International Review of the Red Cross* Vol. 94 No 886 , pg 581

[2] Droege, C. 2012 Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians *International Review of the Red Cross*, Vol. 94 Number 886 pg 533

[3] International Humanitarian Law and the challenges of contemporary armed conflicts. Report of the 31st International Conference of the Red Cross and Red Crescent Geneva-Switzerland, 28 November – 1 December 2011. Retrieved from www.icrc.org on 11th May, 2017

[4] Hughes, R. Towards a Global Regime for Cyber Warfare Cyber Security Project, Chatham House, London

[5] Also referred to as 'IHL'

[6] Droege, C 2012 *op cit* 2 pg 533

proportionality, and precaution, be applied and interpreted in the cyber-realm considering the interconnectedness of the cyber-space?'; 'should information now be regarded as a civilian object under humanitarian law and its destruction as damage to civilian object?'; 'does International Humanitarian Law effectively address the potential consequences of cyber-warfare on civilians?' - These and other such questions have been raised in a bid to assess the feasibility of accommodating cyber-warfare and other new means and methods of warfare under the current regime of IHL. This work will lend a voice to the ongoing discussion on this subject matter by answering the following questions:

1. What are the laws in existence tailored to protect civilians in armed conflicts?
2. Do these laws adequately protect civilians in cyber-warfare?
3. How can International Humanitarian Law effectively address the potential consequences of cyber-warfare on civilians?

In answering the above questions, this article will examine the existing rules of IHL pertaining to the protection of civilians in armed conflict; identify the challenges associated with the application of the existing rules of IHL to cyber-warfare; discuss the need to revise the existing laws to better protect civilians in cyber-warfare; and establish a case for the need for a treaty to specifically regulate cyber-warfare and provide for the protection of civilians in cyber-warfare.

II. DEFINITION OF CIVILIAN

The term "Civilian" under International Humanitarian Law does not enjoy any comprehensive definition. Albeit, Additional Protocol I[7] defines civilians in negative or reverse terms by declaring a civilian to be "any person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol"[8], and adding that - 'in case of doubt whether a person is a civilian, that person shall be considered to be a civilian."[9] Article 4 A (1), (2), (3) and (6) of Geneva Convention III[10] provides as follows:

A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:

1) Members of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces.

2) Members of other militias and members of other volunteer corps, including those of organized resistance movements, belonging to a Party to the conflict and operating in or outside their own territory, even if this territory is occupied, provided that such militias or volunteer corps, including such organized resistance movements, fulfill the following conditions:

   a. that of being commanded by a person responsible for his subordinates;

   b. that of having a fixed distinctive sign recognizable at a distance;

   c. that of carrying arms openly;

   d. that of conducting their operations in accordance with the laws and customs of war.

3) Members of regular armed forces who profess allegiance to a government or an authority not recognized by the Detaining Power.

4) 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.

Article 43 of Additional Protocol I provides as follows:

1. The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, ' inter alia ', shall enforce compliance with the rules of international law applicable in armed conflict.
2. Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities.
3. Whenever a Party to a conflict incorporates a paramilitary or armed law enforcement agency into its armed forces it shall so notify the other Parties to the conflict.

[7] Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Art. 1(2), 12 December 1977, 1125 U.N.T.S. 3 (hereinafter Additional Protocol I or AP I)

[8] Additional Protocol I, Article 50 (1)

[9] *ibid*

[10] International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), 12 August 1949, 75 UNTS 135, Retrieved on 28th May, 2017 from http://www.refworld.org/docid/3ae6b36c8.html (hereinafter referred to as GC III)

The effect of the foregoing provisions is that civilians consist of persons who are neither members of the armed forces, groups assimilated to the armed forces, non-state armed groups nor of a *Levee en masse*[11]. The civilian population comprises all persons who are civilians[12], and interestingly, the presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character.[13]

Protection in this context entails ensuring the full respect of the rights of the individual and the obligations of the authorities/arms carriers in accordance with the letter and the spirit of the relevant bodies of law and, therefore, to preserve people's safety, integrity and dignity. The protection of civilians in armed conflict, therefore, involves all activities aimed at ensuring full respect for the rights of people who do not take part in hostilities in accordance with both the letter and spirit of relevant laws.[14] The protection of civilians in cyber-warfare is governed by the rules and principles of IHL.

III. MEANING OF CYBER-WARFARE

A look at the meaning of "cyber-warfare" will not be complete without defining "cyber-space" since it is the environment in which the former takes place. Cyber-space is a notional environment, a virtual space that provides worldwide interconnectivity regardless of borders.[15]

Cyber-attack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks.[16]The activities may also affect entities connected to these systems and networks. It is worthy of note that the direct effects of a cyber-attack (damage to a computer) may be less significant than the indirect effects (damage to a system connected to the computer).[17] 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".[18] The use of any instrument, including a computer, to cause death, injury, damage or destruction to another party to an armed conflict will cause that instrument, or computer, to become a weapon or means of warfare.[19]

Cyber-warfare refers to the 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. It involves actions taken by parties to an armed conflict to gain advantage over their adversaries in cyber-space by using various technological tools and people based techniques. In 2007, the US Strategic Command (USSTRATCOM) defined cyber-warfare as "the employment of computer network operations with the intent of denying adversaries the effective use of their own computers, information systems and networks."[20]

The International Committee of the Red Cross (ICRC) understands "cyber-warfare" as operations against a computer or a computer system through a data stream, when used as means and methods of warfare in the context of an armed conflict, as defined under IHL.[21] Cyber-warfare can be resorted to as part of an armed conflict that is otherwise waged through kinetic operations. The notion of cyber-warfare might also encompass the employment of cyber means in the absence of kinetic operations when their use amounts to an armed conflict, although no state is known to have publicly qualified an actual hostile cyber-operation as such."[22]

IV. ANALYSIS OF INTERNATIONAL HUMANITARIAN LAW RULES FOR THE PROTECTION OF CIVILIANS IN ARMED CONFLICTS

The protection of civilians and the civilian population in armed conflict is the bedrock of International Humanitarian Law (IHL), with strict rules defining the obligations and duties of parties to a conflict towards civilians. IHL establishes a comprehensive legal framework to protect civilians from the effects of military operations. The 1949 Geneva Conventions and the 1977 Additional Protocols constitute the core of the legal framework regulating the conduct of war, including the protection of civilians and other persons that do not take part in hostilities (e.g. wounded, sick and captured combatants).[23] The four Geneva Conventions

[11] The term applied to the inhabitants of a territory which has not been occupied, who on the approach of the enemy spontaneously take up arms to resist the invading troops without having had time to organise themselves into regular armed forces. They must be regarded as combatants if they carry arms openly and respect the laws and customs of armed conflicts. If captured, they have a right to be treated as prisoners of war. The Levee en masse should not be confused with resistant movements. (How does law protect in war? Retrieved from casebook.icrc.org/gloss on June 25, 2022).

[12] Additional Protocol I, Article 50 (2)

[13] Additional Protocol I, Article 50 (3)

[14] Young, R. M. 2009. Protection of Civilians in Situations of Armed Conflict, UNITAR Workshop, ICRC NYC. Retrieved on 1st August, 2017 from **https://www.unitar.org/ny/sites/unitar.org.ny/files/IV_ICRC_Protection%20of%20Civilians%20UNITAR%20-%20Sept%2009.ppt-final.pdf**

[15] ICRC, 2015. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32nd International Conference of the Red Cross and Red Crescent, EN 32IC/15/11, pg 39

[16] Lin, H. 2012. Cyber Conflict and International Humanitarian Law, *International Review of the Red Cross*. Vol 94. No886: 518 Retrieved on 3rd March, 2017 from www.icrc.org

[17] *ibid*

[18] Schmitt, M. N. 2013. Tallinn Manual on the International Law Applicable to Cyber-Warfare, Cambridge: Cambridge University Press, Rule 30

[19] For the meaning of 'means of warfare', see. Boothby, W. H. 2009. Weapons and the Law of Armed Conflict, Oxford: Oxford University Press, p. 4.

[20] Alexander, K. B. 2007. Warfighting in Cyberspace, *JFQ*, issue 46, 3rd Quarter pg 58-61:61

[21] ICRC, 2015. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32nd International Conference of the Red Cross and Red Crescent, EN 32IC/15/11

[22] *ibid*

[23] Waszink, C. 2011. Protection of Civilians under International Humanitarian Law: Trends and Challenges NOREF Report, Norwegian Peace Building Resource Centre pg 3. Retrieved on 1st August, 2017 from

and Additional Protocol I apply to international armed conflicts. Although significantly less detailed than the rules applicable to international armed conflicts, Common Article 3 to the Geneva Conventions and Additional Protocol II establish rules for non-international armed conflicts, imposing obligations on states and non-state armed groups alike. Furthermore, most of the fundamental rules pertaining to the protection of civilians have attained the status of customary humanitarian law applicable to both international and non-international armed conflicts, and binding on all states, whether signatories or not to the relevant treaty, as well as non-state armed groups.[24] Other relevant treaties and agreements (e.g. the Convention prohibiting or restricting Certain Conventional Weapons, the Cluster Munitions Convention, the Landmines Convention, the Chemical Weapons Convention, the Rome Statute of the International Criminal Court (ICC), etc.) also provide for the protection of civilians in armed conflicts.

IHL regulates the conduct of parties in an armed conflict by imposing limits on means (weapons) and methods (strategies) of warfare. IHL also regulates the treatment of certain categories of persons not taking part in combat.[25]

4.1. Protection of the Civilian Population

The civilian population and individual civilians 'enjoy general protection against dangers arising from military operations'.[26] The IHL rules on distinction, proportionality and precautions are fundamental to the protection of civilians during hostilities.[27]

The principle of distinction requires that the parties to a conflict at all times distinguish between civilians and combatants and between civilian objects (buildings, infrastructure, etc) and military objectives, and that they direct their attacks only against military objectives.[28] Thus indiscriminate attacks (attacks which are not directed at a specific military objective; which employ a method or means of combat which cannot be directed at a specific military objective, or; which employ a method or means of combat the effects of which cannot be limited as required by IHL, and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction)[29] are prohibited. Weapons which are incapable of distinguishing between civilian and military targets are consequently prohibited.[30] This principle aims to protect civilians from being made objects of attack in situations of armed conflict. However, civilians lose this protection if they take direct part in hostilities,. In which case, they can be attacked.[31]

The Principle of proportionality prohibits attacks which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[32] A breach of this principle will amount to an indiscriminate attack.[33] The principle aims to prevent unnecessary collateral damage by requiring that same is allowed only where the military advantage exceeds the injury to civilians. This rule is not codified in general IHL treaty provisions regulating non-international armed conflicts, either in Common Article 3 to the 1949 Geneva Conventions or 1977 Additional Protocol II. However, the principle has been established as a norm of customary international law applicable in both international and non-international armed conflicts.[34]

This principle requires precautions should be taken to ensure that civilian population or civilian objects are spared from the effects of attacks. The principle contains an obligation to do everything feasible to 'avoid and in any event minimize' incidental civilian loss or damage.[35] IHL prohibits attacks whose purpose is to terrorize the population,[36] and also prohibits parties to the conflict from using civilians as a shield.[37]

Civilians lose their protection from attack and the effects of the hostilities if, and for such time as, they directly participate in hostilities.[38] Women are given special protection under IHL, both as civilians and combatants. Children also benefit from special protection during armed conflict.[39] In particular, IHL aims to prevent the participation of children in hostilities and forbids parties to the conflict to recruit children into their armed forces.[40] If captured, child soldiers need to be afforded special protection. Other categories protected are war correspondents and journalists. IHL also recognizes the right of civilian populations affected by armed conflicts to receive humanitarian assistance, and conflicting parties have the obligation to allow humanitarian relief operations to reach civilians.

http://www.operationspaix.net/DATA/DOCUMENT/6547~v~Protection_of_Civilians_Under_International_Humanitarian_Law__Trends_and_Challenges.pdf

[24] *ibid*

[25] Fleck D., (Ed.), 2013. The Handbook of International Humanitarian Law, 3rd Edn Oxford: Oxford University Press.

[26] Art. 51(1), Additional Protocol I.

[27] See chapter 2 for an exhaustive discussion of these principles.

[28] AP I, Article 48.

[29] AP I Article 51 (4)

[30] ICJ, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, para. 78.

[31] AP I Article 51 (3)

[32] Articles 51(5)(b) and 57s of Additional Protocol I

[33] *ibid*

[34] Henckaerts, J. M. and Doswald-Beck, L. (eds.), 2005 Customary International Humanitarian Law, ICRC Cambridge: Cambridge University Press, Rule 14

[35] Schmitt, M. N. 1999. The principle of discrimination in 21st century warfare, Yale Human Rights and Development Law Journal, Vol. 2:170

[36] AP I Article 51(2)

[37] AP I Article 51(7)

[38] AP I Article 51(3)

[39] Additional Protocol II to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non- International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609, 16 (hereinafter Additional Protocol II or AP III) Article 4(3)

[40] AP II Article 4(3)(c) and (d)

4.2. Protection of Civilian Objects

Civilian objects are all objects which are not military objectives.[41] Attacks are to be limited strictly to military objectives.[42] Civilian objects are not to be the object of attack or reprisal.[43] Parties to a conflict are therefore required to distinguish between civilian objects and military objectives at all times. And where there is doubt as to whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.[44]

4.3. Protection of objects indispensable to the survival of the civilian population

IHL seeks to ensure that the survival of the civilian population is not jeopardized in the course of an armed conflict. Thus, parties to an armed conflict are prohibited from using starvation as a method of warfare.[45] It is prohibited to attack, destroy, remove or render useless objects indispensable to their survival, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.[46] The exception is where such objects are used by an adverse party as sustenance solely for the members of its armed forces or in direct support of military action, provided, however, that actions against these objects shall not be taken where it may be expected to leave the civilian population with such inadequate food or water as to cause its starvation or force its movement.[47] These objects are not to be made the object of reprisals.[48] IHL also prohibits means and methods of warfare intended or expected to cause widespread, long-term and severe damage to the natural environment.[49] Attacks against the natural environment by way of reprisals are prohibited.[50]

4.4. Protection of works and installations containing dangerous forces

IHL prohibits attacks on works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.[51] Also, other military objectives located at or in the vicinity of these works or installations are not to be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population.[52]

However, the special protection against attack stated above ceases: for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;[53] for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support;[54] for other military objectives located at or in the vicinity of these works or installations only if they are used in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support.[55] Where the protection ceases and any of the works, installations or military objectives is attacked, civilians remain entitled to all the protection accorded them and all practical precautions shall be taken to avoid the release of the dangerous forces.[56] Attacks by way of reprisals on works, installations or military objectives are prohibited.[57]

4.5. Choice of Weapons

IHL limits the means and methods of warfare.[58] For the purpose of protecting civilians, parties to a conflict are prohibited from using weapons that are by nature indiscriminate. Thus, weapons that cannot be directed at a specific military objective or whose effects cannot be limited as required by IHL and thus are of a nature to strike military objectives and civilians or civilian objects without distinction are prohibited.[59] The rules on precautions require that all feasible precautions in the choice of means and methods of warfare be taken to avoid or in any event minimize incidental loss of life or injury to civilians and damage to civilian objects.[60] Weapons that cause unnecessary suffering or widespread, long-term and severe damage to the natural environment are also prohibited.[61] In addition to the general rules on weapons, a number of treaties prohibit specific weapons (e.g. biological, chemical and blinding laser weapons) or restrict their use due to their potential to have indiscriminate effects in some circumstances (e.g. the use of incendiary weapons in populated areas).

4.6. Protection of hospitals

Civilian hospitals organized to give care to the wounded and sick, the infirm and maternity cases are not to be the object of

[41] AP I Article 52(1)
[42] AP I Article 52(2)
[43] AP I Article 52(1)
[44] AP I Article 52(3)
[45] AP I Article 54(1)
[46] AP I Article 54(2)
[47] AP I Article 54(3)(a) and (b)
[48] AP I Article 54(4)
[49] AP I Article 55(1)
[50] AP I Article 55(2)
[51] AP I Article 56(1)
[52] *ibid*
[53] AP I Article 56(2)(a)
[54] AP I Article 56(2)(b)
[55] AP I Article 56(2)(c)
[56] AP I Article 56(3)
[57] AP I Article 56(4)
[58] AP I Article 35(1).
[59] AP I, Article 51(4)(b) and (c); ICRC CLS, rule 71, pp 244-250.
[60] AP I Article 57(2)(a)(ii); ICRC CLS, rule 17, pp 56-58.
[61] AP I Article 35(2) and (3); ICRC CLS, rule 70, pp 237-244.

attack, but must at all times be respected and protected by the Parties to the conflict.[62] Hospitals are to be located as far as possible from military objectives. The protection is extended to the members of staff of the hospital.[63]

4.7. Protection of means of transportation

Convoys of vehicles or hospital trains on land or specially provided vessels on sea, conveying wounded and sick civilians, the infirm and maternity cases, shall be respected and protected.[64] Also, aircraft exclusively employed for the removal of wounded and sick civilians, the infirm and maternity cases, or for the transport of medical personnel and equipment, shall not be attacked, but shall be respected while flying at heights, times and on routes specifically agreed upon between all the Parties to the conflict concerned.[65] Parties to the conflict are also required to allow the free passage of all consignments of medical and hospital stores and objects necessary for religious worship intended only for civilians.[66] They shall likewise permit the free passage of all consignments of essential foodstuffs, clothing and tonics intended for children under fifteen, expectant mothers and maternity cases.[67]

4.8. Obligation to treat civilians humanely

Under the provisions of common article 3 to the four Geneva Conventions, parties to the conflict should treat humanely persons taking no active part in hostilities, *without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.*[68] *Thus, it is prohibited to commit acts of violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;*[69] *take hostages;*[70] *commit outrages upon personal dignity, in particular humiliating and degrading treatment;*[71] *pass sentences and carryout executions without previous judgment pronounced by a regularly constituted court.*[72] *The wounded and sick are to be collected and cared for.*[73] The duty to protect, respect and treat civilians humanely is part of customary international law.

Accordingly, the principle of non-refoulment must be respected, as protected persons cannot be transferred to states where they fear persecution on political or religious grounds. This principle applies in peacetime as well as in situations of armed conflict. IHL also prohibits forced movement of civilians, and protects internally displaced persons (IDPs) as well as refugees, according to the applicable rules.

V. APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW TO CYBER-WARFARE

The question is whether cyber-warfare can be governed by IHL. Arguments against the applicability of IHL to cyber-warfare have been based on the following grounds. First, no provision in any humanitarian law instrument directly addresses cyber-warfare. Second, the development of cyber-technology and its employment in warfare postdates existing treaty law and was therefore not within the contemplation of the parties to those instruments. Third, IHL was designed for means and methods of warfare that are kinetic in nature, and cyber-warfare, not being one of such is therefore outside the coverage of IHL (that is, cyber-warfare is not armed conflict).[74]

On the first two grounds, the fact that existing conventions are silent on cyber-warfare is of no issue. First, the Martens Clause, a well-accepted principle of humanitarian law, provides that whenever a situation is not covered by an international agreement, "civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity, and from the dictates of public conscience."[75] This clause is further restated in Additional Protocol I to the Geneva Convention.[76] By this norm, all occurrences during armed conflict are subject to application of humanitarian law principles; there is no lawless void.[77] The acceptance of "international custom" as a source of law in Article 38 of the Statute of the International Court of Justice further invalidates the contention of inapplicability based on the absence of specific law.[78]

Furthermore, a review of new weapons and weapon systems for compliance with humanitarian law is a legal requirement.[79] This would not be so if pre-existing law were inapplicable to incipient methods and means of warfare. Thus, the second ground also goes to no issue.

[62] International Committee of the Red Cross (ICRC), Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287, Retrieved on 28th May, 2017 from http://www.refworld.org/docid/3ae6b36d2.html (hereinafter referred to as GC IV) Article 18.
[63] GC IV Article 20
[64] GC IV Article 21
[65] GC IV Article 22
[66] GC IV Article 23
[67] *ibid*
[68] GC I, GC II, GC III, GC IV Article 3(1); AP II Article 4(1) and (2)
[69] GC I, GC II, GC III, GC IV Article 3(1)(a)
[70] GC I, GC II, GC III, GC IV Article 3(1)(b)
[71] GC I, GC II, GC III, GC IV Article 3(1)(c)
[72] GC I, GC II, GC III, GC IV Article 3(1)(d)
[73] GC I, GC II, GC III, GC IV Article 3(2)

[74] Haslam, E. 2000. Information Warfare: Technological Changes and International Law, *Journal of Conflict and Security Law*, Vol. 5, p. 157.
[75] The original formulation of the Martens Clause in the preamble of the Hague Convention IV respecting the Laws and Customs of War on Land, 18 October 1907, 36 Stat. 2295, I Bevans634, states "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 amoung civilized peoples, from the laws of humanity, and the dictates of the public conscience", reprinted in Roberts, A and Guelff, R., 2000. *Documents on the Laws of War*, 3rd ed., Oxford: Oxford University Press, p. 67.
[76] AP I Article 1(2)
[77] Schmitt, M. N. 2002 Wired warfare: Computer network attack and *jus in bello*, *International Review of the Red Cross* Vol. 84 No 846: 369
[78] The Statute of the International Court of Justice defines custom as "a general practice accepted by law". Statute of the International Court of Justice, 26 June 1977, Art. 38(1)(b), 59 Stat. 1031, T.S. No. 933, 3 Bevans 1153, 1976 Y.B.U.N. 1052.
[79] AP I Article 36

The third ground is that cyber-warfare is not armed conflict. The applicability of IHL is triggered by the existence of an armed conflict,[80] the determination of which depends solely on an assessment of the facts on the ground. International Humanitarian Law does not apply to every kind of activity called "cyber-attack". For International Humanitarian Law to apply to a cyber-attack, such an attack must amount to or be conducted within the context of an armed conflict. A possible answer to the question: what would constitute an armed attack in cyber-space? – is that if a cyber-attack causes the same effects as a kinetic attack that rises to the threshold of an armed attack, the cyber-attack would itself be considered an armed attack. Thus, cyber-attacks which can be ascribed to a state; are more than merely sporadic and isolated incidents; and are either intended to cause injury, death, damage or destruction (and analogous effects), or such consequences are foreseeable would constitute an armed conflict. Once the applicability of IHL is triggered, the question becomes one of adaptability of the rules on the conduct of hostilities.

5.1. Adaptability of the rules on conduct of hostilities to cyber-warfare

It has been contended that only those cyber-operations that constitute attacks are subject to the rules on conduct of hostilities.[81]On the contrary however, Melzer, N (2011) holds the view that *"the applicability of the restraints imposed by IHL on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as 'attacks' (that is, the predominant form of conducting hostilities), but on whether they constitute part of 'hostilities' within the meaning of IHL"*.[82] He opines that cyber operations that are designed to harm the adversary, either by directly causing death, injury, or destruction or by directly adversely affecting military operations or military capacity, must be regarded as hostilities.[83] For instance, cyber operations aiming to disrupt or incapacitate an enemy's computer controlled radar or weapons systems, logistic supply, or communication networks would qualify as hostilities even if they do not cause physical damage. However, cyber operations conducted for the general purpose of intelligence gathering would not fall under hostilities. As far as the non-destructive incapacitation of civilian objects is concerned, Melzer does not come to a definite conclusion but points to the dilemma between adopting a too restrictive or a too permissive interpretation of the law.[84] While his argument is attractive in that it gives effect to the very object and purpose of the rules on the conduct of hostilities, which is that innocent civilians must be kept outside hostilities as far as possible and enjoy general protection against danger arising from hostilities, it leaves open the most critical question, namely whether operations that disrupt civilian infrastructure without destroying it fall under the concept of hostilities.[85]

5.1.1. WHAT CONSTITUTES AN ATTACK?

Attacks are defined in Article 49(1) of Additional Protocol I (which reflects customary IHL) as acts of violence against the adversary, whether in offence or in defense. This definition presupposes that an attack must be an act of violence. However, violence here does not refer to the means of attack.[86]It has been generally accepted that what defines an attack is not limited to the violence of the means, but also the violence of the consequences.[87] Thus, even a data stream passed through cables or satellite could fall under the concept of attack if it occasions violent consequences. Where the effects of cyber-operations cause death or injury to persons or physical destruction or damage to objects as kinetic operations would, undoubtedly, such operation will be considered to be an attack and therefore subject to the rules on conduct of hostilities. However this is not usually the case as the consequences of cyber-operations do not necessarily have violent effects in that they do not cause physical damage or destruction.[88] It is indubitable that cyber-operation, like any other operation, constitutes an attack when it results in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects, including when such consequences are due to the foreseeable indirect or reverberating effects of an operation, such as the death of patients in intensive-care units caused by a cyber-attack against the electricity network that then cuts the hospital electricity supply.[89] The controversy however arises with regards to operations that do not cause death or injury to persons or physical destruction or damage to objects but rather disrupt the functioning of objects without causing them physical damage. In the latter circumstance, the ICRC considers that such an operation designed to disable an object – for example a computer or a computer network – constitutes an attack under the rules on the conduct of hostilities, whether or not the object is disabled through kinetic or cyber means.[90] The justification for this reasoning can be found in Article 52

[80] Article 2 Common to the four Geneva Conventions; AP I Article 1

[81] Schmitt, M. N. 2011. Cyber operations and the jus in bello: key issues, Naval War College International Law Studies, Vol. 87 : 91; Geiss, R. and Lahmann, H. 2012. Cyber warfare: applying the principle of distinction in an interconnected space, *Israeli Law Review*, Vol. 45, No. 3 : 2.

[82] Melzer, N 2011 Cyberwarfare and International Law, UNIDIR Resources Paper, available at: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf.

[83] *ibid* pg 28

[84] *ibid*

[85] Droege C. 2012 *op cit* 2 pg 555

[86]Dinstein, Y. 2004. The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge: Cambridge University Press, p. 84

[87]Schmitt, M. N. 2002. 'Wired warfare: computer network attack and jus in bello', *International Review of the Red Cross*, Vol. 84, No. 846 : 377; Schmitt, M . N. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press. Also available at: http://www.ccdcoe.org/249.html., Commentary on Rule 30, para. 3.

[88] Droege C. 2012 *op cit* 2 pg 557

[89]Schmitt, M. N. 2011. Cyber operations and the jus in bello: key issues, Naval War College International Law Studies, Vol. 87 : 6

[90] International Committee of the Red Cross, 2011. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of the 32nd International Conference of the Red Cross and the Red Crescent EN 321c/15/11, Geneva, pg 41

of Additional Protocol I which defines military objective as follows:

> Military objectives are those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[91]

This shows that drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it.[92] The reference to "neutralization" in the definition would be superfluous if an operation aimed at impairing the functionality of an object (i.e. its neutralization) would not constitute an attack. Furthermore, an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities, which is to ensure the protection of the civilian population and civilian objects against the effects of hostilities.[93] Indeed, under such a restrictive understanding, a cyber-operation that is directed at making a civilian network (electricity, banking, communications or other network) dysfunctional, or risks causing this incidentally, might not be covered by the IHL prohibition of directing attacks against civilian objects, the prohibitions of indiscriminate or disproportionate attacks and the principle of precautions in attack, despite the potentially severe consequences of such operations for the civilian population.[94]

Although there is no international consensus on application of International Humanitarian Law to cyber-warfare, an increasing number of states and international organizations have publicly asserted that IHL applies to cyber-warfare. Cyber-technology does not occur in a legal vacuum. Thus, where cyber capabilities are employed in armed conflict, they must comply with all the principles and rules of IHL, as is the case with any other weapon, means or method of warfare, new or old. It makes no difference whether cyber-space should be considered a new war-fighting domain similar to air, land, sea and outer space; a special type of domain or not a domain at all. Customary IHL rules on the conduct of hostilities apply to all means and methods of warfare, wherever they are used. This position is buttressed by the statement of the International Court of Justice in its Advisory Opinion on the legality of the threat or use of nuclear weapons, to the effect that the established principles and rules of humanitarian law applicable in armed conflict apply "to all forms of warfare and to conflicts which must comply with the rules and principles of IHL.

VI. CHALLENGES IN THE PROTECTION OF CIVILIANS IN CYBER-WARFARE

There is no special provision for the protection of civilians in cyber-warfare other than the general protection provided in the general rules of IHL. Therefore, the various principles of IHL and the rules on the conduct of hostilities aimed at protecting civilians and civilian objects in armed conflict also covers cyber-warfare. The *sui generic* nature of cyber-warfare makes the application of the existing rules of IHL to it to be fraught with difficulties. The existing rules of IHL have proven to be inadequate in addressing the unique challenges posed by cyber-warfare to the survival of civilians. While some of the challenges are unique to cyber-warfare, others are more general. Some of such challenges include:

6.1. Imprecise Definition of Rules

The extent of protection afforded to civilians under the general rules of IHL depends on how certain notions and concepts used in the framing of those rules are interpreted by states. The core rules for the protection of civilians from the effects of hostilities contain terms that are not adequately or precisely defined, or the definition leaves considerable room for interpretation. Terms like "civilian objects", "military objectives", "concrete and direct military advantage", and "all feasible precautions" are not defined and its interpretation is therefore left to the states. This results in differences in the interpretation and practical application of the rules. It also gives significant discretion to those in charge of making targeting decisions and assumes that parties will implement the rules in absolute good faith. As stated in the commentary to Additional Protocol I in respect of the principle of proportionality: *"Even if this system is based to some extent on a subjective evaluation, the interpretation must above all be a question of common sense and good faith for military commanders."*[95]

The interpretation and practical application of these rules raise a number of difficulties. For example, with regard to the crucial task of conducting proportionality assessments, the International Tribunal for the former Yugoslavia (ICTY) Ad Hoc Committee established to review allegations of IHL violations during the NATO bombing campaign against the Federal Republic of Yugoslavia stated that *"the main problem with the principle of proportionality is not whether or not it exists but what it means and how it is to be applied".*[96] Some of the questions identified by the committee that remain unresolved in this regard include how to measure and compare the different "values" of military advantage and incidental civilian harm, and the extent to which a commander is

[91] AP1, Art. 52(2)
[92] Droege C. 2012 *op cit* 2 pg 558
[93] International Committee of the Red Cross, 2011. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of the 32nd International Conference of the Red Cross and the Red Crescent EN 321c/15/11, Geneva, pg 41
[94] *ibid*
[95] International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva, ICRC/ Martinus Nijhoff, 1987, pp 683-684.
[96] ICTY Ad Hoc Committee, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, para 49.

required to expose his/her own forces to danger in order to limit civilian harm.[97]

Other challenges to consistent application of the proportionality principle relates to the fact that assessments will depend on individual contexts, and by whom, where and when they are made. For example, the relative value assigned to the anticipated military advantage versus expected civilian losses would likely be judged differently by a military commander and an IHL lawyer or even by different military commanders, depending on their experience and background.[98] There are also different views as to whether the proportionality test must be applied to each element of an attack or to the attack as a whole.

Consequently, it is difficult to question decisions made by commanders in particular cases and to assess whether they have done everything feasible to minimize incidental civilian harm. This challenge was highlighted by the ICRC in a guide developed to assist militaries in integrating IHL during their operations when it stated that *"law is … sometimes too general to serve as a guide for practical behavior in combat …. It is therefore necessary to interpret it, analyze its operational implications and identify consequences at all levels."*[99]

This same interpretation challenge is faced in respect of most of the terms to which strict definitions are not given in IHL. Their interpretations are left at the mercy of whoever is to apply them at a particular time. The fate of civilians is therefore largely left at the whims and caprices of military commanders and decision makers. The situation is even more capricious in cyber-warfare as most of the cyber-operators who carry out these attacks are not trained army personnel. They are not abreast with the IHL rules and principles. It is difficult for them to make decisions in compliance with rules whose existence they are oblivious of. Even where they are military personnel and therefore, have knowledge of the rules, they will still experience difficulties in applying the existing rules of IHL to cyber-warfare. This is because the rules do not specifically address cyber-warfare with all its peculiarities. They will have to adapt the existing rules to cyber-warfare, and the absence of a standard international guideline poses a huge challenge. There is a need to provide an international standard that will serve as a guide to decision makers in the conduct of cyber-attacks.[100]

6.2. Dual Use Objects In Cyber-Space

A dual-use object is one that serves both civilian and military purposes.[101] Examples of common dual-use objects (or objectives) include airports, rail lines, electrical systems, communications systems, and factories that produce items for both the military and the civilian population.[102] The interconnectedness of civilian and military in cyber-space poses a challenge to the protection of civilians and civilian objects in cyber-space. IHL allows attacks to be made on combatants and military objectives and prohibits attacks on civilians and civilian objects. Compliance with this in cyber-warfare is difficult as military and civilian infrastructures in cyber-space are interwoven. Military infrastructures are military objectives and therefore legitimate objects of attack. Since most military networks rely on civilian cyber infrastructure, and it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures, attacks on such military networks will occasion incidental damage on the civilian infrastructure.

The position in IHL is that when a particular object is used for both civilian and military purposes, it becomes a military objective, except for the separable parts thereof, and therefore a legitimate object of attack. Applying this strictly to cyber-warfare could lead to the conclusion that many objects forming part of the cyber-space infrastructure would constitute military objectives and would not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ensuing impact that such a loss of protection could have in terms of disruption of the ever-increasing concomitant civilian usage of the cyber-space. IHL even permits a certain level of collateral damage on civilians and civilian objects provided that such damage is not in excess of the actual military advantage gained from the attack. The military advantage has to be assessed and measured against the incidental harm to civilians. The protection of civilians in this situation hangs on the result of the assessment.

In cyber-warfare, a proper assessment will entail knowing enough about the cyber linkages between the sending computer and the targeted computer to be sufficiently assured that the attack will in fact engage the intended target.[103] The operator will also need to know enough about the characteristics of the particular cyber capability that is being used to undertake the attack to be assured that it will engage the target in the intended way.[104] Also, he will need to know enough about the targeted computer system, its dependencies, and associated networks to be able to assess the proportionality of the planned attack. Finally, if the cyber capability to be used in the attack is liable to affect other

[97] *Ibid* para 49
[98] *ibid* para 50
[99] International Committee of the Red Cross, 2017. *Integrating the Law*, Geneva p 17 Retrieved on 1st August, 2017 from www.icrc.org
[100] Kelsey, J. T.G. 2008 'Hacking into international humanitarian law: The prince-les of distinction and neutrality in the age of cyber warfare' Michigan Law Review pg 106
[101] Schmitt, M. N. 2002 Wired warfare: Computer network attack and *jus in bello, International Review of the Red Cross* Vol. 84 No 846: 398
[102] *ibid*
[103] Boothby, W. 2012. Some Legal Challenges posed by Remote Attack *International Review of the Red Cross* Vol. 94 No 886 , pg 587
[104] *ibid*

networks as it travels to the targeted system, the expected effects on those other networks will need to be assessed as, to the extent that those networks do not themselves consist of military objectives. Damage to them, and consequential damage or injury to their users will have to be factored into the proportionality assessment that is made in advance of the decision to mount the cyber-attack.[105] This assessment is particularly difficult because civilian and military networks are so critically interconnected that incidental civilian harm must be expected in most cases, and it is almost impossible to foresee all possible harm including incidental harm indirectly caused by the reverberating effects of the attack. It is difficult to limit the effects of attacks, as required by IHL.

A lot will depend on the particular cyber tool that is planned to use, on the characteristics of that tool, on whether the damaging effect of the cyber tool can be reasonably limited to the intended target of attack, and on whether enough is known about the target computer system to enable proper precautionary judgments of the sort discussed above to be made. API requires that *'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by [API] or by any other rule of international law applicable to the High Contracting Party'*.[106] In line with this provision, a review of cyber capabilities that are to be used to cause death, injury, damage or destruction to an opposing party to a conflict is required. In carrying out the review, the matters discussed in the previous paragraph will need to be considered when deciding whether the capability is indiscriminate by nature.[107]

6.3. Challenges In Protecting Essential Civilian Data

The existing rules of IHL were made with the aim of protecting civilians and civilian objects from physical injuries and damage to physical objects in order to minimize human suffering in situations of armed conflict. The cyber realm presents a new kind of object that requires protection – data. There is an increasing concern about safeguarding essential civilian data. Important civilian data such as social security data, tax records, hospital records, bank accounts, companies' client files or election lists or records are now stored in the cyber-space. These data are exposed to attacks which could result in their loss. The loss of such data could easily bring government services and private businesses to a complete standstill, and could cause more harm to civilians than even the destruction of physical objects.

Under the existing rules of IHL, there is no provision for the protection of data. An operation which would lead to the loss of data would not be prohibited by IHL in today's ever more cyber-reliant world, either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an object that would bring into operation the prohibition of attacks on civilian objects.[108] This position defeats the purpose of IHL which is to reduce human suffering in armed conflict.

The world is evolving. Technological developments have brought innovations in every area of life, including warfare. The new means and methods of warfare brought about by technological development has widened and increased the causes and nature of human suffering. In response to these developments, IHL has made rules to prohibit and or regulate some new means and methods of warfare which were seen to cause superfluous and unnecessary human suffering. For instance, the Convention prohibiting or restricting Certain Conventional Weapons, the Cluster Munitions Convention, the Landmines Convention, the Chemical Weapons Convention, were all made to prohibit or regulate new weapons brought about by technological developments, the use of which occasioned superfluous and unnecessary human suffering in armed conflicts. While it is true that all these conventions aim to protect humans from suffering arising from physical injury or damage to physical objects, it does not preclude the possibility of making rules to protect civilians from sufferings arising from other causes other than physical injury, and in this case, loss of data. There is a need to make rules to protect civilians from suffering arising from loss of data as it can also be as critical as or even more critical than physical injury.

6.4. Anonymity Of Attackers

The enforcement of IHL thrives on the concept of attribution. To attribute responsibility in IHL, the source of the attack must be identified. Cyber-warfare raises a number of issues with regards to attribution of responsibility. The identification of attackers is difficult as many cyber-operators are located far from the armed conflict and a cyber-attack can be carried out from any part of the world. The remoteness of the cyber-operator from the consequences of his or her activity makes it difficult to determine first, who undertook the cyber-operation in question. Second, on behalf of which state or organization, if any, the operation was undertaken and, third, its purpose. In the absence of information on the cyber-operator, it is difficult to attribute responsibility or even establish that the attack was carried out in furtherance of an armed conflict.

6.5. The Cost Of Combating Cyber Warfare And Lack Of Requisite Technical Skills

The lack of the requisite technical know-how and the cost of combating cyber-warfare is a huge challenge to the protection of civilians. The evolving threat landscape and its innate dynamism continue to place demands on governments and

[105] *ibid*
[106] AP I Article 36
[107] Boothby, W. H. 2009. Weapons and the Law of Armed Conflict, Oxford: Oxford University Press, pp. 69–85 and 345–347.
[108] ICRC, 2011. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of the 32nd International Conference of the Red Cross and the Red Crescent EN 321c/15/11, Geneva,

regulators across the world to develop and implement robust frameworks, policies that can engender the capacity to effectively manage cyber-risks. Cyber-security talents are becoming increasingly difficult to find in today's ever growing and dynamic technology world. Effectively combating cyber-warfare requires young skilled cyber-security professionals who are proactive and willing to combat existing cyber-security threats. However, there is dearth of talents in this regard. In the absence of readily available talents, the services of the available few can only be sought at a very high cost. With the cost involved in preventing and combating cyber-warfare, it is quite difficult for nations, especially the third world to effectively protect their citizens.

VII. RECOMMENDATIONS

The paper proposes the following recommendations:

1. ADOPTION OF SPECIFIC LEGAL FRAMEWORK FOR CYBER-WARFARE: To ensure adequate and effective protection of civilians in cyber-warfare, the need to adopt a specific legal framework to regulate cyber-warfare is critical for various reasons. First, the general rules and principles of IHL are ill fitted to cyber-warfare and an attempt at a symbiosis will occasion great hardship, naturally engendered by the peculiarities of the latter. Second, the extant rules of IHL directly apply to kinetic conflict in the conventional realm and apparently, do not contemplate hostilities prosecuted in the cyber-space, which is a different domain with its own unique characteristics. Also, the nature of injury inflicted by cyber-attacks and the nature of objects and infrastructure affected differs significantly from that in the conventional realm. An effective protection of civilians from the consequences of cyber-attacks requires recognition of the cyber domain as *sui generis* and adoption of rules and principles that fully encompass and address the intricacies associated with it, thereby eliminating the shortages incurred by the current regime. Just like we have specific conventions for armed conflicts on land and sea, the best way to provide for the protection of civilians in the cyber-realm is to provide a specific legislation to govern armed conflicts prosecuted on this domain.

2. PROTECTION OF DATA: The absence of provisions in IHL for the protection of data or information in the cyber-space is one of the challenges highlighted in this work. The rules of IHL were made for situations of kinetic conflict and situations of the nature presented by cyber-warfare were not envisaged at the time. IHL prohibits attacks on civilians, civilian objects and other objects indispensable to the survival of civilians in situations of armed conflicts. Thus, the protection afforded to civilians is in respect of injuries and/or losses of a physical nature. The cyber-realm presents a different kind of object that needs to be protected in the interest of civilians – data/information. Just as the destruction of physical civilian objects can cause suffering among the civilian population, the loss of data and other cyber-infrastructure can also occasion grievous harm and suffering to the civilian population. There is therefore, a need to extend the protection afforded to civilian physical objects to also include data/information as well as other critical cyber-infrastructure. This can be done by recognizing data/information as a civilian object and, therefore, subject to the core principles of IHL.

3. REVIEW OF NEW CYBER WEAPONS: Article 35(1) of Additional Protocol I places a limitation on the means and methods of warfare. Also, weapons that are by nature, indiscriminate, are prohibited. Thus, weapons that cannot be directed at a specific military objective or whose effect cannot be limited as required by IHL and thus, are of a nature to strike military objectives and civilians or civilian objects without distinction are prohibited. The interconnectivity of cyber-space and the resultant intertwinement of military and civilian infrastructures requires strict adherence to this rule if civilians are to be protected from the effects of cyber-attacks. States should therefore ensure the legal review of cyber-weapons, means and methods of warfare to assess their lawfulness under IHL before they proceed with the development or acquisition of such weapons.

4. INCORPORATION OF NATIONAL VIEWS: International policy debates on cyber-warfare should be geared towards streamlining the various national views on cyber-attacks, reaching a mutual understanding on how IHL might or might not apply to cyber-attack, the significance of non-state parties that might launch cyber-attacks, and how nations should respond to such attacks. There is a need for an international consensus on how IHL applies to cyber-warfare.

VIII. CONCLUSION

As with most phenomenal human developments, cyber-technology continues to evolve, with the attendant results of accessibility, high patronage, and unfortunately, corresponding complexities in its abuse. The exigent need to provide for a more effective and specific normative framework to regulate this means and method of warfare cannot be overlooked. While the current regime of IHL generally suffices to safeguard its intended audience from the regular aftermaths of cyber-attacks, and even though the promise of stretching this protection to novel aspects may be present, it is indisputable that significant prescriptive fault lines do exist. It is therefore imperative that a more comprehensive and definitive regulation be advanced to accommodate the unfolding peculiarities in the conduct of hostilities in the cyber-space.

BIBLIOGRAPHY

BOOKS

[1] Boothby, W. H. 2009. Weapons and the Law of Armed Conflict, Oxford: Oxford University Press
[2] Dinniss, H. H. 2012. Cyber Warfare and the Laws of War, Cambridge: Cambridge University Press.
[3] Dinstein, Y. 2004. The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge: Cambridge University Press

[4] Fleck D., (Ed.), 2013. The Handbook of International Humanitarian Law, 3rd Edn Oxford: Oxford University Press
[5] Gasser, H. P. 1993 Humanity for All: the International Red Cross and Red Crescent Movement, H. Haug (ed.), Berne: Paul Haupt Publishers
[6] Harvey, C., Summers J., and White N., (eds.), The Laws of War: Fit For Purpose? Essays in Honour of Professor Peter Rowe, Cambridge University Press
[7] Henckaerts, J. M. and Doswald-Beck, L. (eds.), 2005 Customary International Humanitarian Law: a contribution to the understanding and respect for the Rule of Law in Armed Conflict. Cambridge: Cambridge University Press
[8] Hughes, R. Towards a Global Regime for Cyber Warfare Cyber Security Project, Chatham House, London
[9] Pictet, J. 1952. Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva
[10] Roberts, A and Guelff, R., 2000. Documents on the Laws of War, 3rd ed., Oxford: Oxford University Press
[11] Roxana G. R. 2012. The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security, Power in the 21st Century, International Security and International Political Economy in a Changing World, Enrico Fels, E., Kremer J., and Kronenburg K.,(eds) Germany: Springer-Verlag Berlin Heidelberg.
[12] Sandoz, Y., Swinarski, C., and Zimmermann, B. (eds), 1987. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva: Martinus Nijhoff
[13] Schmitt, M. N. 2013. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press

JOURNALS

[1] Alexander, K. B. 2007. Warfighting in Cyberspace, Joint Force Quarterly, issue 46, 3rd Quarter
[2] Antolin-Jenkins and Vida M. 2005 'Defining the parameters of cyberwar operations: Looking for law in all the wrong places?' Naval Law Review
[3] Boothby, W. 2012. Some Legal Challenges posed by Remote Attack International Review of the Red Cross Vol. 94 No 886,
[4] Brown, D. 2006. *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*. Harvard International Law Journal: Harvard
[5] Brown, G. 2011'Why Iran didn't admit Stuxnet was an attack', in Joint Force Quarterly, Issue 63, 4th Quarter, p. 71,
[6] Droege, C. 2012 Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians International Review of the Red Cross, Vol. 94 Number 886
[7] Dunlap, C. J. 2011. Perspectives for cyber strategists on law for cyberwar, Strategic Studies Quarterly 123
[8] Geiss, R. and Lahmann, H. 2012. Cyber warfare: applying the principle of distinction in an interconnected space, Israeli Law Review, Vol. 45, No. 3 : 2.
[9] Haslam, E. 2000. Information Warfare: Technological Changes and International Law, Journal of Conflict and Security Law, Vol. 5
[10] Lin, H., 2011. Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion, Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity
[11] International Court of Justice, Legality of the threat or the use of nuclear weapons, Advisory Opinion, 8 July 1996, ICJ Reports 226, 1996. Paragraph 86
[12] International Committee of the Red Cross, 2006. A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 26 of Additional Protocol I of 1977, Reports and Documents. International Review of the Red Cross, Vol 88 No 864: 933
[13] International Committee of the Red Cross, 2015. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32nd International Conference of the Red Cross and Red Crescent, EN 32IC/15/11
[14] Kelsey, J. T.G. 2008 Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare Michigan Law Review 529
[15] Lawand, K. 2006 Reviewing the legality of new weapons, means and methods of warfare, Reports and Documents, International Review of the Red Cross, Vol. 88 No 864
[16] Lin, H. 2012. Cyber Conflict and International Humanitarian Law, International Review of the Red Cross. Vol 94. No886: 518
[17] Schindler, D. 1979. The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols, RCADI, Vol. 163: 147.
[18] Schmitt, M. N. 2012. 'Classification of cyber conflict', Journal of Conflict and Security Law, Vol. 17, Issue2,
[19] Schmitt, M. N. 1999. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Colombia Journal of Transnational Law, Vol. 37
[20] Schmitt, M. N. 2011. Cyber operations and the jus in bello: key issues, Naval War College International Law Studies, Vol. 87: 91
[21] Schmitt, M. N. 2002 Wired warfare: Computer network attack and jus in bello, International Review of the Red Cross Vol. 84 No 846: 369

ARTICLES

[1] Broad, W. J., Markoff, J., and Sanger, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times. January 15, 2011.
[2] Tikk, E.; Kaska, K.; Runnimeri, K.; Kert, M.; Taliharm, A., E tal. 2008 Cyber Attacks Against Georgia: Legal Lessons Identified, Cooperative Cyber Defence Centre of Excellence.

ONLINE MATERIALS

[1]. American Red Cross, Summary of the Geneva Conventions of 1949 and Their Additional Protocols. International Humanitarian Law, April 2011. Retrieved on 28th May, 2017 from www.redcross.org/ih
[2]. Department of Defense, 2006. National Military Strategy for Cyberspace Operations. Retrieved on 24th June, 2017 from http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf.
[3]. Dörmann, K. 2004 'Applicability of the Additional Protocols to Computer Network Attacks', ICRC, 2004, p. 3, retrieved on 14th May, 2017 from : http://www.icrc.org/eng/resources/documents/misc/68lg92.htm
[4]. International Committee of the Red Cross, Commentary on the Fourth Geneva Convention: Convention (IV) Relative to the protection of Civilians in Time of War Retrieved on 28th May, 2017 from https://ihl-databases.icrc.org/ihl/full/GCIV-commentary
[5]. International Committee of the Red Cross 2012. Summary of the Geneva Conventions of 12 August 1949 and their Additional Protocols 2nd Edn Geneva: ICRC Retrieved on 31st May, 2017 from www.icrc.org/eng/assets/files/publications/icrc-002-0368.pdf
[6]. International Committee of the Red Cross 2014. The Geneva Conventions of 1949 and their Additional Protocols. Retrieved from https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols on 11th May, 2017
[7]. International Committee of the Red Cross, 2016. Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 2nd edn, Retrieved on 28th May, 2017 from https://ihl-databases.icrc.org/ihl/full/GCI-commentary.
[8]. International Committee of the Red Cross, 2008. "How is the Term 'Armed Conflict' Defined in International Humanitarian Law"? Opinion Paper, Retrieved from https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf

[9]. International Committee of the Red Cross, 2017. Integrating the Law, Geneva. Retrieved on 1st August, 2017 from www.icrc.org
[10]. Julian, T. 2014. Defining Moments in the History of Cyber-Security and the Rise of Incidental Response retrieved on 24th June,2017 from https://www.infosecurity-magazine.com/opinions/the-history-of-cyber-security/
[11]. McMillan, R. 2008. NATO to Set Up Cyber Warfare Center, Network World. May 14, 2008. Retrieved on 24th June, 2017 from http://www.networkworld.com/news/2008/051508-nato-to-set-up-cyber.html.
[12]. Melzer, N. 2011. Cyberwarfare and International Law, UNIDIR Resources Paper, p. 24, retrieved on 14th May, 2017 from: http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf.
[13]. Nelson, C. 2011. Cyber Warfare: The Newest Battlefield. Retrieved on 4th July, 2017 from http://www.cse.wustl.edu/~jain/cse571 11/ftp/cyberwar/index.html
[14]. Rivera, J. 2014. A Theory of Cyber Warfare: Political and Military Objectives, Lines of Communication, and Targets, Georgetown Security Studies Review. Retrieved on 24th June, 2017 from http://georgetownsecuritystudiesreview.org/2014/06/10/a-theory-of-cyber-warfare-political-and-military-objectives-lines-of-communication-and-targets/
[15]. Waszink, C. 2011. Protection of Civilians under International Humanitarian Law: Trends and Challenges NOREF Report, Norwegian Peace Building Resource Centre. Retrieved from**http://www.operationspaix.net/DATA/DOCUMENT/6547~v~Protection_of_Civilians_Under_International_Humanitarian_Law__Trends_and_Challenges.pdf** on 1st August, 2017
[16]. Young, R. M. 2009. Protection of Civilians in Situations of Armed Conflict, UNITAR Workshop, ICRC NYC. Retrieved on 1st August, 2017 from **https://www.unitar.org/ny/sites/unitar.org.ny/files/IV_ICRC_Protection%20of%20Civilians%20UNITAR%20-%20Sept%2009.ppt-final.pdf**