A Case Of Incapacity: The Interrogation Of International Humanitarian Law as a Satisfactory Regulator Of Cyber Warfare.

Maonga, Sharon Kerubo

ADM. No. 078337

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Laws (LL.B), of Strathmore University

Strathmore Law School

2017

DEDICATION

I dedicate this to God almighty for His Grace and to my mother and father for their undivided support.

ACKNOWLEDGEMENTS

I am greatly indebted to Mr. Allan Mukuki for his vehement imparting of International Humanitarian law that enflamed my desire to write on a matter centered on IHLand his guidance as a supervisor of my dissertation. I acknowledge the guidance of Ms Anne Kotonya for her positive criticism and effort at the preliminary stages of my dissertation writing and oral defense. I extend my sincere gratitude to the Strathmore Community for their support.

DECLARATION

I declare that this dissertation is my original work and has not been submitted for the award of a degree or any other award in any other University.

Signature: Date:

Maonga, Sharon Kerubo

Adm. No. 078337

Supervisor

This dissertation has been submitted for examination with my approval as University Supervisor.

Signature: Date:

MrAllan Mukuki

Strathmore Law School

Comment [AM1]: Is this still the position?

ABSTRACT

Cyber warfare for it is a new concept in the conduct of war and is thus not properly understood hence considered a grey area with inadequate legislation. This dissertation seeks to bring to light the emergence and steady growth of cyber warfare as a method of war and to emphasize on the pressing need to regulate such wars. War is inevitable and many States are adopting this method of war because it harbors many benefits for the perpetrators who at first instance have their identity sealed and this enables them to escape liability for such actions. International Humanitarian Law is presently the legal basis through which cyber warfare is regulated. This paper offers an in-depth understanding of the 'law of war' vis-à-vis Cyber warfare. It seeks to examine the principles, philosophies, scope, laws, policies, rules and the rationale of International Humanitarian Law as a foundational basis to its applicability to Cyber warfare. It also looks into the manifestations of cyber warfare in the recent past and present as well as other institutional and regulatory influences in this field such as the Tallinn Manual which further provides that there are no treaty provisions directly addressing cyber warfare and although International law may also derive from custom, it is difficult to establish given the novelty of the field whether there is always enough available material and practice to draw conclusions of customary law from. This dissertation also offers some recommendations for future success in the regulation of cyber war.

LIST OF ABBREVIATIONS

IHL	International Humanitarian Law
ICRC	International Commission of the Red Cross
IAC	International Armed Conflict
NIAC	Non International Armed conflict
NATO	North Atlantic Treaty Organisation
NATO CCD	North Atlantic Treaty Organisation Cooperative
CoE	Cyber Defence Centre of Excellence
UN	United Nations
OAS	Organisation of American States
SCO	Shanghai Cooperation Organization
US	United States of America

LIST OF TABLES AND FIGURES

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION TO THE STUDY

1.1 Background

The advancement of technology over the recent years has given rise to new and unconventional means and methods of warfare. Examples of these 'new technologies' include but are not limited to; drones, automated weapon systems, nanotechnology weapons and cyber warfare[1]. Not only is there presently, fighting capabilities on land and at sea, but also in cyberspace.[2]

Cyber warfare is the conduct of military operations on a virtual realm against or via a computer or computer system through a data stream.[3]The Tallin manual refines the definition of Cyber warfare as including cyber attacks and cyber operations further stating that a cyber operation is a sufficient basis for a claim of cyber warfare[4]. The ICRC defines it as any hostile measures against an enemy designed to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer[5]. It consists of nation-states using cyberspace to achieve essentially the same ends they would pursue through military force. These ends include achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them.[6]This form of military conflict exists in information warfare units to develop viruses to attack enemy computer systems and networks.[7]Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system. By these means, a variety of 'targets' in the real world can be destroyed, altered or disrupted, such as industries,

Comment [AM2]: You can refer to the attempt in the Tallinn Manual

[1]ICRC, 'New Technologies and Warfare' International Review of the Red Cross, 2012.
[2] US Department of Defense, 'US Cyber Command Fact Sheet', US Department of Defense Office of Public Affairs, 25 May, 2010
[3]Herbert Lin, 'Cyber conflict and international humanitarian law' International Review of the Red Cross, 2012, 94(886), 517.
[4]Tallin Manual 2017
[5]International Committee of the Red Cross, *No Legal Vacuum in Cyber Space*, Aug. 16, 2011
[6] Susan Bremner, Cyberthreats: The Emerging Fault Lines of the Nation State, Oxford University Press, Oxford, 2009, p. 65.
[7] Office of the Secretary of Defense, 110th Congress, Annual Report to Congress: Military Power of the People's Republic of China, 2007, p. 22, available at: http://www.defenselink.mil/pubs/china.html

infrastructures, telecommunications, or financial systems.[8]

Cyber operations enable enemy states to commit acts of war without mobilizing their armies. The objectives of cyber-attacks are more inclined towards sabotage and espionage rather than to armed conflict.[9] Although occurring in a virtual space, the effects may felt in reality. For instance, the Stuxnet virus[10]altered the operating conditions for the Iranian uranium enrichment centrifuges, which ultimately resulted in physical damage to those centrifuges.[11]

The tools and techniques of conflict in cyberspace can be separated into tools based on technology and techniques focusing on human beings. Each type is further classified as offensive or defensive tools and techniques[12]. Offensive tools and techniques allow a hostile party to do something undesirable. Defensive tools and techniques seek to prevent a hostile party from doing so.

An offensive technology based tool requires three components namely: Access, vulnerability and payload[13]. *Access* refers to how the hostile party gets at the Information Technology of interest. The access may be remote or may require proximity to the Source of Information. *Vulnerability* is the 'weak point' from which the system can be infiltrated mostly due to the lack of adequate security in the system. The *payload* is the mechanism for affecting the System after access has been used and vulnerability has been taken advantage of.[14]For example, if a virus has entered a computer it's payload may be the fact that the system can now be used to re-program data or destroy it altogether. Examples of defensive tools used in technology based include firewalls, which close off

Comment [AM3]: Source???

[8]Herbert Lin, 'Cyber conflict and international humanitarian law' 518.
[9] William Jackson, 'Cyber attacks in the present tense, Estonian says', in Government Computing News, 28 November 2007, available at http://www.gcn.com/online/vol1_no1/45476-1.html.
[10] A computer worm believed to have been built jointly by American and Israel and is classified as a cyber-weapon. The worm specifically targets programmable Logic controllers.
[11] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 29, p. 36–37.
[12] Herbert Lin, 'Cyber conflict and international humanitarian law' (2012) 94(886) International Review of the Red Cross
[13]Herbert Lin, 'Cyber conflict and international humanitarian law' (2012) 94(886) International Review of the Red Cross, 517.
[14]Herbert Lin, 'Cyber conflict and international humanitarian law' (2012) 94(886) International Review of the Red Cross, 517.

routes used to access the information, or other programs that identify intruder activity. Offensive people based techniques arise when an inside person is blackmailed, tricked or bribed into allowing the hostile party access the information through purely technological means.[15]For example, by bribing a programmer to re-write a defective code. There still exists a technological approach in this setup, since the attack is occurring on a virtual realm. Defensive people-based techniques essentially involve retaliation to acts that compromise the security of the state**.**

The most common actors are known to be States having potent offensive cyber capabilities. The main perpetrators of cyber exploitation and cyber-attack are sub-national parties who are mostly individuals, and mostly for profit as well as terrorist groups.[16]The reasons for cyber warfare include but are not limited to, personal reasons, military, political and financial reasons.[17]. This is because a large form of commerce these days is conducted via the internet and a lot of valuable information is currently accessible online[18], especially after the advent of the Cloud, for instance, trade secrets, credit card information, negotiation strategies and contracts to name but a few. Another loftier reason for conducting such attacks is political advantage. The perpetrators may conduct cyber exploitations and attacks in order to send messages to the adversary, to gather intelligence for National purposes, to persuade or influence another party to behave in a certain manner or to dissuade the opponent. [19]

Comment [AM4]: Sources??

1.2 Statement of the problem

International humanitarian law, also known as the law of war, is a set of rules, which seek, for humanitarian reasons,to limit the effects of armed conflict. [20] In as much as Cyber warfare is a type of war and can occur between states, in some instances, it does not amount to armed conflict. IHL is presently the legal basis through which cyber warfare is regulated. Cyber warfare is presumed to be the war of the future as a result of digital migration due to the advancement of technology. For this reason it is imperative

[15] Herbert Lin, 'Cyber conflict and international humanitarian law' 518.
[16]Herbert Lin, 'Cyber conflict and international humanitarian law' 519.
[17]Herbert Lin, 'Cyber conflict and international humanitarian law' 520.
[18] https://www.peterindia.net/E-businessOverview.html
[19]Herbert Lin, 'Cyber conflict and international humanitarian law' 520.
[20] Advisory service on International Humanitarian Law, ICRC July 2004

that Cyber warfare is adequately regulated in order to ensure future warfare is controlled.In the US, some public policy experts have declared the proximity of cyber warfare is and acknowledge the need for other nations to respond to this threat opting for a call to action'reminiscent of the cold war era'.[21]

1.3 Research Objectives

Comment [AM5]: Have a main objective and specific objectives which inform your research questions and thereafter your chapter breakdown

1. To identify an ideal the regulatory approach to Cyber warfare.
2. To confer an understanding the relationship between International Humanitarian law and Cyber warfare
3. To identify other regulatory approaches to Cyber warfare

1.4 Research questions

1. What is the most suitable approach to take in the effective regulation of Cyber warfare?
2. Is IHL a sufficient regulatory approach to Cyber warfare?
3. What other Laws inform the regulation of Cyber warfare?

Comment [AM6]: Your research questions should be a mirror of your research objectives

1.5 Justification and Scope of Study

This paper seeks to bring to light the emergence and steady growth of cyber warfare as a method of war and to emphasize on the pressing need to regulate such wars. War is inevitable and many States are adopting this method of war because it harbors many benefits for the perpetrators who at first instance have their identity sealed and this enables them to escape liability for such actions. Secondly, Digital migration is a reality as well as a double-edged sword. This is because advancement in technology is unavoidable and in many cases viewed as a tool for economic development vis a vis the negative intention and effects of Cyber warfare. Cyber warfare is a contemporary means of warfare and is said to be 'the war of the future' and undeniably thus prevention is

[21] David Ignatius, Pentagon's cybersecurity plans have a Cold War chill, Wahington Post(August 26,20010) at A13.

better than cure. This study shall adopt an international scope because Cyber attacks and espionage are often conducted inter-state and the popularity of this new method of warfare is bound to gain even more popularity internationally.

1.6 Hypothesis

Cyber warfare is predestinedwar that falls beyond the scope of International Humanitarian Law.

1.7 Theoretical Framework

This study employs Sociological jurisprudence school of thoughtwith the main proponent being Roscoe Pound.

The Sociological theory focuses more on the ways laws develop in society rather than an analysis of legal texts. This is premised on the fact that the law has become an end in itself and without taking the social effects into consideration. Roscoe Pound stated 'in the past, we studied the law from within. The Jurists of today are studying Law from without' [22] The approach he identified as vitalto the question of sociological jurisprudence.Sociological Jurisprudence according to Roscoe Pound is a means of making legal rules effective, as well as studying the actual/real effects of the legal institutions and doctrines, sociological studies of the preparation of legislation particularly comparative legislation, sociological legal historyconsidering effects of legal doctrines that existed in the past, advocacy of reasonable and just solutions of legal cases and making effort more effective in achieving the purpose of law.[23] Pound classifies legal interests into three categories namely; Individual, Public and Social. He defines Individual interests as 'claims or demands or desires involved immediately in the individual's life and asserted in the title of that life'.[24] He defines Public Interests as 'claims or demands or desires involved in the life of a politically organized society and are asserted in title of that organization. They are commonly treated as the claims of a politically organized society thought of as a legal entity'.[25] He further defined Social

[22] Roscoe Pound, *The spirit of the Common Law*, Boston: Beacon press *(1921)* p 212.
[23] Roscoe Pound , The Scope and purpose of sociological Jurisprudence, 25 Havard Law Review (1912) p 514- 516.
[24] Roscoe Pound, *A Survey of Social Interests* 57 Havard Law Review 99 (1943)p 1-2.
[25] Roscoe Pound, *A Survey of Social Interests* 57 Havard Law Review 99 (1943)p 1-2.

interests as ‘Claims or Demands or desires involved in the social life in civilized society and asserted in title of that life’[26] These three interests are balanced out against each other which is the aim of social jurisprudence. Pound framed some assumptions referred to as ‘Jural postulates’, which he claims need not be tested against morality, as they are self sufficient and fit in with the functions of Law. This theory is based on the assumption that the interests sought by society are generally good.

1.7 Literature Review

Comment [AM7]: No literature review…. You have to analyze at least four authors in a thematic kind of format…. The themes are basically informed by your research questions….

Cyberspace is referred to as ‘‘not a ‘law-free’ zone where anyone can conduct hostile activities without rules or restraint” but which, in some circumstances, may be regulated by the law of armed conflict.[27] The International Committee of the Red Cross (ICRC) has steadfastly argued that many of the same principles that regulate battlefield combat also apply in cyberspace[28],which David Éricsimplifies as :do not attack non-combatants, attack combatants only by legal means, treat persons in your power humanely, and protect the victims.[29]

A humanitarian ambition ought to be the Protection of victims by giving them infrastructure indispensable for survival, and setting up monitoring bodies.[30]Scholars biased to the notion that International law is the only avenue of dealing with the problem of Cyber warfare offer that it is difficult to fit cyber problems into the rules on international law with respect to the use of force.[31]

Dinstein and Michael Schmitt[32] advocate for new interpretations of the rules on the use of force in order to have the right to respond to cyber problems with military force instead of looking at other international rules, such as those on non-intervention, countermeasures, economic law, and the like.

[26] Roscoe Pound, *A Survey of Social Interests* 57 Havard Law Review 99 (1943)p 1-2.
[27]Chris Borgen, *Harold Koh on International Law in Cyberspace*, OpinioJuris, September 19, 2012
[28]International Committee of the Red Cross, *Cyber Warfare*, Oct. 10, 2010
[29]David Éric, *Principes de droit des conflitsarmés*, Brussels, Bruylant,Edition 3, (2002), p 921-922.
[30] Maurice Frederic, ‘Humanitarian ambition’ IRRC, Vol.289,(1992) p 371.
[31]Y Dinstein, ‘Computer Network Attacks and Self-Defense’ (2002) 76 Intl Law Studies 99.
[32]MN Schmitt, ‘Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’ (1999) 37 Colum J Transnatl L 885

On the contrary, scholars such as Noah Schachtmanargue that the threat of cyber-attacks has been blown out of proportion to the detriment of preventing the real challenges to cyber security: cybercrime and espionage.[33]The objectives of cyber-attacks are more inclined towards sabotage and espionage rather than to armed conflict.[34] However cyber attacks may in certain situations amount to the use of force within the meaning of article 2(4) of the UN Charter[35] if the cyber attack proximately results in death, injury or significant destruction[36]

1.8 Design Methodology

This study seeks to use is conducted via qualitative research and analysis in dealing with the subject matter, a considerable emphasis on the history and literature on International Humanitarian Law and a comparative analysis of International Human Rights Laws with Cyber warfare. The Desk search shall constitute review of IHL statutes such as the Geneva Conventions I-IV, the Rome Statute commonly referred to as the Geneva Laws and Hague Laws respectively. The study shall make use of books, journal articles, conference papers and online journals as secondary sources.

1.9 Limitations

The concept of Cyber warfare is new in International Law and is seen as ambiguous or as a phenomenon. There is thus not enough literature on the subject matte

The Research design methodology chosen does not incorporate collection of primary data on the subject matter and is heavily reliant on desk research and secondary data. This affects the reliability of the research.

[33]P Singer and N Schachtman, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' Brookings Institution (15 August 2011)
[34] William Jackson, 'Cyber attacks in the present tense, Estonian says', in Government Computing News, 28 November 2007, available at http://www.gcn.com/online/vol1_no1/45476-1.html.
[35]Chris Borgen, *Harold Koh on International Law in Cyberspace*, OpinioJuris, September 19, 2012 *available* at http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/
[36]Chris Borgen, *Harold Koh on International Law in Cyberspace*, Opinio Juris, September 19, 2012 *available* at http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/

1.10 Chapter Breakdown

Chapter 1

Offers an introduction to the study as well as background information on the subject matter. This chapter provides the initial interaction with the concept of cyber warfare. This Chapter also delineates the scope of the study and the theoretical and practical basis through which the research is conducted.

Chapter 2

This chapter will offer an in depth understanding of International Humanitarian Law through examining the principles, philosophies and scope

Chapter 3

This Chapter shall analyze the ways in which Cyber warfare has been manifested internationally in the contemporary world.

Chapter 4

This chapter will also look into other laws that influence the regulation of cyber warfare.

Chapter 5

This chapter shall look into the findings, conclusions and recommendation

CHAPTER 2: THE RELATIONSHIP BETWEEN INTERNATIONAL HUMANITARIAN LAW& CYBER WARFARE

2.1 INTRODUCTION

This chapter confers an in-depth understanding of the law of war vis-à-vis Cyber warfare. It seeks to examine the principles, philosophies, scope, laws, policies, rules and the rationale of International Humanitarian Law as a foundational basis to its applicability to Cyber warfare.

2.2 What is International Humanitarian Law (IHL)?

International Humanitarian Law (IHL) is a set of rules, which seek for humanitarian reasons, to limit the effects of armed conflict.[37] It regulates States, International organizations and other subjects of International Law.[38] It aims to protect the rights of people who no longer directly take part in hostilities and restrict the means and methods of warfare.[39]

International Humanitarian Law has two branches namely: The Laws of Geneva and the Laws of The Hague.[40] The Laws of Geneva protects victims of armed conflict such as military personnel who are *hors de combats* and civilians who are no longer directly participating in hostilities[41]. The Laws of The Hague are a body of rules establishing the rights and obligations of belligerents in the conduct of hostilities and which limits means and methods of warfare.[42] IHL is a compromise between two underlying principles: military necessity and humanity.[43] Military necessity permits only that degree and kind of force required achieving the legitimate purpose of a conflict.[44] The principle of humanity forbids the infliction of all suffering, injury or destruction not necessary for achieving the legitimate purpose of conflict.

[37] www.icrc.org/eng/assets/files/other/what_is_ihl.pdf
[38] International Humanitarian law, 'Answers to your questions' (2014), 1.
[39] www.icrc.org/eng/assets/files/other/what_is_ihl.pdf
[40] International Humanitarian law, 'Answers to your questions' (2014), 5.
[41] International Humanitarian law, 'Answers to your questions' (2014), 5.
[42] International Humanitarian law, 'Answers to your questions' (2014), 5.
[43] www.icrc.org/eng/assets/files/other/what_is_ihl.pdf

[44] International Humanitarian law, 'Answers to your questions' (2014), 6.

States developed IHL mainly through the adoption of treaties and the formation of customary Law. Customary law is formed when State practice is sufficiently widespread, representative, frequent and uniform and accompanied by a belief among States that they are legally bound to act or prohibited from acting in certain ways.[45] The International Court of Justice stated in the *Continental Shelf case* stated "It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opiniojuris* of States[46] that is in State practice and belief that the state practice is required as a general practice accepted by law[47]

An armed conflict arises where there is a resort to armed force between states.[48]IHL applies only in situations of armed conflict: international and non-international armed conflict situations. International armed conflict occurs when one State resorts to war against another[49]The rues on IAC's apply to all situations of armed conflict which may arise between two or more of the High contracting Parties usually states, even if the state of war is not recognized by one of them.[50]As per common article 3, non- international armed conflict occurs when hostilities are taking part between the armed forces of state and organized non-state armed groups or between such groups.[51]

2.3 WHO does IHL protect?

IHL protects victims of armed conflict who are often civilians and combatants who have laid down their arms[52]. Combatants are all members of the armed forces of a party to the conflict, save for medical and religious personnel[53]. Civilians are defined as persons who

[45] International Humanitarian law, 'Answers to your questions' (2014), 7.
[46]ICJ, *Continental Shelf case (Libyan Arab Jamahiriya v. Malta)*, Judgment, 3 June 1985, *ICJ Reports* 1985, pp. 29–30, § 27.
[47]Article 38(1)(b), ICJ Statute
[48]*Prosecutor v Tadic*, ICTY (Case no. 211) part A para.70
[49] Article 1, Additional Protocol 1
[50] Article 2(1), Geneva Convention I-IV
[51] Article 1, Additional protocol 1
[52] Article 3, Geneva Convention I-IV
[53] Rule 3, ICRC Customary IHL Rules, ihldatabases@icrc.org

are not combatants.[54] The nature of the protection IHL provides varies and is determined by whether the person in question is a combatant or a civilian. Civilians are entitled to protection so long as they do not take up arms and participate in hostilities while Combatants are protected for as long as they lay down their arms.[55] Civilians are 'protected persons' under IHL when in the hands of a party to the conflict provided that they are not nationals of the enemy state[56], they are not nationals of an ally of the enemy state[57] they are not nationals of a neutral state[58]. The aim of IHL is to protect civilians from arbitrary acts of an adverse party because of their allegiance to its enemy. IHL prohibits indiscriminate attacks.[59] Protected civilians are entitled to respect of their dignity.[60]Maurice Frederic in his book Humanitarian Ambition wrote:

'*Protecting victims means giving them a status, goods and the infrastructure indispensable for survival, and setting up monitoring bodies. In other words the idea is to persuade belligerents to accept an exceptional legal order – the law of war or humanitarian law – specially tailored to such situations. That is precisely why humanitarian action is inconceivable without close and permanent dialogue with the parties to the conflict. '*[61]

2.4 Principles of IHL

IHL is governed by certain principles and rules. These include: Distinction between civilians and combatants, proportionality, precautions, prohibition against causing superfluous injury or unnecessary suffering, prohibition to attack *hors de combat*and the principle of necessity. Eric David in the *Principles De Droit De ConflitsArmes*stated:

[54] Rule 5, ICRC Customary IHL Rules, ihldatabases@icrc.org
[55] Rule 3, ICRC Customary IHL Rules, ihldatabases@icrc.org
[56] International Humanitarian law, 'Answers to your questions' (2014), 27.
[57] International Humanitarian law, 'Answers to your questions' (2014), 27.
[58] International Humanitarian law, 'Answers to your questions' (2014), 27.
[59] Rule 11, ICRC Customary IHL Rules, ihldatabases@icrc.org
[60] Article 5, Geneva Convention IV
[61] Maurice Frederic, 'Humanitarian ambition' IRRC, Vol.289,(1992) p 371.

'The law of armed conflicts is characterized by both simplicity and complexity – simplicity to the extent that its essence can be encapsulated in a few principles and set out in a few sentences, and complexity to the extent that one and the same act is governed by rules that vary depending on the context, the relevant instruments and the legal issues concerned. [...] The law of armed conflicts – as we have stated repeatedly – is simple law: with a little common sense and a degree of clear-sightedness, anyone can grasp its basic tenets for himself without being a legal expert. To put things as simply as possible, these rules can be summed up in four precepts: do not attack non-combatants, attack combatants only by legal means, treat persons in your power humanely, and protect the victims. [...] At the same time, the law of armed conflicts is complex since it does apply only in certain situations, those situations are not always easily definable in concrete terms and, depending on the situation, one and the same act can be lawful or unlawful, not merely unlawful but a criminal offence, or neither lawful nor unlawful! [62]

2.4.1 Distinction between Civilians and Combatants

Distinction is a key principle under international Humanitarian Law.Military objectives are those objects which "by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[63]

Thus, at a minimum, hospitals and medical units are to be afforded those protections accorded civilian objects and protected from attack, unless they satisfy the definition of military objective above. Similarly, medical personnel are protected from attack, provided they do not directly participate in hostilities.

[62]David Éric, *Principes de droit des conflits armés*, Brussels, Bruylant,Edition 3, (2002), p 921-922.
[63] Article 52(2), Additional Protocol I

Parties to a conflict must always distinguish between civilian objects and military objectives, and between civilians and combatants.[64] Operations may be directed only against military objectives and combatants and never to civilian objects or civilians.[65] Civilians lose their protection from attack if they directly participate in hostilities[66] or if they are being used to perform acts harmful to the enemy.[67]

In case of doubt, as to whether an individual is a civilian, "that person shall be considered to be a civilian."[68] In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military, that civilian object "shall be presumed" to be civilian and not to be making such an effective contribution.[69] The parties to the armed conflict "must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks."[70] The parties to the armed conflict "must, to the extent feasible, remove civilian persons and objects under its control from the vicinity of military objectives."[71] The presence of civilians shall not be used to render immune from attack military objectives. Similarly, the parties to a conflict shall not direct civilians to move or congregate in such a manner as to shield military objectives from attack.[72] It is important to note that a violation of one of these rules by one party to the conflict does not release the opposing party to the conflict from their legal obligations vis-à-vis the protections owed civilians and civilian objects.[73]

Comment [AM8]: This section is good, but what relation with you dissertation… You need to have a seamless connection always between the various parts to avoid them looking like haphazard placements in your work

2.4.2 The prohibition of indiscriminate attacks

Attacks that are indiscriminate in nature are prohibited.[74] Indiscriminate attacks are

[64] art. 48, Additional Protocol I; Rules 1, 7, ICRC Customary International Humanitarian Law Study
[65] art. 48, Additional Protocol I; Rules 1, 7, ICRC Customary International Humanitarian Law Study
[66] Art. 51, First Additional Protocol
[67] Rule 10, ICRC Customary International Humanitarian Law Study.
[68] Article 50 Additional Protocol I
[69] Article 52, Additional protocol I
[70] Article 51, Additional protocol I
[71] Rule 24, ICRC Customary IHL Rules, ihldatabases@icrc.org
[72] Article 51 , Additional Protocol I
[73] Article 51 Additional Protocol I
[74] Article 51, Additional Protocol I.

attacks where:

(a) which are not directed at a specific military objective;

(b) which employ a method or means of combat which cannot be directed at a specific military objective; or

(c) which employ a method or means of combat the effects of which cannot be limited as required by IHL, and are thus of a nature to strike military objectives and civilian or civilian objectives without distinction.[75]

Comment [AM9]: Also refer to Article 8 of the Rome Statute on Indiscriminate Killings

2.4.3 The principle of proportionality

The principle of proportionality prohibits the launching of an attack that "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."[76] Each party to the conflict is must do everything feasible to assess and ensure proportionality.[77]Prior to targeting a military object, if damage to civilian objects or civilian death or injury is anticipated, then an assessment must be undertaken in which the anticipated military advantage to be gained is weighed against the "collateral" damage to protected civilians or civilian objects that is anticipated.Thus, under IHL not every attack that results in civilian death or injury, or the destruction of a civilian object, is prohibited. Whether a strike was legal depends in part on whether the principle of proportionality was respected when the operation targeting the military objective was carried out.

2.5 Rationale of IHL as the Legal regulator of Cyber warfare.

IHL is commonly referred to as the Law of War. 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'. Cyberspace is referred to as ''not a 'law-

[75] Article 51 Additional Protocol I
[76]Rule 14, ICRC Customary International Humanitarian Law Study
[77]Rule 18, ICRC Customary International Humanitarian Law Study.

free' zone where anyone can conduct hostile activities without rules or restraint" but which, in some circumstances, may be regulated by the law of armed conflict.[78]The International Committee of the Red Cross (ICRC) has steadfastly argued that many of the same principles that regulate battlefield combat also apply in cyberspace[79]

Moreover, cyber attacks may in certain situations amount to the use of force within the meaning of article 2(4) of the UN Charter[80] if the cyber-attack proximately results in death, injury or significant destruction[81]

Comment [AM10]: You should add more information… And this is such an anti0climax to this chapter… You can do much better…. Summarize the arguments, show how IHL regulates cyber warfare… Article 36 AP1, Martens Clause, etc…..

3. CHAPTER 3: MANIFESTATIONS OF CYBER WARFARE

3.1 INTRODUCTION:

[78]Chris Borgen, *Harold Koh on International Law in Cyberspace*, Opinio Juris, September 19, 2012
[79]International Committee of the Red Cross, *Cyber Warfare*, Oct. 10, 2010
[80]Chris Borgen, *Harold Koh on International Law in Cyberspace*, Opinio Juris, September 19, 2012 *available* at http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/
[81]Chris Borgen, *Harold Koh on International Law in Cyberspace*, Opinio Juris, September 19, 2012 *available* at http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/

This Chapter shall analyze the ways in which Cyber warfare has been manifested internationally through the investigations of major cyber-attacks namely: Estonia, Stutnex that have occurred in the past decade and look into the approaches different States have had towards Cyber warfare.

3.2 Estonia

3.2.1Facts[82]

Disparities between Russia and Estonia arose in April 2002 when Estonia relocated the bronze soldier of Tallinn, a soviet-era war monument from the center of Tallinn. As a result a demonstrationwas carried out among Estonians of Russian descent who considered this monument as a symbol of honor to the Red army who fought against German Nazis. However, the non-Russian Estonian's viewed the monument as a foreign symbol and a disregard for their sovereignty and thus made yearly protests for its removal from Tallin. During protest by Estonian's of Russian origin, who viewed statue as a symbol of their right to be in Estonia, around 1300 people were arrested, 150 were injured, and one person killed. This incident also raged anger all across Russia and Russian computer experts turned to computer to attack Estonian's IT infrastructureEstonia was heavily dependent on IT services and thus this was a huge setback for the State. According to the CERT Estonia, 98% of banking transactions are done electronically, 66% population uses the internet, 55% households have computer at home, and 91% computers are connected to the internet.[83]Thus started the fifth dimension of 'cyber wars' besides the conventional mediums of air, ground, sea and space wars. Estonia implicated the Russian government for the attacks but Kremlin denied any type of involvement. Estonia has e-government also known as paperless government and even the parliament is elected over the Internet. Being highly dependent on electronic services, such a cyber attack against the country's IT systems can be catastrophic. Main targets of the attacks were: Estonian's Presidency and Parliament; Government Ministries ;Political Parties ; Famous news organizations ; Banks and Communication

[82] Muhammed Saleem ,'Cyber warfare the truth in a real case',https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf
[83]"Facts about Estonia", CERT Estonia, May 10, 2008 http://www.ria.ee/27525

infrastructure.[84]According to BBC [85]these were series of attacks carried out as a protest to deface government and other important websites. The famous British newspaper Telegraphy reported

"Estonia has been hit by a prolonged series of 'cyber attacks' that disrupted leading websites and caused alarm in Europe and the NATO alliance, it emerged last night"[86]

Table 1. Targeted Websites

Attacks	Destination	Address or owner
35	195.80.105.107/32	pol.ee
7	195.80.106.72/32	www.riigikogu.ee
36	195.80.109.158/32	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	195.80.124.53/32	m53.envir.ee
2	213.184.49.171/32	www.sm.ee
6	213.184.49.194/32	www.agri.ee
4	213.184.50.6/32	
35	213.184.50.69/32	www.fin.ee (Ministry of Finance)
1	62.65.192.24/32	

[87]

[85] "The cyber Raiders hitting Estonia", Thursday 17, 2007 http://news.bbc.co.uk/2/hi/europe/6665195.stm

[86]"Cyber Attack, Hit Estonia", May 18, 2007 http://www.telegraph.co.uk/news/worldnews/1551851/Cyber-attacks-hit Estonia.html

[87]*https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf*

Table 2. Number of Attacks

Attacks	Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11

[88]

Table 3. Duration of Attacks

Attack	Time
17	less than 1 minute
78	1 min - 1 hour
16	1 hour - 5 hours
8	5 hours to 9 hours
7	10 hours or more

[89]

3.2.3 Stuxnet

Stuxnet was originally detected in early 2010 by a computer security company in Belarus, and subsequently found to have infected (albeit without causing much actual harm) thousands of industrial control systems world- wide.[90]

What has been discovered is that the Stuxnet virus is malware that attacks widely used industrial control systems built by the German firm, Siemens AG. The company says the malware was initially distributed via an infected USB thumb drive memory device or devices, exploiting vulnerabilities in the Microsoft Windows operating system. Such systems are used to monitor automated plants - from food and chemical facilities to power generators. Analysts said attackers may have chosen to spread the malicious software via a thumb drive because many SCADA (Supervisory Control and Data

[88] *https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf*
[89] *https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf*
[90] Duncan Holis, *Could Deploying Stuxnet be a War Crime?* Opinio Juris (Jan 25, 2011),

Acquisition) systems are not connected to the Internet, but do have USB ports. Once the worm infects a system, it quickly sets up communications with a remote server computer that can be used to steal proprietary corporate data or take control of the SCADA system, said Randy Abrams, a researcher with ESET, a privately held security firm that has studied Stuxnet.[91]

As of September 25, 2010, Iran had identified "the IP addresses of 30,000 industrial computer systems" that had been infected by Stuxnet. According to Mahmoud Liaii, director of the Information Technology Council of Iran's Industries and Mines Ministry, the virus "is designed to transfer data about production lines from our industrial plants" to locations outside of Iran.[92]By 2011, it was still is not clear whether or if the attacks were over: Some experts examined the code and believe it contains the seeds for yet more versions and assaults.[93]

According to Symantec, Stuxnet targets specific frequency-converter drives — power supplies used to control the speed of a device, such as a motor. The malware intercepts commands sent to the drives from the Siemens SCADA software, and replaces them with malicious commands to control the speed of a device, varying it wildly, but intermittently. The malware, however, doesn't sabotage just any frequency converter. It inventories a plant's network and only springs to life if the plant has at least 33 frequency converter drives made by FararoPaya in Teheran, Iran, or by the Finland-based Vacon. Even more specifically, Stuxnet targets only frequency drives from these two companies that are running at high speeds — between 807 Hz and 1210 Hz. Such high speeds are used only for select applications. Symantec is careful not to say definitively that Stuxnet was targeting a nuclear facility, but notes that "frequency converter drives that output over 600 Hz are regulated for export in the United States by the Nuclear Regulatory

[91] *Factbox: What is Stuxnet?* Reuters (Sept. 24, 2010), http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb idUSTRE68N3PT20100924.
[92] Kerr, et al., *supra* note 6, at 3 (translated from *Iran Confirms Cyber Attack, Says Engineers 'Rooting Out' Problem*, Mehr News Agency, (September 25, 2010)).
[93] William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, The New York Times (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Commission as they can be used for uranium enrichment."[94]

Stuxnet is very specific about what it does once it finds its target facility. It accesses a vulnerable system and manipulates it. Once Stuxnet determines it has infected the targeted system or systems, it begins intercepting commands to the frequency drives, altering their operation and according to Symantec Company's Eric Chien other parameter changes may also cause unexpected effects."

"It is about destroying its targets with utmost determination in military style."[95]

Fig. 1 List of recent International Cyber attacks[96]

[94] Kim Zetter, *Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage*, Threat Level (Nov. 15, 2010)

[95] Broad, et al., *supra* note 14.

[96]Tallin manual Final report (2013).

	Significant cyber incidents	**Domestic Policy Developments**	**International Conferences, Significant publications and legislations**	**International policy development**
1982	Alleged Russian Pipeline explosion			
2000	Moonlight Maze			The Information Security Doctrine of the Russian Federation
2001			Budapest Convention on Cybercrime	
2005	Titan Rain			
2007	Cyber attack on Estonia			
	Cyber attack on Syria			
2008	Cyber attacks on Georgian websites			Estonian Cyber Security Strategy
				NATO first cyber defence exercise

2009	DDoS attacks against governmental, media and financial websites in US and S Korea	United Kingdom Cyber Security Strategy		
2010	Discovery of Stuxnet Malware Operation Aurora	Strategic Defence and Security Review initiates £650M National Cyber Security programme (later rising to £860M)	NATO Lisbon Summit identifies cyber domain as significant Security Risk	Canadian Cyber Security Strategy
	Pakistani 'Cyber Army' hack Indian Central Bureau of Investigation website			Japanese Information Security Strategy
	Indian 'Cyber Army' hack Pakistan Army and			South African Cyber Security Policy

	governmental websites _____			
	US Dept of Defence admit its internet traffic was rerouted via China for a short period			
	Google announce attacks			
	originating from China on its corporate infrastructure leading to IP theft			
2011	Japanese governmental and defence contractor websites targeted by cyber attacks	United Kingdom Cyber Security Strategy	London Conference on Cyberspace	Australian Cyber Security Strategy
	Shady RAT report _____		ICRC Report on International Humanitarian Law and the challenges of contemporary armed conflicts	US International Strategy for Cyberspace
			East West Institute Russia-US Bilateral on Critical Infrastructure Protection publication	Columbian Policy Guidelines on Cybersecurity and Cyberdefence

			‘Working Towards Rules for Governing Cyber Conflict’	
				Czech Republic Cyber Security Strategy
				French Cyber Security Strategy
				German Cyber Security Strategy
				Hungarian National Security Strategy
				Indian National Cyber Security Policy
				Lithuania Cyber Security Resolution
				Luxembourg National Cyber Security Strategy
				Polish Cyber Security Strategy
				The Netherlands National Cyber Security Strategy
				New Zealand Cyber Security Strategy
				Romanian Cyber Security Strategy
				Slovak Republic National Strategy for Cyber Security

				US International Strategy for Cyberspace
				Norwegian Cyber Security Strategy
2012	Discovery of Flame Malware		Budapest Conference on Cyberspace	Conceptual views on the Activities of the Armed Forces of the Russian Federation in Information Space (unofficial translation)
			National Cyber Security Framework Manual (NATO CCD CoE)	Austrian Cyber Security Strategy
				Swiss Cyber Security Strategy
2013	Syrian 'Electronic Army' hacks Twitter and Marines.com websites	Joint Forces Cyber Group takes command of development integration of Defence cyber capabilities and	Publication of Tallinn Manual	Finnish Cyber Security Strategy
	Snowden revelations	Joint Cyber Reserves open for recruitment	Seoul Conference on Cyberspace	Hungarian National Security Strategy

			EU Directive on Attacks against Information Systems	Indian Cyber Security Strategy
			University of California Institute on Global Conflict and Co-operation Workshop Report on China and Cybersecurity	Kenyan Cyber Security Strategy (pending)
				Montenegran Cyber Security Strategy (pending)
				Ugandan Cyber Security Strategy (pending)
				NATO annual cyber security exercise now largest of its kind – over 27 countries and partners participate

CHAPTER 4: OTHER LAWS AND APPROACHES TO CYBER WARFARE.

This chapter will also look into other existing laws and approachesthat influence the regulation of cyber warfare.This chapter shall offer insight to the scalability of Cyber warfare regulation for present and future managability.

Comment [AM11]: Surely? Such a 'flavourless' introduction

4.1.1 Countermeasures.

The Draft Articles on State Responsibility define countermeasures as "measures that would otherwise be contrary to the international obligations of an injured State *vis-à-vis* the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[97]The customary international law of countermeasures governs how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense—including, implicitly, cyber- attacks. The international law of countermeasures provides that when a state commits an international law violation, an injured state may respond with proportionality.Some cyber-attacks that do not rise to the level of an armed attack nonetheless violate the customary international law norm of nonintervention.[98]These violations may entitle a harmed state to use countermeasures to bring the responsible state into compliance with the law.

The Draft Articles provide that countermeasures must be targeted at the state responsible for the prior wrongful act and must be temporary and instrumentally directed to induce the responsible state to cease its violation.[99]Countermeasures under international law are however limited and obliged not to use force, as the principle of non -use of force as one of the seven principles of the UN Charter[100]Countermeasures should not violate human rights and ought to look into the interests of the people and not the state and thus reprisals against the wounded, sick,health forces, religious forces and civilians is banned.[101] They are obliged not to violate Jus cogens norms[102]and states ought to commit to peaceful

[97] Draft Articles,*supra* note 99, ch. II, commentary, para. 1.
[98]*supra*Subsection II.A.1.
[99] Article 48, Draft articlesupra note 99 article 49
[100] Article 2, UN Charter 1945
[101] Article 3, Geneva Conventions I-IV 1929
[102] Article 41, Draft Articles

settlement of disputes.[103]

The most important countermeasures in this context are known as “active defenses’’. Active defenses attempt to disable the source of an attack and passive defenses, by contrast, such as firewalls, purpose to repel cyber-attacks.[104]

It is possible international norms will soon coalesce such that states have an obligation not only to refrain from committing cyber-attacks themselves, but also “not to allow knowingly its territory to be used for acts contrary to the rights of other States.”[105]

Hence, this history of state practice indicates that countermeasures are warranted against most cyber-attacks so long they comply with the relevant procedural requirements and the principles of necessity and proportionality.

4.1.2 Tallin manual on cyber warfare

Published in 2013, the Tallin Manual was a rulebook set to govern cyber warfare in international Law.The Tallinn Manual is not a binding legal document, nor does it propose future law, best practice or preferred policy.The views expressed in the Tallinn Manual are those of the expertsacting in their private capacity. The Tallin manual has thus far offered a considerable guide to Cyber warfare regulation despite of its incapacity.

4.2 International legal regimes and institutions that directly or indirectly regulate cyber warfare

4.2.1 United Nations

There has been reportedly only limited U.N. action on the issue of cyber-security. The U.N. General Assembly has passed several related resolutions.[106]These resolutions, have

[103] Article 50, Draft Articles
[104] DOD Strategy, supra note 14, at 7
[105] Corfu Channel case (U.K. v. Albania),I.C.J. Reports. 4, (1949) page 22.
[106] 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.

been claimed to be vague and have not mandated any specific action by U.N. members.[107]

Reportedly, the United Nations in July 2010, when government cyber-security specialists from fifteen countries collaborated met, submitted a set of recommendations to the U.N. Secretary-General as "an initial step towards building the international framework for security and stability that these new technologies require.[108]

4.2.1 NATO

NATO created two new NATO divisions focused on cyber-attacks namely the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.[109]This summit prompted the Article 4 of the NATO treaty, which calls upon members to "consult together" in cases of cyber-attacks, but does not bind them to "assist" each other, as would be required under Article 5.[110]

4.2.3 COUNCIL OF EUROPE

Council of Europe Convention on Cybercrime ("Cybercrime Convention") through legislation and international cooperation promulgated "a common criminal policy aimed at the protection of society against cybercrime," as the first international treaty on crimes committed using the Internet and other computer networks.[111]. The convention allows invited states to join the convention and thus the US ratified the Convention in 2006.[112]

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).

[107] Resolutions on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Informational Infrastructures, G.A. Res. 58/199, U.N. Doc. No. A/RES/58/199 (Jan. 30, 2004).

[108] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4, U.N. Doc.A/65/201 (July 30, 2010).

[109] Scott J. Shackelford, *Estonia Two-and-a- Half Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L. 5

[110] NATO Agrees on Common Approach to Cyber Defence, *supra* note 106.

[111] Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001)

[112] Declan McCullagh & Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET NEWS, (Apr. 4, 2006, 10:25),

4.2.4 THE OAS

The OAS approved a resolution in April 2004 stating that member states should "evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001)" and should "consider the possibility of acceding to that convention."[113] They further ratified the treaty in 2006.

The OAS deployed an experts Group that would "provide technical assistance to member states in drafting and enacting laws that punish cyber-crime, protect information systems, and prevent the use of computers to facilitate illegal activity."[114]Although the OAS has made much progress in regional campaigns for cyber security it has done little for the world as a whole.

4.2.5 The Shanghai Cooperation Organization

In its Yekaterinburg Declaration, "the SCO member states stress the significance of the issue of ensuring international information security as one of the key elements of the common system of international security." [115] The Organization demonstrated cooperation and commitment to the goal of preventing cyber wars is realized in the 2009 Declaration.

[113] Organization of American States IV(8), AG/RES. 2040 (XXXIV-O/04) (June 8, 2004),
[114]see fig..1 table
[115] Shanghai Cooperation Organization, Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City (July 9, 2009), *available at* http://www.uzbekconsulny.org/news/572/.

5. CHAPTER 5: FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings

There is no legal vacuum in the regulation of Cyber space law. Article 36 of Protocol I additional to the Geneva Conventions provides 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 this Protocol or by any other rule of international law applicable to the High Contracting Party. However,Cyber operations that have been carried out thus far, for example in Estonia, Georgia and Iran, do not appear to have had serious consequences for the civilian population. International humanitarian law, or IHL, only comes into play if cyber operations are committed in the context of an armed conflict – whether between States, between States and organized armed groups or between organized armed groups. Therefore, we need to distinguish the general issue of cyber security from the specific issue of cyber operations in armed conflict. Terms like "cyber attacks" or even "cyber terrorism" may evoke methods of warfare, but the operations they refer to are not necessarily conducted in armed conflict.

IHL does not specifically mention or define cyber operations. It has occasionally been argued that IHL is ill adapted to the cyber realm and cannot be applied to cyber warfare. However, the absence in IHL of specific references to cyber operations does not mean that such operations are not subject to the rules of IHL. If the means and methods of cyber warfare produce the same effects in the real world as conventional weapons (such as destruction, disruption, damage, injury or death), they are governed by the same rules as conventional weapons.

The study proves to uphold the hypothesis that cyber warfare is inevitable war and that it falls beyond the scope of International Humanitarian Law.

5.2 Conclusion

The issue arises where a cyber attack does not rise to the level of an armed attack but nonetheless violate the customary international law norm of nonintervention. There is

Comment [AM12]: You miss to deal with the challenges of cyber-warfare… How it makes it hard for IHL to regulate it and if so, the nature of attacks that cyber-warfare bring forth…

only one cyberspace, shared by military and civilian users, and everything is interconnected. The key challenges are to ensure that attacks are directed against military objectives only and that constant care is taken to spare the civilian population and civilian infrastructure. The manual appropriately recalls in this regard that collateral damage consists of both direct and indirect effects, and that any anticipated indirect effect must be factored into the proportionality assessment during the planning and execution of an attack, a point highly relevant in cyberspace. Technology is a 'living' entity and is subject to change as years go by. The real difficulty with respect to the law and cyber warfare is not any lack of law but rather in the complexities that arise in determining the necessary facts, which must be applied to the law to render judgments.[116] These challenges underline the importance of States being extremely cautious when resorting to cyber attacks.

5.3 Recommendations

5.3.1. Regulated countermeasures

Countermeasures allow an injured state to respond to an attack with a reciprocal measure, with the goal of bringing an end to the war. Countermeasures provide states with a tool for addressing cyber- attacks that do not rise to the level of an armed attack but nonetheless violate the customary international law norm of nonintervention.

For countermeasures too be effective they require the identity of the attacker and the computer or network from which the attack originates to be accurately identified. Second, the attacking agent must find the countermeasure costly—ideally costly enough to encourage lawful behavior. If the attacker can readily relocate its operations, as is often possible in the context of cyber-attacks, the countermeasure may not impose a significant cost on the actor responsible for the attack. For this reason, countermeasures are likely to be more effective against state actors and less effective against non- state actors. [117]

[116] Charles Dunlap Junior, *Perspectives for Cyber Strategies on Law of Cyberwar*, Strategic Quarterly Spring (2011) pg 81
[117] Oana Hathaway, *Law of cyber attack*, Yale Law School Legal scholarship, (2012) pg 47-76

It is difficult to distinguish attackers from innocent individuals when conducting a countermeasure since it is difficult to contain the spillover effects. For this reason, the customary law of countermeasures offers only a partial answer to the problem of cyber-attacks.[118]

5.3.2 Creation and Adoption of a Universal Treaty regulating all forms of Cyber warfare

In the spirit of collective security and based on the principles of the Vienna Convention on the Law of treaties, States should convene to draft a treaty which shall be binding upon ratification based on whether the State is monist or dualist. The treaty would possibly offer a consensus definition of Cyber warfare and set a foundational approach to dealing with the ambiguities of this new method of warfare such as what amounts to 'attack' in cyberspace.The treaty should be informed not only by the principles of International humanitarian Law but should draw influence from other laws such as international human rights law, information technology law, international economic law, to name but a few.

[118] Oana Hathaway, *Law of cyber attack*, Yale Law School Legal scholarship, (2012) pg 47-76

Bibliography

ICRC, 'New Technologies and Warfare' International Review of the Red Cross, 2012.

US Department of Defense, U'S Cyber Command Fact Sheet', US Department of Defense Office of Public Affairs, 25 May, 2010

Herbert Lin, 'Cyber conflict and international humanitarian law' International Review of the Red Cross, 2012, 94(886),

Tallin Manual 2017

International Committee of the Red Cross, *No Legal Vacuum in Cyber Space*, Aug. 16, 2011

Susan Bremner, Cyberthreats: The Emerging Fault Lines of the Nation State, Oxford University Press, Oxford, 2009

Office of the Secretary of Defense, 110th Congress, Annual Report to Congress: Military Power of the People's Republic of China, 2007

William Jackson, 'Cyber attacks in the present tense, Estonian says', in Government Computing News, 28 November 2007

ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 29

Advisory service on International Humanitarian Law, ICRC July 2004

David Ignatius, Pentagon's cybersecurity plans have a Cold War chill, Wahington Post(August 26,2010)

Roscoe Pound, *The spirit of the Common Law*, Boston: Beacon press *(1921)*

Roscoe Pound , The Scope and purpose of sociological Jurisprudence, 25 Havard Law Review (1912)

Roscoe Pound, *A Survey of Social Interests* 57 Havard Law Review 99 (1943)

Chris Borgen, *Harold Koh on International Law in Cyberspace*, OpinioJuris, September 19, 2012

International Committee of the Red Cross, *Cyber Warfare*, Oct. 10, 2010

David Éric, *Principes de droit des conflitsarmés*, Brussels, Bruylant,Edition 3, (2002)

Maurice Frederic, 'Humanitarian ambition' IRRC, Vol.289, (1992)

Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 Intl Law Studies 99.

MN Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Colum J Transnatl L 885

P Singer and N Schachtman, 'The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive' Brookings Institution (15 August 2011)

William Jackson, 'Cyber attacks in the present tense, Estonian says', in Government Computing News, 28 November 2007

International Humanitarian law, 'Answers to your questions' (2014)
ICJ, *Continental Shelf case (Libyan Arab Jamahiriya v. Malta)*, Judgment, 3 June 1985, *ICJ Reports* 1985,

ICJ Statute

Additional Protocol 1

Geneva Convention I-IV

Additional protocol 1

UN charter

Maurice Frederic, 'Humanitarian ambition' IRRC, Vol.289,(1992)

MuhammedSaleem ,'Cyber warfare the truth in a real case',https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf

"Facts about Estonia", CERT Estonia, May 10, 2008 http://www.ria.ee/27525

"The cyber Raiders hitting Estonia", Thursday 17, 2007 http://news.bbc.co.uk/2/hi/europe/6665195.stm

Cyber Attack, Hit Estonia", May 18, 2007 http://www.telegraph.co.uk/news/worldnews/1551851/Cyber-attacks-hit Estonia.html

Duncan Holis, *Could Deploying Stuxnet be a War Crime?* OpinioJuris (Jan 25, 2011),

Factbox: What is Stuxnet? Reuters (Sept. 24, 2010), http://www.reuters.com/article/2010/09/24/us-security-cyber-iran-fb idUSTRE68N3PT20100924.

Kerr, et al., *supra* note 6, at 3 (translated from *Iran Confirms Cyber Attack, Says Engineers 'Rooting Out' Problem*, Mehr News Agency, (September 25, 2010)).

William J. Broad, John Markoff& David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, The New York Times (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Kim Zetter, *Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage*, Threat Level (Nov. 15, 2010)

Tallin manual Final report (2013).

Draft Articles,*supra* note 99, ch. II

Corfu Channel case (U.K. v. Albania),I.C.J. Reports. 4, (1949)

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 4, U.N. Doc.A/65/201 (July 30, 2010).

Scott J. Shackelford, *Estonia Two-and-a- Half Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L. 5

NATO Agrees on Common Approach to Cyber Defence, *supra* note 106.

Council of Europe, ETS No. 185, Convention on Cybercrime, pmbl., Budapest (Nov. 23, 2001)
Declan McCullagh& Anne Broache, *Senate Ratifies Controversial Cybercrime Treaty*, CNET NEWS, (Apr. 4, 2006, 10:25),
Organization of American States IV(8), AG/RES. 2040 (XXXIV-O/04) (June 8, 2004),

Shanghai Cooperation Organization, Yekaterinburg Declaration of the Heads of the Member States of the Shanghai Cooperation Organization, Consulate General of Uzbekistan in New York City (July 9, 2009), *available at* http://www.uzbekconsulny.org/news/572/.

Charles Dunlap Junior, *Perspectives for Cyber Strategies on Law of Cyberwar*, Strategic Quarterly Spring (2011) pg 81

Oana Hathaway, *Law of cyber attack*, Yale Law School Legal scholarship, (2012)