MIDLANDS STATE UNIVERSITY

FACULTY OF LAW

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF A BACHELOR OF LAWS HONOURS DEGREE

RESEARCH TOPIC:

A CRITICAL ANALYSIS OF THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW IN THE CONTEXT OF CYBER WARFARE.

SUBMITTED BY

LUCKY JONASI: R10873G

SUPERVISOR: DR. J. TSABORA

2014

MIDLANDS STATE UNIVERSITY APPROVAL FORM

The undersigned certify that they have read and recommended to MSU for acceptance, a dissertation entitled: A critical analysis of the applicability of international humanitarian law in the context of cyber warfare, submitted in partial fulfillment of the requirements for the award of Bachelor of Laws (Honours) Degree (LLB).

SUPERVISOR _____

PROGRAMME CO-RDINATOR _____

EXTERNAL EXAMINER _____

DATE _____

DECLARATION

I, LUCKY JONASI do hereby declare that this dissertation is the result of my own original work, except the extend indicated in the acknowledgements, References and by comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other University.

Student signature----------Date----------

DEDICATIONS

I owe my verbal salute to Mrs P. Lunga for helping me financially, morally and for believing in me. I dedicate this work to you mom.

ACKNOWLEDGEMENTS

The contributions made by various people made my academic journey a success and I wish them success in all their endeavours, may God richly bless them. Of special note is Thembani Lunga, Joseph Nkomo, Julius Chinoda, Try Takaidza, who cannot go unmentioned for the knowledge, encouragement, advice, guidance, help, love and discipline which they imparted in me.

Dr J. Tsabora, my supervisor I am deeply indebted to you for offering the best of your resources in assisting me to achieve the best knowledge I could get during the undertaking of this work. Your instructions from pro to epilogue made this work to be what it is.

I would also like to thank the Lecturers from the Faculty of Law for all their guidance. Their advice went a long way in helping me by encouraging me to do my work with all maximum effort. As Henry Brooke Adams (1906) pointed out that a teacher affects eternity, he or she can never tell where his or her influence stops.

Lastly but not the least, I would like to thank the class of 2010-2014. I am short of words to express my sincere appreciation for you guys.

ACRONYMS/ ABBREVAITIONS

AP	Additional Protocol
IAC	International armed conflict
ICJ	International Court of Justice
ICTR	International Criminal Tribunal of Rwanda
ICTY	International Criminal Tribunal of the Former Yugoslavia
IHL	International Humanitarian Law
NIAC	Non-international armed conflict
UN	United Nations

Contents

CHAPTER ONE: INTRODUCTION

1.1 INTRODUCTION

The means and methods of war have evolved since the Geneva Conventions were drafted in 1949. A wide array of new technologies has entered the modern battlefields and cyber space has opened up a potentially new war-fighting domain, a man-made theatre of war additional to the natural theatres of land, air, sea and outer space and is interlinked with all of them.[1] Walker[2] posits that, *"Because the entire law of war regime has been built upon a Westphalian foundation; the transformative properties of cyber warfare are just breath taking. We are left pondering some fundamental questions….. The international legal regime is lagging behind the problems presented by the increasingly sophisticated technological possibilities in this area."* This observation is what has prompted this study so as to highlight and discuss the increasing phenomenon of cyber warfare, the legal problems it poses and the seemingly inapplicability of International Humanitarian Law-a body of law that was drafted with traditional kinetic warfare in mind.

1.2 BACKGROUND

The interaction between technological development and armed forces is a constant feature of the history of warfare.[3] The rapid technological change in the methods and weaponry of warfare has continued to stress international law.[4] Thus, in 2003 at the 28th International Conference of the Red Cross[5] state parties to the Geneva Convention called for "rigorous and multidisciplinary review" of new weapons and means and methods of warfare to make sure that the laws protection is not overtaken by

[1] 'International Humanitarian Law and the challenges of contemporary armed conflicts' Report Document prepared by the International Committee of the Red Cross, Geneva, October 2011.

[2] JK Walker 'The Demise of the Nation-State, The Dawn of New Paradigm Warfare, and a Future for the Proffession of Arms' (2005) 51 *Air Force Law Review* 323.

[3] H Nasu 'Nanotechnology and challenges to International Humanitarian law: A Preliminary Legal Assessment' (2012) Vol 94 *International Review of the Red Cross* Issue 886, 653-672.

[4] D Fielder 'The meaning of Moscow 'non-lethal weapons and international Law in the early 21st Century' *International Review of the Red Cross*, (2005) Vol. 87. No 859, 552.

[5] International Conference of the Red Cross, '28th International Conference of the Red Cross and Red Crescent' https://www.icrc.org/eng/resources/documents/misc/57jqdy.htm (Accessed 16 October 2014).

developments of technology. The use of cyber operations in armed conflicts is one of the said technological developments and it trespasses traditional legal confines.

Current trends show that cyber warfare has now become a reality. Most recently there were cyber-attacks against Estonia in 2007[6], Georgia in 2008[7] as well as the most recently so-called 'Stuxnet' attack against Iran.[8] Cyber-attacks targeting China and initiated abroad is said to have increased significantly[9] and Chinas military networks suffers 80 000 attacks per month.[10] In 2012, US financial institutions came under a sustained cyber-attack believed to be orchestrated by Iran, but using a diffuse array of servers.[11] The US recently said it is prepared to use military force when necessary to respond to hostile acts in cyberspace. These words means a lot to a student of history in that the same sentiments were echoed when it declared the global war on terror and the result was the use of drones. All these events show that there is a growing possibility of serious cyber-war that would cause much devastating damage.

What is worrying is that there is a dual use technology in cyberspace that is there is one cyberspace shared by the military and civilian users, and everything is interconnected. The US Presidents Commission on Critical Infrastructure Protection 1997[12] had this to say,

> *"The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risks."*

---

[6] A bonet of over a million computers brought down government business and media websites across the country. 'Estonia and Russia: A Cyber-Riot', The Economist, May 12, 2007 http://www.economist.com/node/9163598. (Accessed 20 August 2014).

[7] R Diebert et al 'Cyclones in Cyberspace: Information Shaping and Denial in the 2008-Russia Georgia War' (2012) 43 (3) *Security Dialogue*.3.

[8] 'A silent attack, but not a subtle one', New York Times, 26 September 2010. http://www.nytimes.com/2010/09/27/technology/27virus.html (Accessed: May 2014).

[9] These attacks are said to mostly come from US, Japan, and South Korea http://www.donews.com/net/201210/1678402.shtm (Accessed 1 September 2014).

[10] This is according to a spokesman from Chinas Ministry of Defence the Ministry of Defence website and the People's Liberation Army (PLA). http://www.mod.gov.cn/affairs/2012-03/29content4354898.htm (Accessed 19 August 2014.)

[11] www.voanews.com/content/russia-ukraine-crisis-could-trigger-cyberwar/1894855.html. (Accessed 07 May 2014).

[12] Available at www.cyber.stdhs.gov/docs/PCCIP%20Report20 1997 (Accessed 27 July 2014).

In addition, in the same Presidential Report, it was stated that,

> *"The capability to do harm-particularly through information networks-is real; it is growing at an alarming rate; and we have little defense against it."*[13]

Thus, because of the interconnected system, it is hard to draw a precise line between civilian and military networks in cyber-attacks. In this vein, the impact of cyber warfare could be enormous such that cyber-attacks against airport control and other transportation system, nuclear power plants would likely cause large scale devastating damages and humanitarian consequences.[14]

The core value that civilians should be protected and their livelihoods, environment and cultural property should not be targeted is a principle that is applicable to cyber war as it is applicable to conventional war.[15] Constant care should be taken to spare civilians; wars have rules and limits that apply to all means and methods of warfare.[16]

Cyber-attack of recent past have already shown that cyberspace is becoming a new fighting domain and cyber warfare should no longer be perceived as science fiction suitable only for the theatre room but as a reality that needs to be urgently dealt with.[17] A cyber dimension of conflict in the future is virtually inevitable and policy makers must understand the legal landscape before such a conflict occurs. Thus in this vein, there has to be rules prepared so as to develop a knowledge base so that policy makers will find helpful if and when such a conflict occurs. Decision making should be subjected to pre-given and existent legal norms and principles.[18] Consequently, the object of this research is to contribute to the existing literature in analyzing the application of humanitarian law in the context of cyber warfare.

---

[13] (n 12 above) 34.
[14] C Beerlie 'Technological Challenges for the Humanitarian Legal Framework' 11th Bruges Collequium October 2014 http://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf (Accessed 16 October 2014).
[15] Cyber war and International Humanitarian Law, http://www.transconflict.com/2003/03/cyber-war-and-international-humanitarian-law-213. (Accessed 6, May 2014).
[16] L Gisel 'What is cyber warfare and why is the ICRC concerned?' http://www.icrc.org/eng/resources/documents/interviews/2013/06-27-cyber-warfare-lhl.htm (Accessed 7 May 2019).
[17] C Beerlie (n 14 above) 10.
[18] Shklar, Legalism (1964) as quoted by O Kesseler & W Weiner 'Expertise, Uncertainty, and International Law: a study of the Tallinn Manual on cyber warfare' (2013) Vol 26 *Leiden Journal of International Law* 793-810.

1.3 PROBLEM STATEMENT

It has been submitted that International Humanitarian Law applies to new weaponry and to the employment in warfare of new technological developments as recognized in Article 36 of the Additional Protocol I.[19] In addition, the Tallinn Manual which is a project initiated by NATO has been made as an 'attempt at codification' and a 'handbook' that govern the conduct of states in cyber warfare.[20] The manual it has been argued will be used as 'the likely key reference' when states would decide to adopt rules for conflict in cyberspace.[21] That said questions regarding the applicability of the existing international legal regimes, the law of armed conflict, and the Geneva Conventions to the phenomenon of cyber warfare have been raised. The laws protection seems to be lamentably insufficient and lagging behind and has been overtaken by the development of new technology. Cyber war significantly challenges many aspects of IHL particularly the question of distinction, proportionality, military object, civilian object, state responsibility, use of force inter alia. As a consequence, scholars ask whether we can redevelop, reinterpret, reform, the corpus of IHL so that it includes all kinds of war imaginable. Or could a separate body of IHL be made to deal with cyber warfare because the current IHL is difficult to apply. Thus there is therefore a dire need to examine whether the current International Humanitarian Law regime is sufficient and adequately encompass cyber warfare contexts.

1. 4 OBJECTIVES

The general objectives of the research are;

1. To discuss the increasing use of cyber technology in modern day wars and illustrate how this affect international humanitarian law.
2. Investigate whether international humanitarian law in general practice applies to cyber warfare.

---

[19] This has been confirmed by the International Court of Justice when it considered the legality of Nuclear Weapons *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Rep., 1996, p. 226.

[20] Rules of Cyber war: Don't Target Nuclear Plants or Hospitals, says Nato Manual', Guardian, 18 March 2013 htpp://www.guardian.co.uk/world/2013/war/18rules-cyber warfare-nato-manual (Accessed 07 May 2014).

[21] M Mimoso 'Tallinn Manual Interprets International law in Cyberwar context' 25 March 2013 http://www.threatpost.com Tallinn-manual-interprets-international-law-cyberwar-context-032513 (Accessed 09 May 2014).

3. Expose the gap between the law and technological advancements in the means and methods of warfare.
4. Provide clarification on how established humanitarian rules apply and function in the context of cyber warfare.
5. To make recommendations on how the international laws can best respond to cyber warfare.

1.5 LITERATURE REVIEW

The use of cyber warfare has stimulated intense debates among scholars. Specialist, experts and politicians all concur that cyber warfare should be treated as a reality and there is a bulk of literature which tries to analyze how applicable international humanitarian law applies to cyber warfare.

Beerlie states that cyber space is becoming a new fighting domain and cyber warfare should be perceived as a reality.[22] She traces the recent cyber-attacks and argues that although there were no grave humanitarian consequences in these attacks there is need to prepare for the worst as cyber warfare can result in significant civilian casualties and damages.

Lin discusses the different types and key characteristics of offensive cyber operations and their goal.[23] He also extensively analyses some ambiguities that is the problems posed by cyber operations to International Humanitarian Law.

Lubell analyses whether or not cyber war can be categorized as armed conflict so as to note which law is applicable to cyber warfare. He also defines cyber space and cyber warfare and discusses the requirements that are needed for cyber-attack to be referred to as an armed conflict.[24]

[22] C Beerlie (n 14 above) 9.
[23] H Lin 'The Technology of offensive cyber operation' (n 14 above) 41.
[24] N Lubbell 'Cyber Warfare as Armed Conflict' (n 14 above) 47.

Giess 2011 argues that cyber warfare should be treated as a reality and cyber space is becoming a new war zone. He again discusses the legal constraints of waging war in the cyber space.[25]

1.6 METHODOLOGY

This work is mainly library based. The research is primarily based on literature review obtained mainly from desk research. The internet has also been consulted but much reliance will be put to on authoritative texts, international conventions, treaties, articles and journals as a result of time constraints.

1.7 CHAPTER SYNOPSIS

Chapter 1.

This is an introductory chapter. Its contains a brief background of the study, the statement of the problem, research objectives, literature review, methodology as well as a brief synopsis of the chapters.

Chapter 2.

This chapter will define the concept of cyber warfare, and discuss various example of cyber-attacks. It will also discuss various unique aspects of cyber warfare that separates it forms other forms of warfare.

Chapter 3.

This chapter will discuss the increasing use of cyber technology in modern day wars and illustrate how this affects international law.

Chapter 4.

This chapter will look at the problems and challenges posed by cyber warfare to the current international humanitarian law regime.

[25] Giess 'The Legal Regulation of Cyber Attacks in Times of Armed Conflict' (n 14 above) 54.

Chapter 5.

This chapter contains the final conclusion and recommendations on how the laws can be developed so that it could cater for cyber warfare.

CHAPTER TWO: THE CONCEPT OF CYBER WARFARE

2.1 INTRODUCTION

The terms “cyber-attack,” “cyber-warfare,” and “cyber-crime” has been widely used both in the media and in international law in a variety of contexts some of which are controversial. This part of the dissertation will go through some of the terminology and definitions that are widely used in discussing the concept of cyber warfare as well as discussing their strength and weaknesses. There will also be an analysis of cyber-attacks in the recent past. This is a critical starting point so as to set a podium for an examination of the existing bodies of law and any reform efforts.

2.2 CYBERSPACE

Wingfield[26] postulates that, “cyberspace is not a physical space it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web.”

In this light, one will see that cyberspace adverts to the total interconnectedness of human beings through computers and telecommunication without regard to physical geography.[27] If we put this in the context of military activities, cyberspace can be regarded as a fifth theater of operation albeit one with specific characteristics that interacts with the other four domains of military operation, land, sea, air and space.

[26] T Wingfield ‘The Law of Information Conflict’ (2000) *NATIONAL SECURITY LAW IN CYBERSPACE* 17.
[27] SA Haldreth ‘Congessional Research Service Report for Congress’ (2001) NO. RL 30735, CYBERWARFARE 11.

2.3 COMPUTER NETWORKS ATTACK (or CNA)

The term computer networks attack is commonly employed in the context of cyber warfare. Nevertheless, this term seems, in some cases where it is used, to be too strict regarding the network part.[28] The critical infrastructure might be disconnected from the internet or any other network as part of security measures like the Stuxnet malware which hit an Iranian nuclear facility which was spread via removable USB devices. Yet these systems can and have been targeted by a cyber-attack.[29]

2.4 CYBER-ATTACK

The term cyber war and cyber-attack are used interchangeably. Cyber war as a term has been used to refer to "action by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or destruction."[30] This definition it is submitted is too constricted in that it confines the definition to attacks perpetrated by state actors thereby excluding exclusively conceivable situations in which attacks are carried out by non-state actors.

In addition, the Tallinn Manual describes a cyber-attack as an operation that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[31] The expression 'damage to objects' has been held to be ambiguous as it is not clear whether or what type of impairment of the functioning of the object would fall within this definition. However, experts agree that besides physical damage, loss of functionality of an object may also constitute damage.[32] Thus in this light one can see that a cyber-attack is in other words a cyber-operation whose consequences are expected to reach a certain threshold.

---

[28] J Valo 'Cyber Attacks and the Use of Force in International Law' Unpublished LLM thesis, University of Helsinki, (2014) 5.

[29] N Falliere et al 'W32.Stuxnet Dossier', *Symantec Security Response Whitepaper*, Version 1.4, 11 February 2011, www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf at 29.

[30] RA Clarke & RK Knale 'Cyber War – The Next Treat to National Security and What to Do About It' (2010) *Harper Collins: New York* 6.

[31] MN Schmitt (eds) 'Tallinn Manual on the International Law Applicable to Cyber Warfare' (2013) *Cambridge University Press* 106.

[32] What Limits Does the Law of War Impose on Cyber Attacks? www.icrc.org/eg/resources/documents/faq/130628-cyber-warfare-and-a-eng.htm. (Accessed 18 August 2014).

2.5 CYBER OPERATION

A cyber-operation is defined in the Tallinn Manual as the, "employment of cyber capabilities with the primary purpose of achieving objective in or by the use of cyberspace."[33] This term has also been defined as, "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate or information resident in computers and computer networks themselves, of another state."[34]

However, these definitions it can be contended are too wide in that information may be seen as referring to for example denial of service attack, which generally should not be seen as uses of force nor armed attacks. In addition, limiting the acts to those done to computers of another state seems to be too strict as much of the infrastructure is privately owned and such civilian networks or computers can in certain circumstances be legitimate military targets.[35]

2.6 CYBER WARFARE

The term is used to refer to means and methods of warfare that consists of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL. Cyber-warfare accordingly refers to the small subset of cyber-attacks that do constitute armed attacks or that occur in the context of an ongoing armed conflict.[36] This definition is crucial because it limits the application of the "war" framework to those actions that actually constitute "war" as a matter of international law.

It is important to distinguish between the mutable levels of malicious cyber activity which comprise "cyber-attack," "cyber-crime," "cyber espionage" and "cyber-warfare." The intention of the perpetrator and the effect of the attack have been used as one of the useful way to classifying the malicious activity.[37] Cybercrime is defined as, "any crime that is facilitated or committed using a computer network or hardware device."[38] It involves the production of malware, the distribution of child pornography, hijacking for

[33] J Valo (n 28 above) 22.
[34] AJ Schaup 'Cyber Warfare Operations: Development and use under International Law' (2009) *Air Force Law Review* 64, 127.
[35] MN Schmitt (eds) (n 31 above) 128-129.
[36] OA Hathaway et al 'The Law of Cyber-Attack' (2012) Vol. 100 *CALIFORNIA LAW REVIEW* 817.
[37] J Solse 'The Battlefield of Cyberspace: The Cyber inevitable New Military Branch-The Cyber Force' (2008) 18 ALB.L.J.SCI & TECH.239, 301.
[38] S Gordon & R Ford, On the Definition and Classification of Cybercrime, 2 J.COMPUTER VIROLOGY 13, 13 (2006).

ransom, the sale of mercenary services and the like.[39] Unlike cyber-attack, cybercrimes need not undermine the target computer network, and most don't have a political or national security purpose.

Cyber espionage is characterized by a motivation to discover sensitive information rather than that of causing harm. It can be conducted by an individual or a collective with the goal of pecuniary gain or strategic military advantage. A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.[40]

Cyber-warfare is distinctive among the three cyber-categories considered here in that cyber-warfare *must* also constitute a cyber-attack and to some extent cyber-crime. But not all cyber-attacks are cyber-warfare. Only cyber-attacks with effects equivalent to those of a conventional "armed attack," or occurring within the context of armed conflict, rise to the level of cyber-warfare.

2.7 EXAMPLES OF CYBER-ATTACKS

The Estonian Attack in 2007

After the relocation of a Soviet World War II memorial in 2007[41] which sparked a lot of protest by ethnic Russians in the country there was wide spread cyber-attack on Estonian websites, including those of the government, the parliament, banks and newspapers.[42] The attacks were held to be coordinated, organized distributed denial-of-service (DDoS) attacks which comprised of numerous computers inundating the target with malevolent traffic in order to inhibit them from serving legitimate clients.

The attacks have been used as an example of cyber warfare in the media.[43] Nevertheless, calling these attacks as instances of war has been held to be an overstatement. Since the attacks caused internet traffic flooding in parts of Estonia and

[39] Convention on Cybercrime, Council of Europe, E.T.S No 185, publ., Nov 23, 2001 (entered into force July 1, 2004), available at http://conventions.coe.int/Treaty.EN/T/Treaties?Html/185.htm.
[40] OA Hathaway et al (note 36 above) 826.
[41] This was a bronze soldier statute, which was considered by many as a symbol of the occupation of Estonia from the centre of Tallinn to a nearby military cemetery.
[42] E Tikk et al 'International Cyber Incidents- Legal Considerations' (2010) NATO Cooperative Cyber Defence Centre of Excellence Tallin.
[43] I Trayon 'Russia Accussed of Unleashing Cyberwar o Disable Estonia' The Guardian, 17 May 2007, www.theguardian.com/world/2007/may/17/topstories3.russia (Accessed 16 August 2014).

did not target critical infrastructure thus it can best be described as a nuisance or cyber riot than an act of war.

The Georgian Attack 2008

In 2008, Russia invaded Georgia over disputes in the Georgian province of South Ossetia and Abkazia.[44] Prior to the invasion, Georgia was subject to a cyber-attack in the form of DDos attacks. The attack spread after the physical fighting began and the targets included government websites as well as media communications and transportation companies.[45]

Stuxnet

In June 2010 a highly sophisticated malicious software program (the Stuxnet) which targeted specific types of computers and was widespread in Iran was discovered by a Belarusian computer security company VirusBlok Ada. Security researchers are agreed that the targets of the malware were Iranian nuclear facilities, the uranium enrichment facility near the city of Natanz. The malware tampered with the enrichment process, caused delays and disruptions in the process but failed to cause any catastrophic damage.[46]

It is submitted that the malware was so urbane such that the manufacturing of it required substantial resources merely available to a government. Furthermore, the malware had certain built in limitations and safeguards that made it not to cause damage without which it could have caused catastrophic damage without them.[47] Thus this attack has been held as evidence that it is practically possible for a cyber-attack to cause physical damage.

---

[44] Lieutenant Colonel PW Franzese 'Soveregnity in cyberspace: Can it exists?' (2003) Vol 64 *THE AIR FORCE LAW REVIEW* 1.

[45] J Markoff 'Before the Gunfire, Cyber-attacks' NEW YORK TIMES.COM 12 August, 2013. http://www.nytimes.com/2008/08/13/technology/13cyber:html (Accessed 19 August, 2014).

[46] K Zetter 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', Wired, 7 November 2011, < www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-Stuxnet/all/>

[47] R Langer 'To Kill a Centrifuge- A Technical Analysis of What Stuxnet Creators Tried to Achieve' Nov 2013 www.langer.com/enwp-content/uploads/2013/11/To-kill-a-cetrifuge.pdf at 15 (Accessed 10 July 2014).

Red October

Red October (or Roca) was a unique piece of malware that had been active for a long period of time which was discovered in Russia by a computer security company. This malware attack had the objective of upsetting or destroying communications, data or ultimately even physical objects. Red October was an intelligence gathering tool which targeted government, embassies and research institutions.[48]

Since the Red October performed largely intelligence gathering functions, it then falls beyond the scope of this work. However, it can be used as an example of the variety of possible cyber-attacks and the difficulty of ascertaining the objectives of the attack after a breach has been discovered. Again, it can be noted that, the same susceptibility that it used to intrude the systems could have been used to launch a more active piece of malware with more destructive physical damages.

2.8 UNIQUE CHARACTERISTICS OF CYBER WARFARE

It should be noted that cyber warfare has numerous physiognomies that separates it from conventional warfare and thus it represents a qualitative change in the meaning and nature of warfare. In Nuclear Weapons Advisory Opinion it was noted that the unique aspects of nuclear weapons should be taken into account when applying the Charter law to the case at hand.[49] On the same note, the distinctive characteristics of cyber operations should be considered when jus *ad bellum* and *jus in bello* is being applied to them.

Firstly, cyberspace is entirely man-made, it is not subjected to geopolitical or natural boundaries, thus, information and electronic payloads are transmitted from different points of origin and to various destination.[50] While the cyberspace is readily reachable to governments, non-state organizations, private enterprises and individuals alike, IP spoofing[51] and the use of bonets[52] makes it easy to disguise the origin of an operation,

[48] "Red October" Diplomatic Cyber Attacks/Investigation, Kaspersky Lab SecurityList, 14 Jan 2013. www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_investigation

[49] Nuclear Weapons (n 19 above) at para. 36.

[50] T Wingfield (n 26 above).

[51] IP spoofins refers to the creation of Internet Protocol (IP) packets with a forged source address with the purpose of concealing the identity of the sender or impersonating another computer system.

this renders the reliable identification[53] and attribution of cyber activities particularly difficult.[54]

Secondly, indirectness distinguishes cyber operation because numerous categories of cyber operations entail auxiliary action by a second actor after the initial act such as an attack on the targeting system of a missile, or disabling air traffic control systems.[55] Direct cyber-attacks are conceivable, but usually cyber-attacks have an indirect impact, since everything on the internet is so closely interrelated. Thus, an attack on a military system might have consequences for civil networks. This further makes the issue of distinction between combatants and non-combatants difficult.

Thirdly, cyber-attacks are intangible that is the target of the attack or the weapon used might not exist in a physical level and the damage might also be intangible.[56] For example the Stuxnet attack modified the spinning frequencies of the centrifuges, which directly resulted in physical damage to them.[57] An attack can also be aimed at destructing or altering information, but it can also result in physical consequences, however, with less direct nexus.[58]

Fourthly, cyber technologies and expertise are relatively easy and cheap to acquire, which allows weaker states and even non state actors to use its cyber capabilities as the way of attacking and thus cause considerable damage to countries. Cyber operations may result in various inconvenience or physical destruction and this causes problems in applying the IHL norms to cyber-attacks.[59] Further, the results might in some cases also be more unpredictable than in the case of kinetic force. Some of the issues will be discussed in much detail later.

---

[52] A bonet is an interconnected series of compromised computers used for malicious purposes. A computer becomes a bot when it runs a file that has bot software embedded in it.

[53] MN Schmitt 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 *Villanova Law Review* 594.

[54] D Delibasis 'The Right to National Self-Defence in Information Warfare Operations, 2007, 303.

[55] HH Dinniss '*Cyber Warfare and the Laws of War'* (2012) 65-66.

[56] HH Dinniss (n 55 above) 67.

[57] E Chien 'Stuxnet: A Breakthrough', Symantec Blog, 12 November 2010, <www.symantec.com/connect/blogs/stuxnet-breakthrough>. (Accessed 16 August 2014)

[58] HH Dinniss (n 55 above) 67–68.

[59] MN Schmitt 'Computer Network Attack and the Use of Force in International Law, Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885–937 at 921–922.

2.9 CONCLUSION

It should be noted that key terms and concepts discussed above have no internationally agreed definitions and have to some extent different meanings in different languages. Again, international law has yet to fully comprehend the legal ramifications of cyber warfare because of the intricacy and relentlessly evolving nature of the technology at the core of cyber warfare. As shown in this chapter, cyber operations of the past had no serious consequences for the civilian population and have not so far played a major part in any larger conflict. However, it is technically practicable to interfere with airport control systems, other transport control system, dams or nuclear power plants through space. Thus, potentially disastrous scenarios which may cause damage to noncombatants cannot be dismissed.

There are innumerable practical problems associated with the both launching and defending against cyber-attacks. Though there are difficulties of testing such a new legal regime only through an analysis of the available legal framework may a compromise position be synthesized that responds to the unique challenges posed by cyber warfare? Thus the next chapter will explore how international law rules and principles apply to cyber warfare.

CHAPTER THREE: CYBER WARFARE AND INTERNATIONAL LAW

3.1 INTRODUCTION

This chapter will examine the correlation between cyber operations and current international law in terms of *jus ad bellum* the law governing the resort to force between states. The concepts of force and armed attack which are focal to the question of the legality of military actions will also be scrutinized. However, it should be borne in mind that there is no consensus on meaning for either of the terms, and both will be debated in the context of cyber operations. The aim is to determine if and when cyber operations may constitute a use of force and armed attack. Furthermore, a discourse will be made on the principle of non-intervention.

3.2 APPLICABILITY OF THE EXISTING RULES

There is a general consensus among scholars that the principles of international law apply to cyber-attacks.[60] In the Nuclear Weapons Advisory Opinion it was stated that the United Nations Charter provisions on the use of force apply to any use of force regardless of the weapon employed.[61] This it is submitted has proved to be an effective means of addressing the rapid evolution of military technology.[62] However, as noted above, cyber warfare has some unique characteristics that secernates them from other types of warfare which renders the current international law insufficient[63] as will be shown below.

[60] H Koh 'International Law in Cyberspace' (2012) *Harvard International Law Journal Online* 3; MN Schmitt (ed) (n 32 above) 75-76.
[61] Nuclear Weapons (n 19 above) para 39.
[62] Nuclear Weapons (N 19 above) para. 78
[63] DB Hollis 'Why States need an International Law for Information System Operations' (2007) *Lewis & Clark Law Review* 1039-1040.

3.3. PROHIBITION OF THE USE OF FORCE UNDER INTERNATIONAL LAW

The maintenance of international peace and security builds around Article 2(4) of the United Nations Charter which bans member states from using or threatening to use force against any other state. Article 2(4) of the United Nations Charter states that,

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

Moreover, the proscription on the use of force is considered to be part of customary international law,[64] and also part and parcel of jus cogens, a set of unconditional peremptory norms from which no exceptions are allowed.[65]

3.3.1 NOTION OF 'FORCE'

Article 2(4) of the UN Charter bans the threat or the use of 'force', but there is no unambiguous delineation of what force entails. The term 'force', it is widely acknowledged, refers chiefly to armed force and excludes economic force.[66] Certain cyber-attacks have been held to constitute force[67] but since cyber operations take various forms, not all cyber-attacks can be held to fall under the notion of force. This makes the classification of which kinds of cyber operations do constitute force problematic. Furthermore, cyber-operation can cause serious economic consequences that may pose challenges for the marginalization of economic force from the prohibition of Article 2(4).

3.3.2 CYBER OPERATION AS USES OF FORCE

Scholars have proposed three main approaches that is the effects-based, target-based, and instrument-based to be used for solve the problem of cyber operations and the threshold of force. However, it should be noted that each of these approaches have

[64] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment, I. 43 C. J. Reports 1986 at paras 188–190

[65] Report of the ILC, Eighteenth Session, at 247.

[66] A Randelzhofer 'Article 2(4)' in Bruno Simma (ed.) *The Charter of the United Nations – A Commentary* (2002) 117–118.

[67] M Roscini 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 108–109.

their problems [68] but the most prevalent of the approaches seems to be the effects-based one, also adopted by the Tallinn Manual.[69]

The instrument-based approach uses the weapon used as the determining factor hence a cyber-operation may qualify as force if the weapon used sufficiently resembles the conventionally used ones. The target-based approach treats any operation targeting critical infrastructure as an armed attack and also as force. This approach has been criticized because it enlarges the notion of force to be unnecessarily all-embracing.

The effects-based approach uses the overall effects of the operation as the determining factor.[70] The Manual refers to the 'scale and effects' assessment used by the International Court of Justice in Nicaragua and postulates that *'acts that injure or kill persons or damage or destroy objects are unambiguously uses of force'*.[71] The scale and effects of the attack are mentioned by the ICJ with regard to the threshold of an armed attack, but the Tallinn Manual have construed it to be applicable in assessing whether an operation constitutes force.[72]

In addition, non-destructive, psychological cyber operations which aim at undermining confidence in a government or economy do not qualify as force.[73] The Manual provides for eight factors which are considered to be persuasive when states gauge whether a cyber-operation constitutes a use of force[74] but it should not be used as a legal criteria.[75] These are severity, immediacy, directness, invasiveness measurability of effects, military character, state involvement and presumptive legality.[76] This criteria however has been held to be problematic in that it is ambiguous and malleable[77] because it allow for wide interpretation.[78]

---

[68] R Nguyen 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 California Law Review 1117–1124.
[69] OA Hathaway et al (n37 above) 847.
[70] DB Hollis (n 63 above) 1041.
[71] Nicaragua (n 64 above) para 195.
[72] MN Schmitt (ed.) (n 31 above) 45–46.
[73] MN Schmitt (ed.) (n 31 above) 46–48.
[74] MN. Schmitt (ed.) (n 31 above) 47–51.
[75] MN Schmitt (ed.) (n 31 above) 48.
[76] MN Schmitt (n 59 above) 914–915.
[77] MN Schmitt 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 Villanova Law Review 578.
[78] OA Hathaway et al (n 36 above) 847–848.

3.3.3 CYBER ASSISTANCE AS FORCE

There are copious means by which a state may help another state or a non-state actor in concocting a cyber-attack thus the question of assistance counting as force is relevant to cyber operations. Assistance can be in the form of knowledge about a zero-day vulnerability, and data about how to take advantage of these susceptibilities or provide a ready-made piece of software.

The Tallinn Manual states, that mere funding of for example a hacktivist group who conducts cyber operations does not constitute a use of force. However, providing an organized group with malware and the training necessary to use it to carry out attacks would, however, qualify as a use of force.[79] This raises the question of what kind of malware suffices.

3.3.4 ECONOMIC OR POLITICAL FORCE

Article 2(4) it is submitted does not cover economic or political force however, there is a possibility that cyber-attacks may cause potentially catastrophic economic consequences without any physical damage. Such as an extensive bout on the banking system or a stock exchange which can trigger cross-border damage. Thus, cyber operations affect and cause snags to the previously more clear dissimilarity between physical and economic force.

Economic force can cause substantial danger to the political independence of states and to the stability of international relations.[80] Cyber operations it is respectfully submitted heralds new occasions for the comprehension of such a threat because they are capable of wholesome economic magnitudes unachievable by other types of attacks.[81] Thus they might be a need to reevaluate the scope of the notion of force.

[79] MN Schmitt (ed.) (n 31 above) 46.
[80] Grigorij Ivanovič Tunkin, Recht und Gewalt im internationalen System (Duncker & Humblot: Berlin 1986) 62.
[81] M Benatar 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 *Goettingen Journal of International Law* 391.

3.4 CYBER OPERATION AS ARMED ATTACKS AND THE RIGHT TO SELF-DEFENCE

3.4.1 OUTLINE OF THE RIGHT TO SELF-DEFENSE

The right to self-defence is considered to be a part of customary international law,[82] and it is also included in the UN Charter, whose Article 51 states that

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."

As with the notion of force, there is no unequivocal and established definition and this makes it difficult to determine what kind of an armed attack that trigger the right to self defence. The International Court of Justice stated in Nicaragua that just as Articles 2(4) and 42 of the UN Charter, also Article 51 does not refer to specific weapons.[83] This again apply to cyber operations and a state has the right to use force in self-defence if it is a victim of a cyber-attack that rises to the level of an armed attack. Congruently, a state may use cyber operations when acting in self-defence in reaction to an armed attack notwithstanding the weapons used in the attack against it.

The purpose of self-defence is to stop and repel an attack and not retaliate.[84] Thus providing a comprehensive definition for a proportionate attack in cyber operations is difficult and the facts and context of a particular case influence the answer.[85] The right to distinct or collective self-defense is also enshrined under Article 51 and there is no need of any pre-existing arrangement.[86] Thus, ad hoc assistance of another state is conceivable, however, the victim state of the attack must still declare that it has been the target of an armed attack.[87] A third state in this vein, may not unpromptedly, solely based on its own assessment, act in self-defence of the victim state.

[82] Nicaragua (n 64 above) para. 176.
[83] Nuclear Weapons (n 19 above) para. 39.
[84] C Gray *International Law and the Use of Force* (2008) 150.
[85] C Gray (n 84 above) 151.
[86] SA Alexandrov 'Self-Defense Against the Use of Force in International Law' (Kluwer Law International: The Hague 1996) 101.
[87] Nicaragua (n 64 above) para. 195.

3.4.2 NOTION OF AN 'ARMED ATTACK'

As in the case of Article 2(4) and the term 'force', the UN Charter does not unequivocally define the term 'armed attack' either. Traditionally, an armed attack is when there is adequately grave attack with significant damage, including fatalities carried out by the armed forces of a state.[88] In Nicaragua case, the ICJ found that even though the assistance to the contras could be regarded as a threat or use of force or an intervention, it did not constitute an armed attack that would have justified collective self-defence,[89] The ICJ stated that it did not have enough information available about the circumstances and the possible motivations of the incursions into the territory of Honduras and Costa Rica.[90] This it is submitted suggest that the Court would find the circumstances and motivations relevant for the determination of whether the operation would be classified as a frontier incident or an armed attack.[91]

However, after the 9/11 attacks the much of the debate has concerned the issue of attacks which have consequences that are less grave, attack that carried out by non-state forces and the possibility of self-defence against terrorist attacks. The questions are also relevant to the discussion about cyber operations, since the consequences of such operations are varied and do not in most cases clearly cross the threshold of an armed attack. Cyber operations can also easily be carried out by non-state actors, either with or without the support of a state.

3.4.3 ACCUMULATION OF EVENTS

Small-scale attacks and incursions have been considered in light of a theory of accumulation of events. States have responded to a series of attacks that jointly have amounted to an armed attack, even though each individual attack considered separately has not crossed the threshold.[92]

[88] Nicaragua (n 64 above) paras 193-5.
[89] Nicaragua (n 64 above) para. 195.
[90] Nicaragua (n 64 above) para. 231.
[91] C Gray (n 84 above) 179.
[92] C Gray (n 84 above) 155.

In Nicaragua, the ICJ stated that the lack of information made it difficult to decide whether or not the separate smaller incidents 'singly or collectively' amounted to an armed attack.[93] This suggests that such a possibility existed[94] thus, a series of small scale attacks could be collectively seen as an armed attack if the attacks are sufficiently related and the consequences sufficiently grave. This reasoning applies to cyber-attacks as well and a series of related cyber-attacks by the same actor may be considered as a 'composite armed attack'.[95]

3.4.4 CYBER ASSISTANCE AS AN ARMED ATTACK

In Nicaragua it was stated that the supply of weapons, logistical or other support to the rebels did not amount to an armed attack. It however, state that this could be regarded as a threat or use of force as well as an intervention in the affairs of other states.[96] The Security Council has also discussed the supply of arms or other forms of support in several cases, but it did not hold them to amount to an armed attack.[97]

It is improbable that assistance in the context of cyber operations would constitute an armed attack. It might, of course, be possible for a state to supply a ready-made cyber-attack for a non-state actor to be launched, or such guidance that it would, constitute an armed attack provided, of course, that the resulting attack would be of sufficient gravity. However, such close connection with the attack would probably mean that the question would be approached from the side of state responsibility and whether or not the attack would be attributable to a state.

3.4.5 ACTS OF NON-STATE ACTORS AS ARMED ATTACK

Article 2 (4) refers explicitly to member states and bans them from using force, whereas Article 51 does provide for member states the right to self-defence against an armed attack without reference to the perpetrator. The prevailing view is that Article 51 covers the acts of states and acts committed by non-state actors that are attributable to the

[93] Nicaragua (n 64 above) at para. 231.
[94] Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I. C. J. Reports 2003, at para. 64.
[95] MN. Schmitt (ed.) (n 33 above) 56.
[96] Nicaragua (n 64 above) para. 195.
[97] C Gray (n 84 above) 132.

state.[98] In Wall Advisory Opinion, Israel claimed that it was acting in self-defence, but the Court found that Article 51 had no relevance in the case and noted that Israel had not claimed that the attacks against it were in fact imputable to a state.[99] This was also stated in Armed Activities on the Territory of the Congo[100]

The majority of the group behind the Tallinn Manual agreed that state practice established a right of self-defence also in response to attacks by non-state actors and groups but recognized the 'significant uncertainty' when it comes to the degree of organization such a group must have.[101]

3.4.6 LEVEL OF CONTROL FOR STATE RESPONSIBILITY

For a state to be responsible for the acts of non-state actors, it has to have a certain level of control over the acts. In Nicaragua, the ICJ formulated the 'effective control' test which states that for a state to be responsible it has to be proved that it had effective control of the acts.[102] In Tadić case, the ICTY applied an 'overall control' test, which is less strict than the one used by the ICJ.[103] Thus, one will see that it is possible for the acts of non-state actors to be attributed to a state.

Self-defence against non-state actors can also apply in situations where a state is unable to prevent its territory to be used in preparation or carrying out terrorist attacks.[104] The Tallinn Manual adopted a similar view regarding cyber operations and noted that if a state is unable or unwilling to take actions to repress the attack, self-defence is permissible. Interestingly, the Manual noted that the inability might stem from the lack of expertise or technology.[105] However, the question of attribution regarding cyber operations makes it impossible to determine whether a state is involved or not

[98] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I. C. J. Reports 2004, p. 136, Separate Opinion of Judge Kooijmans at para. 35.
[99] Wall (n 99 above) para. 139.
[100] Armed Activities, on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I. C. J. Reports 2005, at para. 146.
[101] MN Schmitt (ed.) (n 31 above) 59.
[102] Nicaragua (n 64 above) at para. 115.
[103] Prosecutor v. Tadić, Case no. IT-94-1-A, ICTY Appeals Chamber, Judgment (15 July 1999) at para 120.
[104] A Randelzhofer (n 66 above) 802.
[105] MN Schmitt (ed.) (n 31 above) 60–61.

because the original source of the operation can be hidden so that it is difficult if not impossible to timeously determine it.

3.4.7 CYBER OPERATION AS ARMED ATTACK

The Tallinn Manual adopts the position that uses of force that injure or kill persons or damage or destroy property do satisfy the scale and effects requirement derived from the Nicaragua judgment and thus qualify as armed attacks.[106] Conversely, cyber espionage and operations that merely cause brief or periodic interruption of non-essential services do not count. Attacks that are lethal or cause significant property damage may constitute an armed attack.[107]

The exact point of the threshold of an armed attack is unclear even with armed attacks.[108] In Nicaragua, the ICJ distinguished between mere frontier incidents and armed attacks,[109] and in Oil Platforms case it did not exclude the possibility of the mining of a single military ship to constitute an armed attack.[110] It would thus seem that the operation does not have to be widespread for it to cross the threshold of an armed attack. A cyber-attack can effectively be carried out in fractions of a second, thus scholar argue for the idea of automatic self-defence.[111] However, this concept has several problems, one of which is the identification of the attacker because, the true origin of the attack may be masked making it difficult to respond to such an attack.[112]

Further, with respects to self-defence to cyber-attack, the requirement of necessity is problematic because data moves fast in cyber space, and the attack may be carried out in a very short space of time. Thus a strict interpretation of the necessity requirement makes it very difficult to resort to self-defence in response to cyber-attacks, as the attack could already be over when it is discovered.

---

[106] MN Schmitt (ed.) (n 32 above) 55.
[107] HH Dinniss (n55 above) 81.
[108] MN Schmitt (ed.) (n 32 above) 56.
[109] Nicaragua (n 64 above) at para. 195.
[110] Oil Platforms, supra (n 94 above) at para. 72.
[111] Y Dinstein *Computer Network Attacks and Self-Defense* (2012) 106.
[112] Y Dinstein (n 111 above) 107.

3.5 ANTICIPATORY SELF-DEFENCE AND CYBER ATTACKS

Article 51 of the UN Charter enunciates a right to self-defence 'if an armed attack occurs'. There are various interpretations to this Article however, a strict textual reading of it makes it conceivable to claim that it does not allow for anticipatory self-defence. Yet, it seems counterintuitive to claim that the Charter requires states to sheepishly wait for an attack to befall before they can act. A 2004 report by a UN High-Level Panel on Threats, Challenges and Change stated that according to 'long established international law', a state can take military action as long as the threatened attack is 'imminent, no other means would deflect it and the action is proportionate'.[113] In addition, the Secretary-General's report in 2005 states that 'imminent threats are fully covered by Article 51'.[114]

The question that arise in the context of cyber warfare is what level of certainty and proof is required for anticipatory self defence to apply. Cyber-attacks are prepared secretly and there might not be any exterior indicators of a looming attack as in the case of a traditional kinetic attack, such as gathering of troops near a border.[115] Thus, a strict interpretation of the temporal limits of self-defence would practically render it impossible to respond to cyber-attacks in self- defence.

Further, a state need not wait in cases where a cyber-attack rising to the level of an armed attack is 'imminent'.[116] The Manual states that the insertion of a logic bomb qualifies as an armed attack if the conditions for activation 'are likely to occur'. A mere placement of the malware or backdoor to the targeted computer or a network does not, however, meet the criterion of imminence[117] and thus does not justify self-defence.[118] Self-defence is justified when the attacker has decided to launch the attack and the target state faces a situation where postponing the defensive act would deprive it from effectively defending itself.[119] Self-defence after the attack has ceased is legitimate only

[113] Report of the High-Level Panel on Threats, Challenges and Change. UN Doc. A/59/565 at para. 188.
[114] In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the Secretary- General. UN Doc. A/59/2005 at para. 124.
[115] HH Dinniss (n 54 above) 90.
[116] MN Schmitt (ed.) (n 31 above) 63.
[117] That is, a piece of software allowing unauthorized access to a system.
[118] HH Dinniss (n 54 above) 90.
[119] MN Schmitt (ed.) (n 31 above) 65.

if it is reasonable to conclude that further attacks are likely to follow.[120] Without such a conclusion, the self-defence may be seen as retaliatory.[121]

3.6. RIGHT TO COUNTERMEASURES

States that have been subjected to an intervention[122] by another state under the threshold of an armed attack may respond by countermeasures and acts of retorsion. According to the commentary of the International Law Commission on the Draft Articles on State Responsibility, countermeasures are *'measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible State'* which are carried out as a response to an internationally wrongful conduct.[123] Countermeasures must be non-forceful.[124]

Additionally, attribution is also relevant to countermeasures as it is to self-defence and it involves the same kind of problems that is the origin of the attack may be difficult to unmask.[125] Further, the law of state responsibility applies to cyber operations of states as well.[126] Thus, if the conditions are met, states may respond to cyber-attacks conducted on them as well as use cyber operations as countermeasures themselves.[127] Yet it should be noted that in the context of cyber operations, the attack may be over in a matter of seconds, after which the countermeasures could easily be seen as retaliatory and contrary to Article 49 of the Draft Articles. Tallinn Manual notes, however, states have sometimes appeared to carry out countermeasures punitively.[128]

[120] MN Schmitt (ed.) (n 31 above) 66.
[121] MN Schmitt (ed.) (n 31 above) 66.
[122] The principle of non-intervention envisages the right of every sovereign state to conduct its affairs without outside interference. TD. Gill 'Non-Intervention in the Cyber Context' in K Ziolkowski (ed.) Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy (NATO CCD COE Publications: Tallinn, 2013), 217–238 at 220.
[123] Report of the ILC, Fifty-third Session, supra note 99 at 324–325.
[124] N White & A Abass 'Countermeasures and Sanctions' in Malcolm D. Evans (ed.), *International Law* (2010) 532.
[125] R Geiß & H Lahmann 'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention' in K Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy (NATO CCD COE Publications: Tallinn, 2013), 621–657 at 634.
[126] MN Schmitt (n 53 above) 661.
[127] MN Schmitt (ed.) (n 31 above) 36–37.
[128] MN Schmitt (ed.) (n 31 above) 37.

3.6.1 PROPORTIONALITY AND NECESSITY OF COUNTER MEASURES

According to Article 51 of the Draft Articles, countermeasures must be commensurate with the injury suffered, taking into account the gravity of the wrongful act and the rights in question.[129] Countermeasures are also subject to a requirement of necessity as stated in Article 52(1) of the Draft Articles on State Responsibility. However, this, too, presents difficulties for countermeasures in the cyber context.[130] Even though the limitations are strict, the peril does not need to originate from a state actor and the origin need not necessarily even be identified. This is especially relevant to cyber operations, because of the possible difficulties in determining the origin of the attack.[131] Uncertainty of the origin does, of course, in practice set quite strict limits on the possible responses. The Tallinn Manual notes that it is 'highly uncertain' whether or not a state may use force in accordance with the plea of necessity.[132]

3.7 CONCLUSION

The advent of cyber-attacks transported changes which challenge the outline on the use of force, as well as other relevant facets of international law.[133] This is worsened because the notion of force and armed attack is not clear thus creating problems of when a state may respond to a cyber-operation in self-defence. The predominant view is that Article 2(4) does not concern economic force, but since cyber operations make it very much possible for attackers to inflict even severe economic consequences without any physical damage, this bring about a lot of complications.

Again, because of the unique characteristics cyber warfare poses a lot of challenges to international law thus there have been calls for a treaty that would regulate the issue of cyber-attacks conducted by states. However, the question of non-state actors is also relevant to cyber-attacks and need also to be addressed. Having examined the correlation between cyber operations and current international law in terms of *jus ad*

[129] MN Schmitt (n 53 above) 682–683.
[130] MN Schmitt (n 53 above) 677.
[131] MN Schmitt (n 53 above) 663.
[132] MN Schmitt (ed.), (n 31 above) 39.
[133] J Arquilla & D Ronfeldt 'Cyberwar is Coming!' in J Arquilla & D Ronfeldt (eds) *Athena's Camp – Preparing for Conflict in the Information Age* (1997) 24–25.

bellum in this chapter, the next chapter will look at how international humanitarian law will responds to cyber warfare.

CHAPTER FOUR: CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW

4.1 INTRODUCTION

This chapter will examine the correlation between cyber warfare and current *jus in bello* that is the law concerning the conduct of hostilities. The first section will examine the applicability of the existing rules of international humanitarian law to cyber operations and examining the areas where fundamental issues arise. The next section will focus on the classification of armed conflicts under international humanitarian law.

After discussing this question, this chapter will look at some of the most important rules of IHL governing the conduct of hostilities and the interpretation in the cyber realm of those rules, namely the principles of distinction, military necessity, proportionality, humanity, and precaution. The aim is to try and focus on current attempts to reconcile cyber-warfare within IHL, try to address the question of why a mere interpretation of current law is not enough and show the issues that arise in attempting to apply IHL principles to cyber-warfare.

4.2 APPLICABILITY OF THE EXISTING RULES OF INTERNATIONAL HUMANITARIAN LAW TO CYBER WARFARE

It is only in the context of armed conflicts that the rules of IHL apply, imposing specific restrictions on the parties to the conflict.[134] The principles of international humanitarian law apply to cyber warfare. Article 1(2) of the Additional Protocol I to the Geneva Conventions:[135] states that,

'in cases not covered by this Protocol or by other international agreements, 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'.

[134] GC III, Art. 126(5), GC IV, Art. 143(5), and Statutes of the International Red Cross and Red Crescent Movement, Art. 5(2)(g).

[135] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, in force 7 December 1979, 1125 UNTS 3.

Furthermore, 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."

This rule clearly shows that IHL rules apply to new technology. The International Group of Experts also agreed that the current framework of international law applied to cyber warfare[136] in times of peace and of conflict nonetheless they recognizes the need for additional amplification and reconsideration concerning some of the unique aspects of cyber operations.[137] With respect to all of the rules of IHL, it will be noted that the cyber realm postures a numeral of questions that are still open. Thus, whether the traditional rules of IHL will provide sufficient protection to civilians from the effects of cyber warfare remains to be seen.

4.3 CLASSIFICATION OF ARMED CONFLICT

Under current IHL, there are two categories of armed conflict: international armed conflicts (IAC) and non-international armed conflicts (NIAC). According to Article 2 of the Geneva Conventions of 1949, an international armed conflict is any '*declared war or any other armed conflict which may arise between two or more States even if the state of war is not recognized by one of them'.* In International Criminal Tribunal for the former Yugoslavia (ICTY), it was held that an international armed conflict arises 'whenever there is a resort to armed force between States'.[138] The application of IHL depends on the factual situation. The question that begs a riposte in cyber warfare is whether an international armed conflict can be triggered by a cyber-attack in the absence of any other (kinetic) use of

[136] MN Schmitt "The Law of Cyber Warfare: Quo Vadis?" (2014) 27 *Stanford Law and Policy Review* 2-3.

[137] The United States International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World, May2011 <www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> at 14; L Zhang, 'A Chinese Perspective on Cyber War', 94 International Review of the Red Cross (2012) 801– 807 at 804. (Accessed 10 June 2014).

[138] Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70

force. To answer this one has to ask whether a computer network attack is attributable to the state[139] and amounts to a resort to armed force.

In addition, The ICTY stated that: a non-international armed conflict exists *'whenever there is ...protracted armed violence between governmental authorities and organised armed groups or between such groups within a State'*.[140] The 'protracted' requirement has with time been subsumed under a requirement that the violence must reach a certain intensity. Thus, two gauges define the existence of a non-international armed conflict that is, the armed conflict must reach a minutest level of concentration and the parties involved in the conflict must show a minimum of organisation.[141] Under non-international armed conflicts in the cyber realm, this might also bring about the question of differentiating amongst criminal behaviour and armed conflict.

It is worth reiterating that the ICJ,[142] and the ICTY,[143] held that most of the IHL principles whether in IAC or NIAC are customary and must be perceived in equal degree. It is submitted that, 'the protection of civilians from hostilities, in particular from indiscriminate attacks' is blind to the categorisation of the conflict.[144] In this vein, one will see that, it is the resolution of IHL that matters much and this is likely to be applied in the context of cyber warfare since the essential principle of humanity during an armed conflict is to protect civilians within the bounds of lawful warfare.

[139] The International Law Commission's commentary states: 'it will be a matter of appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it' Commentary on Article 8 of the Draft Articles on State Responsibility, (n 36 above) para. 5.
[140] Tadic case (n 103 above) para. 70.
[141] All non-international armed conflicts are covered by common Article 3 to the Geneva Conventions; in addition, the provisions of Additional Protocol II also apply to NIAC 'which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol' (AP II, Art. 1(1)).
[142] Nuclear Weapons case (n 20 above) 434.
[143] Tadic case (n 103 above) 435.
[144] Tadic case (n 103 above) para 127.

4.4 GENERAL PRINCIPLES OF THE LAW OF ARMED CONFLICT

4.4.1 THE PRINCIPLE OF DISTINCTION

The principle of distinction[145] draws the line between belligerents, who may be targeted and non-belligerents, who may not be targeted. It also differentiates between legitimate military targets and civilian objects, which may not be attacked.[146] Military objectives denote those objects which by their nature, location, purpose or use make an effective contribution to military action and those who's total or partial destruction, capture or nuetralisation, in the circumstances ruling at the time, offers a definite military advantage.[147] The trouble is that Internet is a dual-use target because both civilian and military networks are interlinked to a great extent.

Cyber operations can disable an object's functioning without causing physical damage, some commentators have argued that the use of cyber operations expands the range of legitimate targets because it enables attacks with reversible effects against objects that it would otherwise be prohibited to attack.[148] It has also been argued that,

"The potentially non-lethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare."[149]

Consequently, there is a very strong possibility that the signals used for cyber-attacks will interfere with civilian networks.[150] This has been submitted to be one of the reasons why the principle of distinction is problematic under cyber warfare.[151]

---

[145] Article 48, Article 57 (2)(a)(ii) and the article 51 (4) of the 1977 Additional Protocol I. to the Geneva Conventions as well as in the Article 27 of the IV. Hague Convention.

[146] A Kasher 'The Principle of Distinction' (2007) 6 *Journal of Military Ethics* 152.

[147] Art 52(2) Additional Protocol I of 1977 to the 1949 Geneva Conventions; M Sassoli 'Targeting: The scope and utility of the concept of 'military objectives' for the protection of civilians in contemporary armed conflicts' (2005)184 in D Wippman & M Evangelista (eds) New wars, new laws? Applying the laws of war in the 21st century conflicts (2005)181.

[148] MR Shulman 'Discrimination in the law of information warfare' (1999) *Columbia Journal of Transnational Law* 963.

[149] JTG Kelsey 'Hacking into international humanitarian law: the principles of distinction and neutrality in the age of cyber warfare' (2007-2008) Vol 106 *Michigan Law Review* 1439.

[150] S Brenner & M Dion, 'Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense' International Conference on Information Warfare and Security, April 2010, 49.

[151] JTG Kelsey (n 149 above "Hacking) 1439.

Moreover, the International Group of Experts decided that "*as a matter of law, status as a civilian object and military objective cannot coexist; an object is either one or the other….all dual-use objects and facilities are military objectives, without qualification*."[152] This exposes civilians because dual-use targets are common in cyber warfare. Some scholars recommends that the peculiarity between civilians and combatants should be adapted[153] because targeting dual-use infrastructure, is common for cyber warfare. This might also lead to the question as to who can be considered combatant, because if the dual-use infrastructure is attacked, civilians might take part in defending it.[154] Thus they can be dragged into cyber war unintentionally as defenders of dual-use targets. Brenner believes that *"civilian involvement in information warfare raises new and difficult legal issues, both domestic and international. Resolving these issues will require lawmakers and policy analysis to formulate new legal doctrine."*[155]

Furthermore, because tracing the origins of a cyber-attack is difficult, using cyber weapons can be very attractive for governments.[156] States can also use civilians in cyber warfare so as to avoid liability.[157] For example, Georgia claimed that in 2008, during the conflict over South Ossetia, Russia paid criminals and it supported patriotic hackers in carrying out cyber-attacks against Georgia.[158]

Moreover, it is respectfully submitted that, persons who partook in designing or launching the cyber weapon or semi-independent groups involved in launching the cyber weapon could fall under the definition of lawful combatants laid down in the article 4 (A) (2) of the III. Geneva Convention.[159] For those to be the case, cyber-combatants should be able to satisfy the requirements under this convention. For instance it is unclear how they could fulfil the requirement described in article 4 (A) (2) - to wear "…a

[152] Tallinn Manual, rule 39 (1).
[153] VM Padmanabhan 'Cyber Warriors and the Jus in Bello (2013) 89 *International Law Studies* 307.
[154] VM Padmanabhan (n 153 above) 291.
[155] S Brenner & M Dion (n 150 above) 54.
[156] W McGavran 'Intended Consequences: Regulating Cyber-Attacks' (2009) 12 *Tulane Journal of Technology and Intellectual Property* 265.
[157] VM Padmanabhan (n 153 above) 291.
[158] VM Padmanabhan (n 153 above) 293.
[159] VM Padmanabhan (n 153 above) 293.

fixed distinctive sign recognizable at a distance."[160] It should be mentioned here that the International Group of Experts did not agree on whether this requirement was necessary to be fulfilled in cyber warfare.[161]

For the reasons above, it seems to be inevitable to accept that cyber warfare has a civilian dimension. In cyber space the significances can be intensified to an thrilling point where nothing civilian remains and the simple rule that the civilian population will enjoy universal defense against dangers arising from military operations becomes practically empty of content, subject only to the principles of proportionality and precaution. In sum, it becomes clear that, in cyber space, the principle of distinction appears to hold little promise for the protection of civilian cyber infrastructure and all the civilian infrastructure that relies on it.

4.4.2 THE PRINCIPLE OF NUETRALITY

The principle of neutrality[162] means that a state, which is not involved in a conflict holds a neutrality status, it is not taking part in hostilities. This status involves both rights and duties.[163] Article 2 of the 1907 Hague Convention V states that *"belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral power."*[164] However, Kelsey points out that "when Belligerent A launches a cyber-attack against Belligerent B, the attack may be routed through the Internet nodes of Neutrals C and D, even if the belligerents share a common border."[165] Therefore, it seems that a cyber-weapon could easily travel through the territory of a neutral state.

In addition, according to the Article 5 of the Geneva Convention V neutral states should not assist or allow its territory to be used by another state. However, this is problematic in the context of cyber warfare because it might be difficult for a neutral state to halt

[160] 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, art. 4(2)(b).
[161] Tallinn Manual, rule 26 (10)-(12).
[162] This principle is rooted in the 1907 Hague Convention XIII as well as in the articles 1, 2 and 5 of the 1907 Hague Convention V.
[163] J Pictet 'The principles of international humanitarian law (III)' (1966) 6 *International Review of the Red Cross* 6 567.
[164] International Conferences (The Hague), Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, 18 October 1907, art. 2.
[165] JTG Kelsey (n 149 above) 1441.

cyber-activities taking place under its jurisdiction.[166] Under IHL, if a neutral state is incapable to stay desecration of its noninvolvement, other parties to the conflict have the right to interfere.[167] The result of this would be the exercising of the right to self-defense by the neutral state and eventually, more and more states could participate in the conflict.[168]

The Tallinn Manual states that *"a state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states*."[169] However, the International Group of Experts did not agree on whether this obligation also applies to the neutral states, through which the cyber-operations are routed.[170]

From the foregoing one will see that it is evident that IHL and the Tallinn Manual has some serious limitations. The doctrines of neutrality show that the scope to which the archetypal context of IHL was calculated for a completely different kind of warfare. Any attempts to interpret cyber activities through IHL is thus incompatible.

4.4.4 THE PRINCIPLE OF MILITARY NECESSITY

Military necessity entails that, an attack on a particular target is lawful only if its destruction, damage, or neutralization furthers a legitimate military objective or confers a definite military advantage.[171] When this principle is applied to cyber warfare, attacks on most of the enemy's military computer systems are permitted. However, cyber-attacks against innocently civilian computer systems, such as a systematic campaign to damage the enemy's economy are not justified. Thus attacks would be permitted only if it would not be reasonably expected to cause damage to civilian population centers.

Additionally, the law of armed conflict confers a protected status on certain kinds of sites. These sites include medical units which should be identified by using distinctive

[166] A Schaap 'Cyber Warfare Operations: Development and Use under International Law' (2009) *The Air Force Law Review* 64, 153.
[167] SK Verma *An Introduction to Public International Law* (2004).
[168] JTG Kelsey (n 149 above) 1445.
[169] Tallinn Manual, rule 5.
[170] MN Schmitt (n 59 above) 8.
[171] Additional Protocol I (n above), art. 35, para. 1; WM Reisman & D Stevick 'The applicability of international law standards to United Nations Economic Sanctions Programmes' (1998) 9 *European Journal of International Law* 94-95.

emblems, religious establishments,[172] and specially marked cultural property.[173] Conventional attacks on these protected sites are prohibited. Cyber-attacks on the computer systems of protected sites should be treated similarly. Occasionally, the protected status of a site may conflict with the right to engage legitimate targets. Similarly, if a state deliberately makes it impossible to attack its military computer systems, for example with malicious code, without also attacking the computer systems associated with protected sites, the protected systems lose their protection. Just as it is possible to use protected sites as shields against bombs, it is also possible to use protected servers as shields against malicious code. States should be required to separate computer systems with a protected status from those without one.

4.4.5 THE PRINCIPLE OF HUMANITY

The other central principle governing the methods and means of warfare is humanity. Modern international law articulates the principle as follows: "It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[174] Whereas the principle of distinction protects noncombatants from needless suffering, the principle of humanity protects combatants from the same. Computers and the Internet can be used in ways that target military personnel but cause excessive injury in the process, particularly in a form of psychological warfare known as "personal information warfare."[175]

4.4.6 THE PRINCIPLE OF PROPORTIONALITY

The principle of proportionality provides that attacks which cause excessive 'incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof' unjustifiable by the 'concrete and direct military advantage anticipated' or accrued are prohibited.[176] Thus, the principle of proportionality 'is not a free-standing

[172] Hague Regulations, Art. 27.
[173] Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 215; Hague Regulations, Art. 27.
[174] Additional Protocol I, art. 35, para. 2
[175] Y Alexander 'Terrorism in the Twenty-First Century: Threats and Responses' (1999/2000) 12 DePaul Bus. L.J. 59, 83.
[176] Art 51(5) of Additional Protocol I; Art 8(2) (a) (iv) of Rome Statute; J Gardam 'Proportionality and force in international law' (1993) 87 *American Journal of International Law* 391.

legal rule' but is fundamental during the decision making on whether to target or not[177] and it is important in determining not only 'which things may be attacked' but 'how things may be attacked'.[178] Proportionality in this vein, is the tool by which military necessity and humanity are balanced. If the necessity of decisively and expeditiously disabling the target outweighs the foreseeable harm, that is death, injury, and property damage, that will be inflicted, then the operation is permitted. If not, it is prohibited.[179]

The applicability of the principle of proportionality to cyber warfare is most evident in the context of responding to malicious code and denial-of-service attacks. As stated in the above chapters, it can be difficult to trace the source of such an attack as they are carried out surreptitiously. Wedgwood notes:

If . . . [a country] were the victim of an attack on vital computer systems, the temptation to respond in kind would be considerable. Yet the ultimate source of a computer attack can be acutely difficult to determine—a problem magnified by the deliberate use of "looping" or "weaving"—using another's server to disguise the origination of the attack. An attack is likely to be sent through an unrelated server in order to mask its authorship, and a response in kind may end up damaging or disabling the "looped" server.[180]

Again, reverberating effects–that is, indirect second- or third-tier effects from an attack–must be taken into account, there remains some discussion as to how far this obligation goes.[181] Because of the interconnectedness of networks in the cyberspace, it may be difficult to predict the effects than with a classic kinetic weapon, but at the same time it is all the more critical to do everything feasible to assess those effects. In practical terms this leads mainly to the question of precautions to be taken in attacks.

[177] M Sassoli 'Legitimate targets of attacks under international humanitarian law' (2003) 2 Background paper prepared for the Informal High Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge (27-29 January 2003) 181.
[178] Y Dinstein 'Collateral damage and the principle of proportionality' in D Wippman & M Evangelista (eds) New wars, new laws? Applying the laws of war in the 21st century conflicts (2005) 211.
[179] Y Dinstein 'The Conduct of Hostilities under the Law of International Armed Conflict' (2004) 120–23.
[180] RG Wedgwood 'Proportionality, Cyberwar, and the Law of War' (2002) 76 Int'l L. Stud 219, 222.
[181] MN Schmitt 'Computer network attack: the normative software' (2001) Yearbook *of International Humanitarian Law*, 82.

4.5 CYBER WARFARE AND THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES

The principle of direct participation in hostilities (DPH) was introduced into modern IHL in 1977 where it was stated that: 'Civilians shall enjoy the protection of this Section of the Protocol, unless and for such time as they take a direct part in hostilities'.[182] An international Group of Experts published an important guidance document on how the notion of DPH is to be interpreted.[183] The Guidance has some portions that are applicable to situation where civilians participate directly in cyber-hostilities.

The notion of DPH also describes the conduct which, if carried out by civilians, entails the suspension of their protection against direct attack.[184] Thus, when civilian experts or individual hackers carry out cyber operations amounting to direct participation in hostilities, they should comply with IHL governing the conduct of hostilities and also become legitimate military targets. The notion of DPH includes not only the infliction of death, injury or destruction, but essentially any act likely to adversely affect the military operations or military capacity of a belligerent party threshold of harm.[185]

Furthermore, in order to establish part of the hostilities within the denotation of IHL, the cyber operation in question must cause the required threshold of harm directly that is direct causation, and it must also be designed to do so in support of a belligerent and to the detriment of another belligerent nexus. Where cyber operations attributable to a belligerent party are designed to harm the adversary, either by directly causing death, injury or destruction, or by directly adversely affecting military operations or military capacity, such operations must be regarded as "hostilities" and, therefore, subject to all restrictions imposed by IHL on the choice and use of means and methods of warfare. If conducted by civilians, such operations also entail loss of protection against direct attacks.

[182] Art 51(3), AP I.
[183] ICRC 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (2008) 90 Intl Rev Red Cross 991 ('Interpretive Guidance').
[184] Art. 51(3), AP I, and art. 13(3), AP II.
[185] N Melzer 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL' (2009) ICRC 47.

4.6 CONCLUSION

In conclusion, there is no question that IHL applies to cyber warfare. However, it is a generally acknowledged that new developments in war has posed challenges to the international community. Cyber-warfare is an example of a concept causing confusion concerning its reconcilability with international humanitarian law (IHL). Cyber-warfare is not simply an additional technological expansion in waging war it epitomizes a new class of warfare. The difference between cyber warfare and conventional warfare is so significant that although the issues that need to be resolved in cyber-warfare are often similar to those arising in conventional warfare, the solution has to follow a different path. The fundamental difference with conventional warfare means that the current framework of IHL is incapable of governing cyberspace. The regulation of cyber-warfare requires an international treaty with global applicability.

CHAPTER FIVE: CONCLUSIONS AND RECOMMENDATIONS

5.1 INTRODUCTION

The previous chapters discussed the concept of cyber warfare, giving examples and also showed how there is significant amount of grey areas regarding cyber warfare in international law and international humanitarian law. Cyber operations involve novel means and methods of combat, the effects of which are still untested or poorly understood and they pose unique challenges to the application of IHL, in particular with respect to the very premise that civilian and military objects can and must be distinguished in armed conflict. Again, there is no clear guidelines on how the principles of distinction, proportionality, and precaution will be applied.

The law lags behind in dealing with the advancement of technology or weaponry. The international community struggles to promulgate and implement rules of conduct with universal support and adherence in a timely manner regarding the advancement of weaponry. In this light, this chapter proceed to make recommendations which will try to respond with the problems raised in this paper.

5.2 RECOMMENDATIONS

In light of the inadequacies in international law and international humanitarian law in the context of cyber warfare underscored in the preceding chapters, the following recommendations are made *de lege lata* and *de lege ferenda;*

Firstly, there should be a new treaty or treaties or conventions with universal applicability on cyber warfare. A separate instrument would strengthen the rules by clarifying and codifying them. Again, the treaty could overcome a lot of problems by creating relatively ambiguous norms leaving a considerable room for interpretation, which would however, embrace the unique characteristics of cyber-warfare.

Secondly, there is need for clarification and communication on what amounts to an armed attack under Article 51 and what would allow a conventional or other kind of attack in response. The internet is a ‘dual-use’ area and we have to preserve it

predominantly for civil and private use; this means we must have clarification in order to restrict and have a set of responses built in when a state considers that it has been injured as a result of another country's failure of due diligence.

Thirdly, the duty to assist model should be incorporated into international regime regulating cyber-attacks and cyber warfare. There should be an international law that sanctions assistance, if it has been judiciously entreated by party under cyber-attack and the ability to help exist. Cyber-attacks can be severe, incapacitate a state and thus require urgent help from without the attacked state. Assistance happened when Georgia was under attack and Estonia sent cyber specialist aid to bring Georgia back online. Assistance will also help in solving the question of attribution because if professionals come to the aid of those under attack they can unmask its origin timeously.

Fourthly, there must be promotion of discussion among cyber security experts and academics on cyber space and cyber warfare issues, to raise awareness of the need to assess the humanitarian impact of developing technologies, and to ensure that they are not prematurely employed under conditions in which respect for the law cannot be guaranteed. The regional cooperatives that have been created, such as the NATO Cyber Defence Centre in Tallinn[186] should be enlarged in scope so as to enhance wide cooperation, information sharing among nations and partnership in cyber defense.

Fifthly, there should be an International Cyber Security Organization (ICSO), as an independent platform for international cooperation. Further, the organization will also be responsible for investigating cyber-attacks and help to respond to cyber-attacks among member states.

5.3 CONCLUSION

In conclusion, it is indisputable that IHL applies to cyber warfare. Nevertheless, whether it will provide sufficient protection to the civilian population, by defending civilians and

[186] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) was formally established on the 14th of May, 2008

civilian infrastructure from damage, will depend on how IHL is interpreted with respect to cyber warfare. Protection of civilian infrastructure from being attacked or from suffering damage that is catastrophic for the civilian population can only be guaranteed if IHL is interpreted purposively. Thus in this vein, it can be concluded that more strict rules to govern cyber warfare are essential.

BIBLIOGRAPHY

Books

1. Alexandrov SA (1996): *Self-Defense Against the Use of Force in International Law-Kluwer*-Law International.
2. Anthony CA & Robert J B (1993): *International Law and the Use of Force – Beyond the UN Charter Paradigm*- Routledge.
3. Asrat B (1991): *Prohibition of Force Under the UN Charter – A Study of Art. 2(4)* - Iustus Förlag: Uppsala.
4. Brownlie I (1963): *International Law and the Use of Force by States*-Clarendon Press.
5. Cassese, A (2005): *International Humanitarian Law* - Oxford University Press.
6. Clarke RA & Knake RK (2010): *Cyber War – The Next Threat to National Security and What to Do About It*-HarperCollins.
7. Dinniss H H (2012): *Cyber Warfare and the Laws of War*-Cambridge University Press.
8. Dinstein Y (2012): *War, Aggression and Self-Defence*-Cambridge University Press.
9. Franck TM (2002): *Recourse to Force – State Action Against Threats and Armed Attacks*-Cambridge University.
10. Gazzini T (2005): *The Changing Rules on the Use of Force in International Law*-Manchester University Press.
11. Gray C (2008): *International Law and the Use of Force*-Oxford University Press.

12. Greenberg LT et al (1998): *Information Warfare and International Law*-National Defense University.

13. Healey J & Grindal K (eds) (2013): *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*-Cyber Conflict Studies Association.

14. Kaska EKT & Vihul L (2010): *International Cyber Incidents – Legal Considerations*-Cooperative Cyber Defence Centre of Excellence.

15. Kelsen H (1954): *Collective Security Under International Law*-U.S. Naval War College.

16. Kennedyn D (2006): *Of War and Law*-Princeton University Press.

17. Malanczuk P & Akehurst's MA (1997): *Modern Introduction to International Law*-Routledge.

18. Oppenheim L (1906): *International Law – A Treatise. Volume II: War and Neutrality*-Longmans, Green and Co.

19. Palojärvi P (2009): *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict*-The Erik Castrén Institute of International Law.

20. Rid T (2013): *Cyber War Will Not Take Place*-Oxford University Press.

21. Schmitt MN (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*-Cambridge University Press.

22. Sharp WG Sr (1999): *Cyberspace and the Use of Force*-Aegis Research Corporation: Falls Church.

23. Singh JN (1984): *Use of Force under International Law*-Harnam Publications.

Book Chapters

1. Arquilla, J & Ronfeldt, D *'Cyberwar is Coming!'*, in J Arquilla & D Ronfeldt (eds) (1997) *In Athena's Camp – Preparing for Conflict in the Information Age (Rand Corporation*: Santa Monica.

2. Caton, JL, *'Exploring the Prudent Limits of Automated Cyber Attack'*, in K Podins, J. Stinissen, M. Maybaum (eds) (2013) *International Conference on Cyber Conflict Proceedings*: NATO CCD COE Publications: Tallinn.

3. Geiß, R & Lahmann, H, *'Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention'*, in K Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (2013): NATO CCD COE Publications.

4. Giles, K & Hagestad W II *'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English'*, in K. Podins et al (eds), (2013) *International Conference on Cyber Conflict Proceedings* (2013): NATO CCD COE Publications.

5. Gill, TD *'Non-Intervention in the Cyber Context'*, in K Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (2013): NATO CCD COE Publications.

6. Randelzhofer, A *'Article 2(4)*', in B Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2002): Oxford University Press.

7. Randelzhofer, A *'Article 51'*, in B Simma (ed.), *The Charter of the United Nations – A Commentary, Volume I* (2002): Oxford University Press.

8. Schmitt, MN *'Responding to Transnational Terrorism under the Jus ad Bellum'*, in M N Schmitt & J Pejic (eds), *International Law and Armed Conflict: Exploring the Faultlines – Essays in Honour of Yoram Dinstein* (2007): Martinus Nijhoff Publishers.

9. Schmitt, MN *'Cyber Activities and the Law of Countermeasures'*, in K Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace – International Law, International Relations and Diplomacy* (2013): NATO CCD COE Publications.

10. Schmitt, MN *'The "Use of Force" in Cyberspace: A Reply to Dr. Ziolkowski'*, in C Czossek, et al (eds) (2012) *International Conference on Cyber Conflict Proceedings* (2012): NATO CCD COE Publications.

11. White N & Abass A *'Countermeasures and Sanctions'*, in M D. Evans (ed.), *International Law* (2010): Oxford University Press.

12. Ziolkowski, K *'Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force'*, in C Czossek et al (2012) *International Conference on Cyber Conflict Proceedings* (2012) NATO CCD COE.

Articles

1. Barber, RJ 'The proportionality equation: balancing military objectives with civilian lives in the armed conflict in Afghanistan' (2010) 15 Journal of Conflict and Security Law 467.

2. Bartolini, G 'The civilianization of the contemporary armed conflicts' (2008) 2 Select Proceedings of the European Society of International law 569.

3. Benatar, M 'The Use of Cyber Force: Need for Legal Justification?*'* (2009) 1 *Goettingen Journal of International Law* 375.

4. Brown, D 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harvard International Law Journal* 179.

5. Dinstein, Y 'Computer Network Attacks and Self-Defense' (2002) 76 *U.S. Naval War College International Law Studies* 99.

6. Gill, TD 'The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy', 11 *Journal of Conflict & Security Law* (2006) 369.

7. Gervais, M 'Cyber Attacks and the Laws of War', (2012) 30 *Berkley Journal of International Law* (2012) 525.

8. Hathaway, O et al 'The Law of Cyber- Attack' (2012) 100 *California Law Review* 817.

9. Hollis, DB 'Why States Need an International Law for Information Operations', (2007) 11 *Lewis & Clark Law Review* 1023.

10. Jamnejad, M & Wood, M 'The Principle of Non-intervention' (2009) 22 *Leiden Journal of International Law* 345.

11. Jensen, ET 'Computer Network Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207.

12. Kanuck, SP 'Information Warfare: New Challenges for Public International Law' (1996) 37 Harvard International Law Journal 272.

13. Kelly, MJ 'Time Warp to 1945 – Resurrection of the Reprisal and Anticipatory Self- Defense Doctrines in International Law' (2003) 13 Journal of Transnational Law and Policy 1.

14. Koh HH, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal Online* 56.

15. Nguyen, R 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 *California Law Review* 1079.

16. Raboin, B 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare', (2013) 31 *Journal of National Association of Administrative Law Judiciary* 602.

17. Robertson, HB Jr., 'Self-Defense Against Computer Network Attack Under International Law' (2002) 76 *U.S. Naval War College International Law Studies* 121.

18. Roscini, M 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 85.

19. Schaap, AJ 'Cyber Warfare Operations: Development and Use Under International Law', (2009) 64 *Air Force Law Review* 123.

20. Schmitt, MN 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885.

21. Schmitt, MN 'Cyber Operations and the Jus Ad Bellum Revisited', (2011) 56 *Villanova Law Review* 569.

22. Schmitt, MN 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed' (2012) 54 *Harvard International Law Journal Online*.

23. Shackelford, S 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 Berkeley Journal of International Law 192.

24. Silver, DB 'Computer Network Attack as a Use of Force Under Article 2(4)' (2002) 76 U.S. Naval War College International Law Studies 73.

25. Zhang, L 'A Chinese Perspective on Cyber War' (2012) 94 International Review of the Red Cross 801.

News Articles and Reports

1. Brian Krebs, 'A Short History of Computer Viruses and Attacks', The Washington Post, 14 February 2003, <www.washingtonpost.com/wp-dyn/articles/A50636-2002Jun26.html>.

2. Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', The Guardian, 17 May 2007 <www.theguardian.com/world/2007/may/17/topstories3.russia>.

3. 'War in the Fifth Domain', The Economist, 1 July 2010, <economist.com/node/16478792>.

4. Josh Halliday, 'Stuxnet Worm is the “Work of a National Government Agency”', The Guardian, 24 September 2010, <www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency>.

5. Erik Chien, 'Stuxnet: A Breakthrough', Symantec Blog, 12 November 2010, <www.symantec.com/connect/blogs/stuxnet-breakthrough>.

6. Kim Zetter, 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', Wired, 7 November 2011, <www.wired.com/threatlevel/2011/07/how-digital- detectives-deciphered-stuxnet/all/>.

7. '”Red October” Diplomatic Cyber Attacks Investigation', Kaspersky Lab SecureList, 14 January 2013, <securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investi gation>.

8. Jarno Limnéll, 'Defining the Qualities of Cyber Warfare', SC Magazine, 11 March 2013, <www.scmagazine.com/defining-the-qualities-of-cyber-warfare/article/283902/>.

9. Ralph Langner, To Kill a Centrifuge – A Technical Analysis of What Stuxnet's Creators Tried to Achieve, November 2013, <www.langner.com/en/wp-content/uploads/2013/11/To- kill-a-centrifuge.pdf>.

Treaties

1. Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 29 July 1899, in force 4 September 1900.

2. Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907, in force 26 January 1910.

3. The General Treaty for the Renunciation of War, 27 August 1928. LNTS vol. XCIV, No. 2137, 33.

4. Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945. 1 UNTS XVI.

5. Vienna Convention on the Law of Treaties, 23 May 1969, in force 27 January 1980. 1155 UNTS 331.

6. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, in force 7 December 1979, 1125 UNTS 3.

7. Rome Statute of the International Criminal Court, 17 July 1998, in force 1 July 2002, 2187 UNTS 90.

8. Council of Europe Convention on Cybercrime, 23 November 2001, in force 1 July 2004, CETS No. 185.

United Nations Resolutions

General Assembly

1. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res. 2131 (XX), 21 December 1965.

2. Declaration on Principles of International Law concerning Friendly Relations and Co- operation among States in Accordance with the Charter of the United Nations, GA Res. 2625 (XXV), 24 October 1970.

3. Definition of Aggression, GA Res. 3314 (XXIX), 14 December 1974.

4. Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, UN Doc. A/RES/42/22, 18 November 1987.

5. Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83, 28 January 2002.

Case Law

International Court of Justice

1. Corfu Channel Case (UK v. Albania), Judgment, I. C. J. Reports 1949, p. 4.

2. North Sea Continental Shelf Cases (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands), Judgment, I. C. J. Reports 1969, p. 3.

3. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment, I. C. J. Reports 1986, p. 14.

4. Territorial Dispute (Libyan Arab Jamahiriya/Chad), Judgment, I. C. J. Reports 1994, p. 6.

5. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I. C. J. Reports 1996, p. 226.

6. Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Equatorial Guinea Intervening), Judgment, I. C. J. Reports 2002, p. 303.

7. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I. C. J. Reports 2004, p. 136.

8. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, I. C. J. Reports 2005, p. 168.

9. Armed Activities on the Territory of the Congo (New Application: 2002) (Democratic Republic of the Congo v. Rwanda), Jurisdiction and Admissibility, Judgment, I. C. J. Reports 2006, p. 6.

International Criminal Tribunal for the Former Yugoslavia

1. Prosecutor v. Furundzija, Case no. IT-95-17/1-T, ICTY Trial Chamber, Judgment (10 December 1998).
2. Prosecutor v. Tadić, Case no. IT-94-1-A, ICTY Appeals Chamber, Judgment (15 July 1999).