

Cyber Warfare: The Notion of Armed Conflict and Applicability of International Humanitarian Law

A thesis submitted in partial fulfillment
Of the requirements of the degree of
MASTER OF LAWS IN INTERNATIONAL LAW
(Faculty of Shari'ah and Law)
In The International Islamic University Islamabad

By

Mehreen Aman

Reg. No. 183-FSL/LLM(IL)/S14

Supervised by

Dr. Muhammad Mushtaq Ahmad

Associate Professor of Law

Faculty of Shari'ah and Law

International Islamic University Islamabad



Accession No TH:18225



MS
341.481
MEC



Humanitarian Law.

Cyber crimes - law and legislation

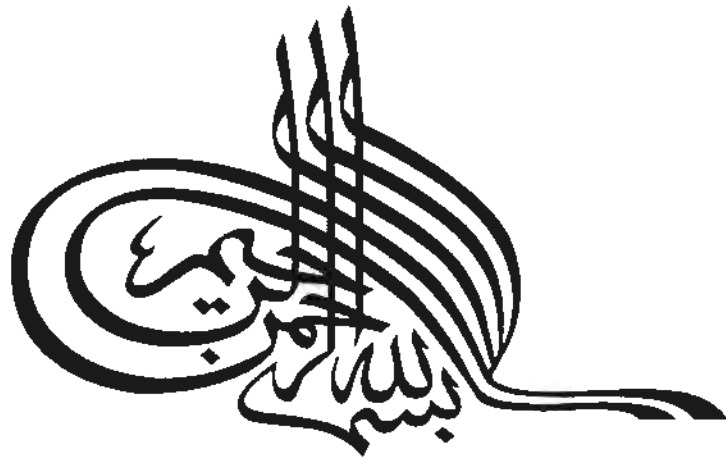
War (International Law)

War crimes (" ")

Mehreen Aman

© _____ 2017

All rights reserved.



*In the name of Allah,
the Most Beneficent,
the Most Merciful*

DEDICATED TO MY PARENTS

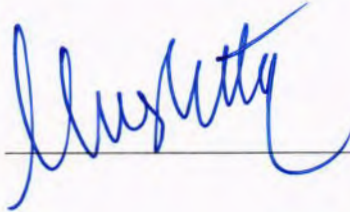
**International Islamic University Islamabad
Faculty of Shari'ah & Law**

Approval Sheet

This is to certify that we evaluated the thesis entitled "Cyber Warfare: The Notion of Armed Conflict and Applicability of International Humanitarian Law" submitted by Miss Mehreen Aman, Reg. no.183/FSL/LLM(IL)/S14 in partial fulfillment of the award of the degree of LLM International Law. The thesis fulfills the requirements in its core and quality for the award of the degree.

Dr. Muhammad Mushtaq Ahmad,
Associate Professor of Law, Faculty of
Shari'ah & Law, International Islamic University
Islamabad, Pakistan.

Supervisor



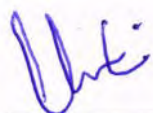
Dr. Farkhanda Zia,
Professor of Law, Faculty of Shari'ah &
Law, International Islamic University
Islamabad, Pakistan.

Internal Examiner



Mr. Usman Khan,
Legal Advisor, ICRC Pakistan.

External Examiner

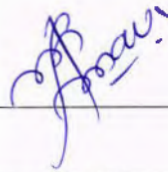


DECLARATION

I, **Mehreen Aman**, hereby declare that this dissertation is original and has never been presented in any other institution. I, moreover, declare that any secondary information used in this dissertation has been duly acknowledged.

Student **Mehreen Aman**

Signature



Date

Supervisor: Dr. Muhammad Mushtaq Ahmad, Associate Professor of Law

Signature

Date:

TABLE OF CONTENTS

ACKNOWLEDGMENTS	ii
ABSTRACT.....	iii
ACRONYMS.....	iv
LIST OF CASES.....	v
LIST OF FIGURES AND TABLES.....	vi
INTRODUCTION	1
Literature Review.....	3
Framing of Issues.....	8
CHAPTER 1	10
CYBER WARFARE: NATURE AND SCOPE	10
Introduction.....	10
1.1 Defining Cyber Warfare.....	11
1.1.1 Two Distinct Aspects of Cyber warfare	13
1.1.2 Cyber warfare Versus Traditional Warfare	15
1.2 Defining Cyberspace	17
1.2.1 Characteristics of Cyberspace	19
1.2.2 Forms of Operations in the Cyber Domain	22
1.3 Defining Cyber Attack	23
1.3.1 Types of Cyber Attacks	24
1.4 Cyber Crime	26
1.5 Relation among Cyber-Attack, Cyber-Crime and Cyber Warfare.....	27
1.5.1 Cyber-actions as Cyber-crime	29
1.5.2 Cyber-actions as Cyber-attack.....	30
1.5.3 Cyber-actions as Cyber warfare	31
1.6 Cyber Weapons	32
1.7 Challenges Raised by Cyber Warfare	33
1.8 Cyber Policing.....	34
Conclusions.....	36
CHAPTER 2	38
CYBER WARFARE AND THE NOTION OF ARMED CONFLICT.....	38
Introduction.....	38
2.1 The Basic Typology	39
2.1.2 The Notion of Armed Conflict.....	40
2.2 Categorization of Armed conflict under IHL.....	41
2.2.1 International Armed Conflict.....	43
2.2.2 Non international Armed Conflict.....	45
2.3 Qualification of Cyber warfare as International Armed Conflict	47
2.3.1 Threshold of Harm for Armed Conflict.....	48
2.3.2 The Requirement of Armed Force.....	50
2.3.3 Intervention of the Armed Forces.....	51
2.3.4 Requirement of Being International	56

2.4	Non-international Armed Cyber Conflict	58
2.4.1	Requirement of Organized Armed Group	58
2.4.2	Requirement of Responsible Command	60
2.4.3	Particular Level of Intensity	62
	Conclusions.....	63
	CHAPTER 3	65
	APPLICATION OF INTERNATIONAL HUMANITARIAN LAW ON CYBER WARFARE.....	65
	Introduction.....	65
3.1	Application of International Humanitarian Law on Cyber Warfare	66
3.1.1	Application during Conventional Armed Conflict	68
3.1.2	Cyber-Attack on its Own.....	69
3.1.3	Computer Network Attacks in Support of Conventional Attacks	70
3.2	Military Necessity	71
3.3	The Principle of Distinction	72
3.3.1	Targeting in Cyber Warfare.....	74
3.3.2	Computer Data as an Object.....	74
3.3.3	Dual Use Object.....	76
3.3.4	Targeting Civilians Objects	78
3.3.5	Attacks and Operations.....	79
3.3.6	Indiscriminate Attacks.....	81
3.4	Principle of Proportionality.....	83
3.4.1	Knock-on Effect	84
3.5	The Principle of Precaution.....	85
3.5.1	Verification of Objectives	87
3.5.2	Choice of Means and Methods	88
3.5.3	Choice of Targets and Interconnectedness	88
3.6	Perfidy and Ruses of War.....	89
	Conclusions.....	91
	CHAPTER 4	92
	COMBATANT STATUS, DIRECT PARTICIPATION IN HOSTILITIES AND CYBER WARFARE.....	92
	Introduction.....	92
4.1	Combatants.....	93
4.1.1	Requirements of Combatant Status and Cyber Warriors.....	95
4.1.2	Distinction	96
4.1.3	Compliance, Organization, Belonging and Allegiance	97
4.2	Direct Participation in Hostilities by Civilians	98
4.2.1	DPH in the Context of Cyber warfare	100
4.2.2	Specific Cyber Warfare Activities as DPH	101
	Conclusions.....	108
	CONCLUSIONS AND RECOMMENDATIONS	109
	ANNEXTURE	116
	BIBLIOGRAPHY.....	121

ACKNOWLEDGMENTS

Praise be to Allah, the sustainer of the worlds, the Merciful, the compassionate and may his ing blessings and peace be on Muhammad, the last of his Messengers!

Thanks to *Allah Almighty* for giving me strength and capability to understand, learn and complete this thesis.

I am deeply grateful and wish to express my sincere gratitude to my supervisor Dr. Muhammad Mushtaq Ahmad, Chairman of Department of Law for his invaluable guidance, suggestions and supervision of the work. it was a great honor to finish this research work under his supervision.

I also owe a debt of gratitude to Madam Sadia Tabbasum, Assistant Professor, Department of Law, who remains a source of inspiration for me. She has been very gracious to me and has always taken keen interest in my humble efforts in analyzing minor issues.

A special thanks to my parents and siblings, without their moral support, love and affection this research could not have been possible.

I am also genuinely appreciative of my friends particularly Miss Afshan Abbasi and my best friend who tirelessly listened to me and offered encouragement when it was most needed.

ABSTRACT

Technology has dominated warfare since the early 1900s. Throughout history, societies have put their best minds to work creating new ways to fight each other. One of such new means of warfare is cyber warfare fought in cyber space. It is a current scenario under International Humanitarian law (IHL). Cyberspace has opened up a potentially new war-fighting domain, additional to land, air, sea and outer space. States have already embraced using cyber-attacks as a method of conducting hostilities. Cyber warfare starts to represent the latest challenge at an international level as it seems that rapid technological advances may render IHL ill-adapted for modern technologies of war.

This thesis covers the observable fact of cyber warfare and its applicability on IHL. In the first place, the terms of cyber warfare and cyber-attack are clarified. Subsequently, an effort has been made to look into whether and, if so, under what kind of circumstances, cyber-attack can amount to an armed conflict, by employing the traditional distinction between an International Armed Conflict and a Non-International Armed Conflict. Eventually, issues posed by cyber warfare in application of core principles of IHL upon this new kind of warfare are discussed.

Based on research and inter alia the issues identified with IHL and cyber warfare, this thesis concludes that the current body of law is inadequate to deal with Cyber warfare explicitly; and that better technical consultation and interpretation of existing principles of IHL is required for an effective and proportionate regulation of cyber warfare.

ACRONYMS

API	Additional Protocol I 1977
AP II	Additional Protocol II 1977
CA3	Common Article 3 to Geneva Conventions 1949
CNA	Computer Network Attack
CPU	Central Processing Unit
CW	Cyber Warfare
DDoS	Distributed Denial of Service
DoD	Department of Defense
DoS	Denial of Service
DPH	Direct Participation in Hostilities
GPS	Global Positioning Satellite
IAC	International Armed Conflict
ICJ	International Court of Justice
ICRC	International Committee of Red Cross
ICT	Information and Communications Technology
ICTR	International Criminal Tribunal for Rwanda
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
NIAC	Non-International Armed Conflict
SCADA	Supervisory Control and Data Acquisition
UNICRI	The United Nations integrated crime and Research Institute
UNO	United Nations Organization

LIST OF CASES

1. **Beit Sourik Village Council v. The Government of Israel 2004.**
2. **Legality of the Threat and Use of Nuclear Weapons, International Court of Justice 1996.**
3. **Prosecutor v. Dusko Tadić (Interlocutory Appeal on Jurisdiction) ICTY Appeals Chamber 1995.**
4. **Prosecutor v. Haradinaj, ICTY, 2008.**
5. **Prosecutor v. Jean-Paul Akayesu, ICTR 1998.**
6. **The Prosecutor v. Fatmir Limaj, ICTY 2005.**

LIST OF FIGURES AND TABLES

Figure 1: Cyber warfare compared to traditional warfare representing of the kind of war which is Waged as they identify.

Figure 2: Relationship Between Cyber-actions.

Table 1: Essential Characteristics of Different Cyber-Actions.

Table 2: Specific Cyber Warfare Activities as DPH.

INTRODUCTION

The concept of cyber warfare does not cover the notion of Armed Conflict given by International Humanitarian Law and therefore, it is significant to reform and noticeably define the rules of that Law on cyber warfare in order to limit its potential effect on people.

The word 'war'¹ invariably prompts images of a battle front, guns pointed at the ready, men in uniform standing with grim expressions, tanks, bombs, grenades, trenches, death and destruction.² While this sounds like a universal form of war, common throughout much of history.³ However, the accelerated technological evolution has led to the development of new means and methods of conducting hostilities, not simply the weaponry and artillery of war, but the very battlefield itself. For there now exists a

¹ Generally, word "war" means a state of armed conflict between different countries or different groups within a country. For details see, dictionary Merriam Webster, available at, <http://www.merriam-webster.com/war>, (last accessed: October 1, 2015).

² Ian Brown, *International Law and the Use of Force by States* (UK: Clarendon Press, 1969), 47.

³ Ibid.

bloodless, weaponless warfare, the Cyber warfare⁴. It is concerned as current debatable issue under International Humanitarian law (herein after- IHL).⁵

In the past 150 years of IHL frequently all treaties were not stipulated in advance whether a war or armed conflict occurred or not, albeit; treaties were so far enacted after the arise of a certain warfare.⁶ Rules for war on land, sea, and air exist, but cyberspace is undefined.⁷ 21st century is the Era where several new military warfare concepts have emerged and posed a challenge for IHL.⁸ The concept of Cyber warfare is one of them.⁹ There is no internationally agreed definition for Cyber warfare albeit, for the sake of understanding it is Internet- based conflict involving politically motivated attacks on information and information systems.¹⁰ It can also be defined as a well-known trend through which foreign invaders can access information structures. It can also be declared a well-known trend through which foreign invaders can access information structures.

⁴ Cyber warfare involves units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks. These individuals often operate under the auspices and possibly the support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner. For details see, Cordula Droege, "Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross* 94:886 (2012), 533-556.

⁵ IHL also known as Jus in Bello or Law of Armed Conflict (herein after- LOAC) is a set of rules that seek to limit the effects of armed conflict. For details see, Jonathan Crowe, *Principles of International Humanitarian Law* (UK: Edward Elgar Publisher, 2013), 71-101. See also, Dan Saxon, *International Humanitarian Law and the Changing Technology of War* (Brill: Nijhoff, 2013), 114.

⁶ Vincent Bernard, "The Quest for Humanity – 150 Years of International Humanitarian Law and Action", *International Review of the Red Cross* 888(2012), available at: <https://www.icrc.org/en/ILpdf>, (last accessed: October 10, 2015).

⁷ Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkley Journal of International* 27:193(2009), 83-116.

⁸ Jason Barkham, "Information Warfare and International Law on the Use of Force", *New York University, Journal of International Law & Pol.* 34:57(2001), 62-63.

⁹ Ibid.

¹⁰ Ibid.

One of the means and methods of Cyber War are cyber-attacks.¹¹ Up till now no definition of Cyber-Attack is recognized at an international level however, it may generally be understood to refer to the hostile use of Malware, which is software implemented for the purpose of disrupting the correct operation of computer and network-based.¹²

Currently, no treaty exists to expressly regulate international cyber-attacks.¹³ Cyber-attacks are “global in nature therefore, the need of time is to amend or adapt existing legal frame work of IHL to cyber warfare, as the threat of a Cyber-Attack within a global cyberspace requires a global solution.”¹⁴

Literature Review

The literature review related to a certain area has always been a fundamental ingredient for its assembling and construction. This part of the research work signifies marvelous efforts done with regards to the phenomenon of the thesis. For literature review, the researcher got help from available resources some of which were primary, that include international legal instruments such as Geneva Convention 1949 and other were secondary such as books and articles some of them are mentioned below:

¹¹ Charles J. Dunlap, “Perspectives for Cyber Strategists on Law for Cyber War”, *Strategic Studies Quarterly* (2011), 81.

¹² Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber warfare* (Cambridge University Press, Cambridge, 2013), 247.

¹³ Barkham, “Information Warfare and International Law on the Use of Force”, 62-63.

¹⁴ They occur in cyberspace, which involves thousands of interconnected networks across the globe. Moreover, “International laws further establish uniformity and clarity where numerous domestic laws may not.” See briefly, Oona A. Hathaway, Crotoof Rebecca, Levitz Philip, et al, “The Law of Cyber-attack”, *California Law Review* 100 (2012), 817–885.

Heather Harrison Dinniss, a Senior Lecturer at the International Law Centre of the Swedish Defence University in her book *Cyber war and the Laws of War*¹⁵ has analyzed the status of computer network attacks in International Law and examined their treatment under the laws of armed conflict. The first part of the book deals with the resort to force by states and discusses the threshold issues of force and armed attack by examining the permitted responses against such attacks. The second part offers a comprehensive analysis of the applicability of international humanitarian law to computer network attacks. By examining the legal framework regulating these attacks and addressing the issues associated with this method of attack in terms of the current law and explore the underlying debates which are shaping the modern laws applicable in armed conflict. The book is undoubtedly a meaningful contribution to the literature on cyber warfare. However, this thesis tends to explore whether IHL applies as it is to cyber warfare or it need to be changed to accommodate this new means of warfare. Therefore, the researcher has to explore other significant work for a more comprehensive understanding to recommend some better points to uproot the concerned problem.

Scott Shackelford, Associate Professor of Business Law and Cyber-security Law in his article, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*¹⁶ has analyzed that International law has been slow to adapt. The facts on the ground, and the widespread, amorphous use and rapid evolution of the internet in many ways challenge state sovereignty. He has advocated that the best way to ensure a comprehensive regime for cyber-attacks is through a new international accord dealing

¹⁵ Heather Harrison Dinniss, *Cyber war and the Laws of War* (New York: Cambridge University Press, 2014).

¹⁶Shackelford, Scott, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, *Berkley Journal of International Law* 25:3(2009) available at: <http://ssrn.com/abstract=1396375>, (last accessed: October 9, 2015).

exclusively with cyber security and its status in international law. Further this paper has examined the most apt analogues in international law to form an appropriate legal regime for the various types of cyber-attacks - whether it is humanitarian law, human rights law, or some novel combination of these and other treaty systems. According to him, the main failings of existing international treaties that touch on cyber law though are those that neither carry enforcement provisions nor do they specify how the frameworks change or fall away entirely during an armed attack. The researcher agrees with the author. However, the researcher needs further literature to review and to reach some possible and practicable recommendations regarding cyber-attacks to stop them.

Michael N. Schmitt, Professor and Chairman, International Law Department, United States Naval War College, in his article *Classification of Cyber Conflict*¹⁷ examines the classification of conflicts consisting of only cyber operations under IHL. 'International armed conflicts' are those which are 'armed' and 'international'. The article contends that the former criterion is met when cyber operations amount to an 'attack' because they injure individuals or damage objects, whereas the latter requires that the operations be between or attributable to States. 'Non-International Armed Conflict' occurs when hostilities between a State and an 'organized' armed group reach a particular level of intensity. To be sufficiently intense, such cyber operations must be 'protracted'; isolated incidents do not suffice. Intensity also requires that the level of violence exceed that of riots or civil disturbances. Injury or damage is not alone sufficient. Cyber operations conducted by individuals cannot qualify because they are

¹⁷ Michael N. Schmit, "Classification of Cyber Conflicts", *International law Studies*, 89(2013), 240-258.

insufficiently 'organized'. Groups organized on-line may be assessed on a case-by-case basis, but the traditional organization criteria render it difficult for them to qualify. The article concludes that while cyber exchanges may sometimes amount to international armed conflict, classification as non-international armed conflict is problematic.

This research work has asserted that cyber warfare does not cover the notion of armed conflict even in case of armed conflict. Because all cyber-attacks do not trigger an armed conflict, only those which rise to the level an attack under IHL which have not yet observed by international community.

In the book *Contesting Cyber Space and Coming Crises of Authority*¹⁸ by Ronald Deibert and Rafal Rohozinski has examined the increasing struggle for superiority and the competition for power, influence, and control which defines the contestation of cyberspace. They have laid out the major driving forces of cyberspace contests: the continued rapid expansion of cyberspace throughout all aspects of society, including the rapid rise of mobile access devices, the increasingly dynamic competition among states for influence in and through cyberspace; manifest in the creation of dedicated cyber armed forces and an arms race in cyberspace; and more aggressive measures taken by authoritarian and democratically challenged states to counter a regime mobilization through offensive activities. In this book authors have covered moral, social and political aspects of cyber space and its role in uprising of cyber warfare. However, attention should be given to legal aspects of cyber space due to increase in unregulated incidents of cyber-attacks. For this purpose, the researcher, therefore, needed to review more

¹⁸ Ronald Deibert, Rafal Rohozinski, *Cyber Space and Coming Crises of Authority* (Oxford: MIT Press, 2011).

literature which could clear the mind of the readers regarding the legal aspects of cyber space operations.

Dan Saxon international law at Leiden University College in The Hague and formerly, a Senior Prosecutor at the United Nations International Criminal Tribunal for the Former Yugoslavia, in his book *International Humanitarian Law and the Changing Technology of War*¹⁹ explores the legal challenges for armed forces resulting from the development and use of new military technologies – automated and autonomous weapon systems, cyber weapons, “non-lethal” weapons and advanced communications - for the conduct of warfare. It has provided analysis and recommendations for armed forces as to how these new technologies may be used in accordance with international law particularly use of force under article 2(4) of UN charter in cyber context. However, it is also significant to review cyber warfare in the light of the notion of armed conflict under IHL because application of IHL comes into play afterwards.

Oona A. Hathaway, Professor of International Law at the Yale Law School, in her article, *the Law of Cyber-Attack*,²⁰ has examined how existing law may be applied, adapted and amended to meet the distinctive challenge posed by cyber-attacks as means and methods of cyber war. It begins by clarifying what cyber-attacks are and how they already are regulated by existing bodies of law, including the law of war, international treaties, and domestic criminal law. This review has made clear that existing law effectively addresses only a small fraction of potential cyber-attacks. This Article

¹⁹ Dan Saxon, *International Humanitarian Law and the Changing Technology of War* (Brill: Martinus Nijhoff, 2013).

²⁰Oona A. Hathaway, Crootoof Rebecca, Levitz Philip, et al, “The Law of Cyber-attack”, *California Law Review* 100 (2012), 817–885.

concludes that a new, comprehensive legal framework at both the domestic and international levels is needed for more effective addressing of the cyber-attacks. Yet the challenge cannot be met by domestic reforms alone. International cooperation will be essential to a truly effective legal response. Although, the author has comprehensively covered the subject however, instead of going into making of separate legal framework to regulate cyber-attack better option is to amend IHL in context of this new form of warfare which would be enough able to address a large number of potential cyber-attacks more effectively.

Framing of Issues

The above mentioned literature review has brought forth the following issues which the present thesis will address:

1. What is Cyber-Attack and Cyber Warfare?
2. Can cyber-attack trigger an Armed Conflict?
3. Whether cyber warfare fits into the bifurcated armed conflict and existing IHL rules apply on cyber warfare or not, if so, do they deal adequately with this new element of war?
4. What are the current challenges of cyber warfare and what seems the impact of cyber warfare on civilians?
5. What is status of those conducting Cyber-attacks whether they are combatants, civilians, or civilians taking direct part in hostilities under IHL?

For analyzing these issues this thesis is divided into following four chapters.

The first chapter, *Cyber Warfare: Nature and Scope*, aims at clarifying the notion of cyber warfare, cyber space cyber-attacks, cyber-crime. It also covers cyber weapons and challenges raised by cyber warfare.

The second chapter, *Cyber Warfare and the Notion of Armed Conflict*, covers the basic typology of armed conflict under IHL and assess whether cyber warfare fits into the ambit of dichotomous classification of armed conflicts under IHL or not.

The third chapter, *Application of International Humanitarian Law on Cyber warfare*, first considers the general applicability of the IHL to cyber-attacks. Then it turns its direction to the application of cardinal principles of IHL on cyber warfare.

The fourth Chapter, *Combatant Status, Direct Participation in Hostilities and Cyber warfare* provides an examination of status of persons involved in cyber warfare in the light of combatant's status and civilian's direct participation in hostilities under IHL, and assesses whether these rules are relevant to cyber warfare or not.

Finally, the thesis is wrapped up by giving conclusion and some recommendations.

CHAPTER 1

CYBER WARFARE: NATURE AND SCOPE

“You can’t say that civilization don’t advance, however, for in every war they kill you in a new way.”

—Will Rogers, the New York Times,

December 23, 1929.

Introduction

Advancement in internet particularly in computer technology has brought countless advantages to the public as well as State activity, it has disadvantages too, as the nervous system of our contemporary world is a double-edged sword.²¹ It is now a factual thing that over the last few years cyber space is not only an arena for hacker or criminal activity but also for attacks of a different kind.²² The use of cyber technology has caused an extensive transformation and a major challenge to the regulation of the waging of

²¹ Rapid development in the fields of science and technology can be seen in the last century. Each new technology has not only effect the nature of peace but also on war and ultimately outcome of battles got changed. And it resulted in introduction of new, unique and superior ways of fighting. The two gulf wars and number of nation states set up and took note of how a sudden Revolution in Military Affairs had taken place. The first Morse Code, sent in 1836 to a distance of 500 yards over a wire, set the foundation for a revolution that of such technologies is now required to ensure information assurance and information dominance at all times. For details see, Evangelia Linaki, “Cyber warfare and International Humanitarian Law: A Matter of Applicability”, *Journal of Law of Peace and Armed Conflicts* 27:4(2014), 169-175, <http://www.academia.edu/10057719>, (last accessed: May 16, 2016). See also, Bill Kasperkosk, Morse Code Secrets, available at, <http://www.skecgroup.com/morse>, (last accessed: March 12, 2016).

²² Nilz Melzer, “Cyber warfare and International Law”, 22.

armed conflicts. The incident of Russian-Georgian armed conflicts in 2008 where cyber-attacks were used to hamper the Georgian communication and in 2010 the deployment of the Stuxnet worm to disrupt Iranian Nuclear Facilities have proven that the Cyber space has emerged as a new battlefield and cyber activities have to be considered as new means of warfare. Hence, challenging us to revise our former understanding on the changing aspects of armed conflict and on the top of that it has no universally accepted definition.²³

Universally accepted definitions for cyber space, cyber warfare and cyber-attacks are under discussion. Therefore, this thesis differentiates between the various concepts and natures of cyber actions, precisely and this chapter covers already prevalent terminology in the cyber warfare research field.

1.1 Defining Cyber Warfare

The complex nature of cyber warfare raises many questions regarding definitions, differences with reference to other warfare, and compatibility with *jus ad bellum*²⁴ and *jus in bello*.²⁵ The solution of some questions lies in interpretation of existing law, others remain open and without a clear solution. Such complexity is due to the fact that attacks may differ reasonably depending on the final target, scope, hardware and software tools used. Commonly, they all aim to exploit computer systems and

²³ Michael Gervais, "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law* 30:2(2012), 525-579, available at, <http://scholarship.law.berkeley.edu>, (last accessed: February 22, 2016).

²⁴Jus ad bellum is a body of International Law governing the resort to force as instrument of national policy. For details see, Crowe Jonathan, *Principles of International Humanitarian Law* (UK: Edward Elgar Publisher, 2013) 12.

²⁵ Jus in bello is a body of International Law regarding State's conduct during a war. For details see, Jonathan, *Principles of International Humanitarian Law*, 12.

networks in order to achieve a military advantage. Due to the wide range of information technologies, scopes and targets, it is quite difficult to provide a comprehensive definition. There are not many definitions of cyber war and cyber warfare that are available. If put simply, Cyber warfare is war in cyber space. The United Nations Integrated Crime and Justice Research Institute (UNICRI) defines Cyber warfare as “any action by a nation state to penetrate another nations’ computer networks for the purpose of causing damage and the phenomenon also includes ‘cyber hooliganism’²⁶, ‘cyber vandalism’²⁷ and cyber terrorism²⁸ undertaken by a nation state.”²⁹ According to UNICRI’s definition cyber warfare can consist of many threats, namely:

- (a) Online acts of espionage and security breaches- these are carried out to acquire national material and information of a sensitive or classified nature

²⁶ Computer network related mischief such as defacing websites or releasing a virus or worm, without causing serious disruptions to the general population, widespread panic nor terror is known as cyber hooliganism. For details see, Cyber warfare or Cyber hooliganism, available at, <http://seclit.com/archives/374/>, (last accessed: April 7, 2017).

²⁷ Computer vandalism is a type of malicious behavior that involves damages computers and data in various ways and potentially disrupting businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks such as erasing hard drive data or extracting login credentials. Computer vandalism differs from viruses, which attach themselves to existing programs. For details see Cyber vandalism, available at, <https://asaka.persky.com/internet-security-center/threats/>, (last accessed: April 7, 2017).

²⁸ It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. For details see, Cyber Terrorism by Sarah Gordon, available at, <https://www.symantec.com/cyberterrorism.pdf>, (last accessed: April 7, 2017).

²⁹According to The United Nations integrated crime and justice research institute (UNICRI) Cyber warfare, cyber espionage, terrorist use of the internet, online crimes against property and persons embody growing transnational menaces. The United Nations Interregional Crime and Justice Research Institute (UNICRI) organizes a specialized course on cyber security journalists and public information professionals to deepen the understanding of these terms and emerging challenges posed by them. For details see, Understanding and Reporting on Cyber Threats, available at, <http://www.unicri.it/news/article/understand/>, (last accessed: last accessed: March 15, 2016).

through the exploitation of the internet. For instance, exploitation of network flaws through malicious software.

- (b) Sabotage –when one nation state to disrupt online communication systems of another nation state via internet. For example, to sabotage military communication networks with the intent to cause damage and disadvantage.
- (c) Attacks on Supervisory Control and Data Acquisition (SCADA)³⁰ networks and National Critical Infrastructures.³¹

Richard A. Clarke, a former “counter-terrorist tsar” and an expert on a cyber-security, provides a commonly accepted description of cyber warfare “actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.”³²

1.1.1 Two Distinct Aspects of Cyber warfare

On one occasion Cyber warfare is defined as follows:

Cyber warfare is [the warfare grounded on certain] uses of information and communication technologies(ICTs) within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational

³⁰ SCADA stands for supervisory control and data acquisition. It is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions. SCADA is used in power plants as well as in oil and gas refining, telecommunications, transportation, and water and waste control. For details see definition of SCADA, available at, <http://whatis.techtarget.com/definition/>, (last accessed: March 15, 2016).

³¹ National Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being people and the effective functioning of government. For details see, National Critical Infrastructure, available at, <http://www.definitions.net/definition/infrastructure>, (last accessed: April 6, 2017).

³² Richard A. Clarke, Robert Knake, *Cyber War* (UK: Hyper Collins, 2010), 34.

environment, with agents and targets ranging both on physical and non-physical domains and whose level of violence may vary upon circumstances.³³

This definition reveals two aspects of Cyber warfare, its information nature and its transversality.³⁴ Cyber warfare rests on the military deployment of technological artifacts devoted to elaborate, manage and communicate data and information that's why it is informational in nature. And it is related to the Information revolution.³⁵

The 'Information Revolution' has brought the non-physical domain to the fore and makes it as important and valuable as the physical one. Cyber warfare indicates that there is a new environment, where physical and nonphysical entities coexist and are somehow equally valuable. Moreover, where states have to prove their authority and new means and methods of warfare are being developed specifically to be used in this new environment.³⁶

The shift towards the non-physical domain provides the ground for the transversality of Cyber warfare. This complex aspect can be better grasped by comparing cyber warfare with traditional form of warfare.

³³Mariarosaria Taddeo, "Information Warfare: The Ontological and Regulatory Gap", *APA Newsletter on Philosophy and Computers* 14:1(2014), 13-20.

³⁴ This aspect seems quite different from traditional warfare, which is violent, conducted by militaries and mainly by human agents. For details see, Gervais, "Cyber Attacks and the Laws of War", *Berkeley Journal of International Law* 30:2(2012), 525-579.

³⁵ The Information Revolution is a multi-faced phenomenon. It rests on the development and the capillary dissemination of the use of ICTs, which have a wide impact on several of our daily practices, from working, to interacting with other human beings, to driving around and planning holidays. The dissemination of ICTs has important philosophical implications for the Information Revolution changes fundamentally the way reality is perceived and understood. For details see, Luciano Floridi, "The Philosophy of Information: Ten Years Later as a Conceptual Framework", *Knowledge, Technology & Policy* 23:2(2010), 253-270.

³⁶ Mariarosaria Taddeo, "An Analysis for A Just Cyber Warfare", *Philosophy and Technology* 25:1 (2012) 105-120. available at, <https://philpapers.org/rec/TADAAE>, (last accessed: March 26, 2016).

From aforementioned definitions it is observed that cyber warfare refers to conducting military operations in the cyber domain. Like other forms of warfare, the intent of operation in this virtual domain is to influence the will and decision making capabilities of the enemy's political leadership, economic power, armed forces and war waging capabilities of states.³⁷ Cyber war is a conflict in virtual space with means of information and communication technology and networks. These operations in the virtual world are often referred to as computer network operations or cyber-attacks.³⁸

1.1.2 Cyber warfare Versus Traditional Warfare

Cyber warfare seems to be different from traditional warfare in a sense; it may not be violent and destructive.³⁹ It may involve a computer virus capable to disrupt or deny access to the enemy's database, and in doing so cause a severe damage to the enemy without applying physical force or violence. Similarly, it is not necessary that cyber warfare involve human beings. Cyber warfare in this context can be conducted by a computer virus, aiming other artificial agents or informational infrastructures, like websites or databases (see Table 1).⁴⁰ As remarked above, this aspect of cyber warfare differentiates it the most from traditional warfare, and also engenders ethical and legal problems posed by cyber warfare. However, transversality makes adoption of Cyber

³⁷Taddeo, "An Analysis for A Just Cyber Warfare", 105-120.

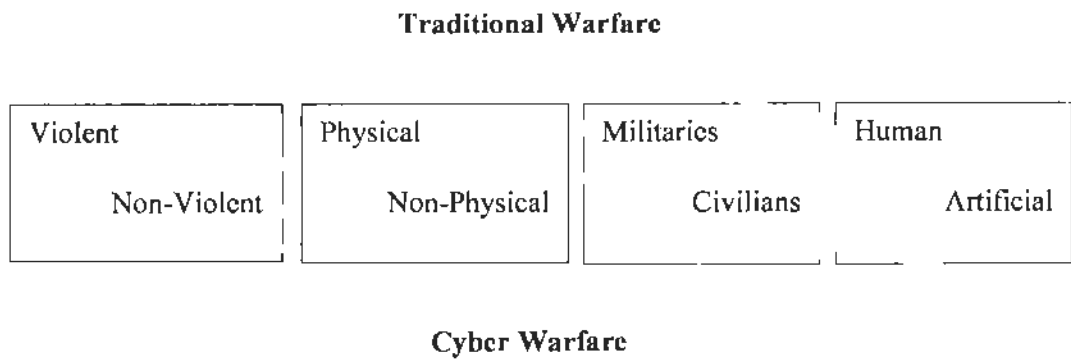
³⁸Graham H. Todd, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", *The Air Force Law Review* 64(2009), 65-102, available at, <https://cdde.20pdf>, (last accessed: March 26, 2016).

³⁹ Ibid.

⁴⁰However, keeping in mind its transversality with respect to the level of violence and may become from non-violent to more violent cyber warfare is to be feared as much as traditional warfare. For example, consider a cyber-attack targeting a military aerial control system causing aircraft to crash. Ibid.

warfare more likeable from legal, ethical and political perspectives.⁴¹ In addition, Cyber warfare seems bloodless and therefore it liberates political authorities of the burden of justifying military actions to the public opinion.⁴²

Figure 1: Cyber warfare compared to traditional warfare representing of the kind of war which is Waged as they identify.⁴³



Traditional war is understood as the use of a force through the state military forces to determine the conditions of governance over a determined territory. It is violent in nature, involves the sacrifice of human lives, the damage of both military and civilian infrastructures. The problem in waging traditional warfare is how to reduce or minimize damages while ensuring to overpower the enemy and cyber warfare is contrary to it as shown in figure 1.

⁴¹ John Arquilla and David Ronfeldt, *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: Rand Cooperation, 1997), 231.

⁴² Mays, "Cyberwar as Anti-War: The Keystroke is Mightier than the Sword", 10.

⁴³ Taddeo, "An Analysis for A Just Cyber Warfare", 105.

1.2 Defining Cyberspace

To understand cyber warfare one must know about cyber space. Besides air, land, sea and outer space now there is a fifth domain, the cyber domain or cyberspace. The word Cyber and Cyberspace⁴⁴ first appeared in number of science fiction literature. And through the work of William Gibson, a science fiction author, the word became prominently identified with online computer networks.⁴⁵ Since, the creation of the term Cyberspace a large number of definitions of this term too appeared. It is therefore, significant to analyze some of these definitions for better understanding of Cyberspace.⁴⁶

The word 'Cyberspace' is combination of two words that is cyber(netics) and space. Word 'Cyber' is derived from Greek word '*kybernetics*' which means one who steers or governs. On the other hand, word Space has many meaning in English, referring to philosophical, physical, geographical, mathematical, social, psychological and many

⁴⁴ The word "cyberspace" is credited to William Gibson, who used it in his book, *Neuromancer*, written in 1984. Gibson defines cyberspace as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system, unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data". Unlike most computer terms, "cyberspace" does not have a standard, objective definition. Instead, it is used to describe the virtual world of computers. For example, an object in cyberspace refers to a block of data floating around a computer system or network. With the advent of the Internet, cyberspace now extends to the global network of computers. So, after sending an e-mail to anyone, one could say he sent the message to them through cyberspace. For details see, William Gibson, *Neuromancer* (New York: Berkley Publishing, 1989), 16.

⁴⁵ *Ibid.*, 129

⁴⁶ The United Nations Organization (UNO) defines cyber as "the global system of systems of Internetted computers, communications infrastructures, online conferencing entities, databases and information utilities generally known as the Net." Usually it refers to Internet; but the term may also be used to refer to the specific, bounded electronic information environment of a corporation or of a military, government, or other organization. See, United Nations(UN) terms, <http://unterm.un.org/dgaacs/unterm.nsf>, (last accessed: May 15, 2016). One of the most comprehensive definition of Cyberspace is given by Dr. Daniel T Kuehl, Professor of Systems Management at the Information Operations, National Defense University Virginia. He contends that, "Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected ICT based systems and their associated infrastructures." For details see, Chapter 2, "From Cyberspace to Cyber power: Defining the Problem" by Dr. Daniel T Kuehl in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, *Cyber power and National Security* (Washington D.C: National Defence University Press, 2009), 24, available at, <https://books.google.com.pk/books>, (last accessed: March 02, 2016).

other properties. It can also be defined as a “boundless, three dimensional extents in which the event and object occur and have relative position and direction.”⁴⁷

On another occasion cyber space is defined as; “A domain characterized by the use of electronics and electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought as the interconnection of human beings through computers and telecommunication, without regard to physical geography.”⁴⁸

David Clark, Senior Research Scientist, MIT's Computer Science and Artificial Intelligence Laboratory, has suggested a four layered model to understand cyber space given as follow:⁴⁹

- (a) The participants in the cyber-experience, who communicate, work with information, make decisions and carry out plans, and transforms the nature of cyberspace by working with its component services and capabilities.
- (b) The transmission and transformation and storage of information in cyberspace.
- (c) The logical building blocks which generate the services and support the platform nature of cyberspace.
- (d) The physical foundations to support the logical elements.⁵⁰All the aforementioned definitions contain some common elements, like; Computer networks,

⁴⁷ Gibson, *Neuromance*, 17.

⁴⁸ This definition is given by Margaret Rouse, who writes for and manages WhatIs.com, Tech Target's IT encyclopedia and learning center. For details see, defining Cyberspace, available at, <http://searchsoa.techtarget.com/definition/cyberspace>, (last accessed: February 28, 2016).

⁴⁹ For details see, David Clark, “Characterizing Cyberspace: Past, Present and Future”, available at, <http://www.acmepublic.com/resource-library/whitepapers/characterizing-cyberspace-past-present-and-future-david-clark/>, (last accessed: March 12, 2016).

Information space and resources available on the internet. If one analyses these definitions and many more invented later on, these indicates that:

- (a) Cyberspace is such type of domain where individuals and organizations use technologies, act and create effects.
- (b) The usage of energies and properties of the electromagnetic spectrum that sets cyberspace different from the Air and Space domains.
- (c) Another common factor perhaps also the most significant is the networking of interconnected ICT based systems and infrastructures. These systems have brought cyberspace to the forefront of debates over its impact on and importance to national security and international affairs.⁵¹

1.2.1 Characteristics of Cyberspace

Cyberspace has some unique characteristics that differ it from the traditional, physical, kinetic battlefield.⁵² Understanding those characteristics means moving one step forward toward identifying the challenges that cyber warfare poses to IHL because those characteristics do not exist in the world of the kinetic or traditional warfare.⁵³

⁵⁰This four-layer model suggests that it is not only the computer, the interconnecting networks or the internet that creates the phenomenon of cyberspace. Ibid.

⁵¹ Sean Brandes, "The Newest War fighting Domain: Cyberspace", *Synesis: A Journal of Science, Technology, Ethics, and Policy* 4(2013), 90-95, available at, <http://www.synesisjournal.com/vol1.pdf>, (last accessed: March 03, 2016).

⁵² Cordula Drooge, "No Legal Vaccum in Cyberspace", available at, <https://www.icrc.org/eng/pdf>, (last accessed: May 15, 2016).

⁵³ Ibid.

- Interconnectedness and National Dependency** The tendency of states today to use electronic or computer networks to base their 'critical infrastructure' is growing rapidly. This infrastructure generally consists of essential services, for example telecommunication, finance, transportation, energy etc. Dependence of nations on those critical information infrastructures is undisputed and today functioning without those infrastructures cannot be imagined.⁵⁴ Therefore, massive damage can be done if systems are disrupted by keeping in view the sensitive nature of critical infrastructure and indirect effects on networks of other sectors.⁵⁵ The military highly depends upon electronic networks, mainly for communication and logistics.⁵⁶ Moreover, interconnectivity of cyber infrastructure, globally and domestically, prevents the distinction between the military and civilian infrastructure which in turn makes it difficult to separate a specific cyber target, and at the same time causing uncertainty as to the scope of the damage that will be the result of the cyber-attack.⁵⁷
- Anonymity** The users in cyberspace are anonymous which characterizes it. Besides anonymity it is also possible for perpetrators to evade identification by sophisticated manners, such as proxy,⁵⁸ which disguises the identity of the actual perpetrator, or simply by using computer in another uninvolved state, which

⁵⁴ Ido Kilovaty, "Cyber warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", *National Security Law Brief* 5:1 (2014), 91-124, available at, <http://digitalecommons.wcl.american.edu/cgi/viewcontent.cgi>, (last accessed: May 19, 2016).

⁵⁵ Jason Andress and Steve Winterfeld, *Cyber warfare Techniques, Tactics and Tools for Security Practitioners* (USA: Syngress, 2011), 22

⁵⁶ Ibid, 23.

⁵⁷ Kilovaty, "Cyber warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", 95.

⁵⁸ Handler S. Gosnell, "The New Face of Battle: Developing A Legal Approach to Accommodate Emerging Trends in Warfare", *Stanford Journal of International Law* 48(2012), 233-250.

results in confusion and false perpetrator identification by the victim state. Physical evidence, visibility and the intent of the perpetrator are all elements of anonymity, which differs the battlefield of cyberspace from the physical one.⁵⁹ Physical evidence exists in the physical battlefield, in the shape of kinetic weapon used, the physical damage caused by that weapon, the intelligence that binds a specific perpetrator to the event. However, in the cyberspace, there is less or almost physical evidence nonexistent and, at times, gathering such evidence is very challenging.⁶⁰ And, the intent and motivation behind the attack are usually apparent from the investigation of a physical kinetic incident while in case of cyberspace, cyber-attacks mostly remain 'silent' with regard to the intent.⁶¹

- **Simplicity, Quickness and Ease of Entry** Cyberspace allows actions to be taken in fairly simple and quick ways which is contrary to the war in the physical realm. As physical actions require physical preparations, including troops, weaponry and precise military strategies, cyber-attacks—apart from preparing the specific plan or malware, only require, a click of a mouse⁶². And physical actions are also restricted by their pace to a certain degree.⁶³ For instance, State A sends fighter jets to attack. In such a case State A is still bound by the fighter jets' speed limit and physical capabilities. On the other hand, despite the geographical distance cyber-attacks can happen instantly. These factors are forming a new system of conducting war, which may allow the weak states, unable to afford enormous

⁵⁹ Ibid.

⁶⁰ Ibid.

⁶¹ Christian Czosseck and Kenneth Geers eds., *The Virtual Battlefield: Perspectives On Cyber warfare* (Netherland: IOS Press, 2009), 66.

⁶² Ibid.

⁶³ Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, 56.

military expenses to engage in a relatively cheap, simple and quick scheme for waging a war.⁶⁴ Consequently, the relative ease of entry brings a diversity of players.

The high dependency of nation states' infrastructures on cyberspace, the anonymity encompassed by the cyberspace, and the simplicity of the cyberspace altogether reflect the uniqueness of cyberspace as opposed to the traditional instruments of warfare.⁶⁵

1.2.2 Forms of Operations in the Cyber Domain

Three different forms of operations in the cyber domain are: -

- (a) **Computer Network Attack:** Such operations are planned to disrupt, deny, degrade or destroy information stored in computers networks or the computers or networks themselves.
- (b) **Computer Network Exploitation:** In these operations networks are used for repossessing intelligences grade data and information from enemy computers.
- (c) **Computer Network Defense:** It comprises of all measures necessary for the protection of one's own ICT and infrastructures against intimidating computer network attacks and exploitation.⁶⁶

⁶⁴ Hathaway et al., "The Law of Cyber-Attack", 817-842.

⁶⁵ Ibid.

⁶⁶ Ibid., 9-10

1.3 Defining Cyber-attack

In cyber warfare, the method chosen is based on the goals of attacker. In order to understand cyber warfare, it is important to understand cyber-attack. Although, it has been debated upon throughout the last decades, sometimes addressing synonym concepts, sometimes similar and sometimes different developments even then cyber-attacks and operations in cyber space as instruments of warfare up to some extent still not known to the world.⁶⁷

Cyber-attacks also known as Computer Network Attack (CNA) are initiated in cyber space. Generally speaking, cyber-attack means deliberate manipulation of computer systems, technology-dependent enterprises and networks.⁶⁸ More generally, cyber-attacks are defined as “efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them.”⁶⁹ According to the U.S. Army’s Cyber Operations and Cyber Terrorism Handbook, a cyber-attack is: “The premeditated use of disruptive activities, or the threat there-of, against computers and/or networks,

⁶⁷ The denomination “Network-centric warfare” for instance has been more or less replaced by a deviating terminology in most academic research. The term cyberwarfare, can be understood as a military doctrine that relates to both offensive as well as defensive, operations in cyberspace. This term however has some unscientific connotation and is often used outside of academia. For details see, Handler, “The New Cyber Face of Battle, developing a Legal Approach to Accommodate Emerging Trends in Warfare”, 233-250. Other terms used are for example by Michael N Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, in Michael N Schmitt (Ed.), *Essays on Law and War at the Fault Lines* (Netherlands: Asser Press: 2012), 175, available at, <http://download.springer.com/static/pdf/>, (last accessed: January 31, 2017); Computer network attacks: “operations to disrupt, deny, degrade, or destroy information resident in computers and networks themselves” and information warfare: “information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries”.

⁶⁸ Afroditi Papanastasiou, “Application of International Law in Cyber warfare Operations”, *Social Science Research Network* 3(2010), 31-57, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1673785, (last accessed: March 10, 2016).

⁶⁹ Matthew C. Waxman, “Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)”, *Yale Journal of International Law* 36(2011), 421-422.

with the intention to cause harm or to further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.”⁷⁰

Malicious codes are used in cyber-attacks to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.⁷¹ Harm from these attacks can be inflicted either on a computer network, or physical facilities and persons. This makes cyber-attacks distinguishable from cyber-crimes.⁷²

1.3.1 Types of Cyber-Attacks

Cyber warriors have three types of cyber-attacks using their arsenal namely syntactic⁷³, semantic⁷⁴ and mixed cyber-attacks⁷⁵. The weapons vary in intensity, ranging from

⁷⁰ Critical Infrastructure Threats and Terrorism, U.S. Army Training & Doctrine Command, Dissent Handbook 1.02(2006), vii-2, available at, <https://fas.org/ftp/threat/terrorism/sup2.pdf>, (last accessed: November 15, 2016).

⁷¹ Natasha Solce, “The Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force”, *Albany Law Journal of Science and Technology* 18 (2008), 293-300.

⁷² *Ibid.*, 301 (explaining that those who commit cyber-crimes exhibit personal desires like stealing money whereas a cyber attack’s purpose can be to take out a military target). Cyber-crimes, like fraud or posting obscene and offensive content on the Internet, are governed by national criminal laws. The intentions of those that commit cyber-crimes are also very different from those who initiate cyber-attacks.

⁷³ Syntactic attack is that type of cyber-attack which is comprised of malicious code. Malicious code is computer language made to affect operating system of a computer in order to modify it, retrieve information, or destroy it.

⁷⁴ Semantic attacks alter the information on computer system. The semantic attack targets the information by substituting it with inaccurate or misleading information. Particularly, the Logic Bomb is one of the most dangerous semantic attacks. Due to implication their composition is that of a bomb. Logic bombs are planted in a targeted area and ignited upon desire. Upon ignition, logic bombs send false data to information systems that can cause them to malfunction. For details see, Lesley Swanson, “The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict”, *Loyola Law School International & Contemporary Law Review* 32(2010), 303-314, available at, <http://digitalcommons.lmu.edu/iccylaw/content.cgi?article=1010>, (last accessed: November 15, 2016).

⁷⁵ *Ibid.* The combination of syntactic and semantic attacks makes the third type of cyber-attack called as the mixed attack.

annoyance to destruction and may pose some serious threats to national security.⁷⁶ Some of the commonly recognized attack vectors are given as follow:

- (a) **Virus:** It is a self-replicating program that spreads through some form of infected files. It replicates by inserting its copies into another computer programs, data, or the boot sector of the hard drive. Often some harmful activities are performed by virus on infected hosts, like stealing hard disk space or CPU time, accessing personal information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts or logging their keystrokes. Subtypes of virus are file, system/boot record infectors and macros.⁷⁷
- (b) **Worms:** it is a self-replicating program that propagates without using infected files. Usually these worms spread via network services on computers or through email. Mostly they cause at least some harm to the network, even if only by consuming bandwidth contrary to viruses, they almost modify or corrupt files on targeted computers. Subtypes of worms include mass mailing via botnet.⁷⁸
- (c) **Trojans:** A program designed in such a way that appears benign to serve some malicious purpose. On the other hand, in computing Trojan or

⁷⁶ Gervais, "Cyber Attacks and Law of War", 525-579.

⁷⁷ Sharon R. Stevens, "Internet War Crimes Tribunals and Security in an Interconnected World", *Transnational Law & Contemporary Problems* 18(2009), 657-663.

⁷⁸The Morris worm - one of the first recognized worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the US' computer fraud and abuse act. For details see, Wolfgang McGavran, "Intended Consequences: Regulating Cyber Attacks", *Tulane Journal of Technology & Intellectual Property* 12 (2009), 259-26.

Trojan horse, is a non-self-replicating type of malware program containing malicious code. Upon execution, it carries out actions determined by the nature of the nature of the Trojan. Typically, it causes loss or theft of data, and possible system harm. Its subtypes are remote access and data destruction.⁷⁹

- (d) **Denial of Service Attacks:** In the context of computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS)⁸⁰ attack is an attempt to make a machine or network resource unavailable to its intended users. Generally, it may temporarily or indefinitely interrupts or suspends services of a host connected to the network. Although the motives, means to carry out an attack and targets may vary in DoS. In this type of attack legitimate users are not permitted to access or use the network.⁸¹

1.4 Cyber-Crime

Contrary to cyber-attacks, cyber-crime is a broad and analytically distinct concept. Although there is no universally recognized definition of cyber-crime,⁸² the aspects of cyber-crime are broadly recognized. By and large, cyber-crime is the use of a computer-based means to commit an illegal act. As goes a classic definition, cyber-crime is “any

⁷⁹ A Trojan often acts as a back door, contacting a controller which can then have unauthorized access to the affected computer. John anzano, “Deconstructing SubSeven, the Trojan Horse” *Journal of Sans Institute* (2003), 920-953, available at http://www.sans.org/reading_room/, (last accessed: November 15, 2016).

⁸⁰ Above all, DOS and DDOS attacks are of the most concern. DOS attacks temporarily or permanently incapacitate a website by overwhelming it with false data requests. The network becomes so overworked that it crashes. DDOS attacks are similar to DOS attacks, but use thousands of botnet computers that exponentially cause websites to crash, or alternatively damage the websites' host hardware

⁸¹ Duncan Blake & Joseph S. Imburgia, “Bloodless Weapons”? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as “Weapons”, *Air Force Law Review* 157:66(2010), 181-203.

⁸² Despite the fact that the word ‘Cybercrime’ has entered into common usage, many people would find it hard to define the term precisely. For details see, e.g., Sarah Gordon & Richard Ford, “On the Definition and Classification of Cybercrime”, *Journal of Computer Virology* 13:2(2006), 13-27.

crime that is facilitated or committed using a computer, network, or hardware device.”⁸³ In this light, cyber-crime is often defined by its means—that is, a computer system or network. As such, cyber-crime holds a very broad range of illicit activity. According to the priorities of the Department of Justice and FBI units’ -crimes are fraudulent practices on the Internet, online piracy, storage and sharing of child pornography on a computer, and computer interruptions.⁸⁴ Moreover, like all crimes, cyber-crimes are generally understood to be committed by individuals, not states.⁸⁵

1.5 Relation among Cyber-Attack, Cyber-Crime and Cyber Warfare

TABLE 2: Essential Characteristics of Different Cyber-Actions⁸⁶

Type of cyber-action	Cyberattack	Cybercrime	Cyberwarfare
Involves only non-state actors		•	
Must be violation of criminal law, committed by means of a computer system		•	
Objective must be to undermine the function of a computer network	•		•
Must have a political or national security purpose	•		•

⁸³ In addition, some proposed definitions are broad enough to include not only all crimes committed by means of a computer, but also any crime in any way involving a computer as a means or a target. For details see, Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (California: Greenwood Publishing Group, 2010), 19, available at, <https://books.google.com.pk/books?id=gsWQ-xgbLbUC&q>, (last accessed: May 19, 2016).

⁸⁴ Ibid.

⁸⁵ Ibid.

⁸⁶ Nathaway et al., “The Law of Cyber-Attack”, 817-842.

Effects must be equivalent to an “armed attack,” or activity must occur in the context of armed conflict			•
--	--	--	---

FIGURE 2: Relationship Between Cyber-actions⁸⁷

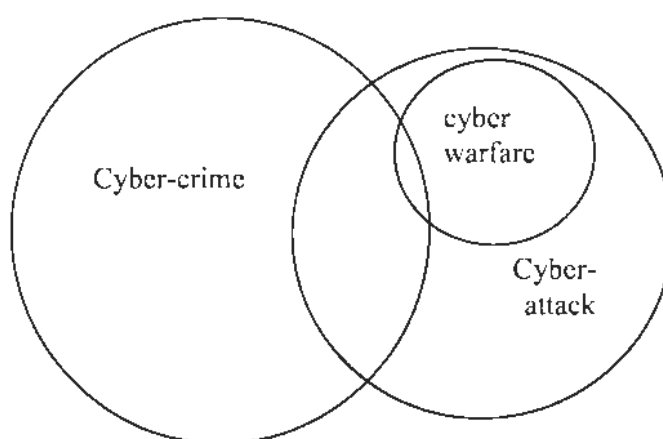


Table 1 and Figure 2 shows that a cyber-attack may be carried out by state or non-state actors, must involve active conduct, must aim to disrupt the function of a computer network, and must have a political or national security purpose. Some of the cyber-attacks are cyber-crimes, but not all cyber-crimes are cyber-attacks. On the other hand, cyber warfare always meets the conditions of a cyber-attack. To be noted, 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, deemed to be cyber warfare

As compared to cyber-attacks, cyber-crimes need not undermine the target computer network (though in some cases they may do so), and most do not have a

⁸⁷ Ibid.

political or national security purpose.⁸⁸ Mostly cyber-crimes do not also constitute cyber-attack or cyber-warfare, as shown in Figure 2.⁸⁹

1.5.1 Cyber-actions as Cyber-crime

Consider the following scenarios for a better understanding:

- First an illegal act for a political or national security purpose by means of a computer network but does not undermine that network is committed by non-state actor. For example, an individual may commit a cyber-crime by expressing political opposition over the Internet which is illegal under domestic law. In the same way, an individual may commit a cyber-crime by hacking major bank's records with a national security or political purpose but without damaging the bank's system in the process.⁹⁰
- Second, a non-state actor commits an illegal act by means of a computer network—and undermines a computer network other than political or national security purpose. Reconsider the hacker of bank's data, who manages to damage the bank's online account system but whose only purpose is economic gain. This would be considered as cyber-crime, but not a cyber-attack or cyber-warfare.⁹¹
- Third, for example a person who transfers child pornography would commit a cyber-crime but not a cyber-attack because the actions do not undermine the

TH:18225

⁸⁸ Sarah Gordan and Richard Ford, "On the Definition and Classification of Cybercrime", *Journal of Computer Virology* 2:1(2006), 13-27.

⁸⁹ Hathaway et al., "The Law of Cyber-Attack", 817-842.

⁹⁰ Gordan and Ford, "On the Definition and Classification of Cybercrime", 13-27.

⁹¹ Ibid.

function of a computer network and he or she is not motivated by a political or national security purpose.⁹²

1.5.2 Cyber-actions as Cyber-attack

As shown in Table 1 and Figure 2, some cyber-crimes are neither cyber-attacks nor cyber-warfare, in the same way some cyber-attacks are neither cyber-crimes nor cyber-warfare. Consider two scenarios:

- First, attacks carried out by a state actor, outside the context of an armed conflict, and its effects do not rise to the level of an armed attack. For example, an attack by the Chinese government on the Falun Gong website in 2011.⁹³
- The second scenario includes cyber-attacks by non-state actors that do not rise to the level of an armed attack and which do not constitute a cyber-crime, either because they have not been criminalized under national or international law or because they do not use computer-based means.⁹⁴ It is to be noted majority of cyber-attacks would likely involve computer-based means.⁹⁵ As shown in Figure 2 and Table 1, the overlapping area between cyber-crime and cyber-attack occurs when a non-state actor commits an illegal act by means of a computer network,

⁹² Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, 61.

⁹³ However, such attacks must satisfy all elements of the cyber-attack definition, including damaging the function of a computer network for a political or national security purpose. As noted above, however, any act by a state actor automatically satisfies the political or national security purpose requirement. For details see, Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, 61.

⁹⁴ *Ibid.* Practically speaking, it is unlikely for a private actor to purposefully undermine the function of a computer network without also violating the law but such gaps in the criminal law are conceptually possible. Because a cyber-attack must be “for a political or national security purpose,” the only actions falling into this category would be purposeful. Stefano Mele, “Legal Considerations on Cyber-Weapons and Their Definition”, 62.

⁹⁵ Though such means are not necessary to cyber-a While cyber-activity may constitute only cyber-crime or only cyberattack, a substantial proportion of cyber-crimes are also cyber-attacks. Papanastasiou, “Application of International Law in cyber warfare Operations”, 31-57.

undermines a computer network for a political or national security purpose. The consequences of this act would not rise to the level of an armed attack, or the activity would constitute cyber-warfare.⁹⁶

1.5.3 Cyber-actions as Cyber warfare

Cyber warfare is distinct among the three cyber-categories. Cyber warfare must also constitute a cyber-attack. In figure 2 the overlapping area between cyber-attack and cyber-warfare includes two types of attacks.

- The first type includes attacks carried out by any actor in the context of an armed conflict. However, those actions would not be considered as cyber-crimes, either because they are not war crimes, or do not employ computer-based means, or both.
- The second type of attacks are those which are carried out by a state actor and produce effects equal to those of a conventional armed attack.⁹⁷

Sometimes cyber warfare may also constitute both cyber-attack and cyber-crime. The area of intersection between all three circles as shown in Table 1 includes two types of attacks carried out by a non-state actor. First type of attacks is those which are carried out in the context of an existing armed conflict that hamper the function of a computer

⁹⁶ Note also that a state committing this very same act would not fall within this overlap, since only a non-state actor can commit a cyber-crime. Take, for example, a hypothetical group of individuals who hacked into the U.S. State Department's server and shut it down out of disdain for the U.S. government. This instance would fall within the overlap between cyber-crimes and cyber-attacks given that a non-state actor committed the act, for a political or national security purpose, and it undermined a computer network attacks. Hathaway et al., "The Law of Cyber-Attack", 817-842.

⁹⁷ Note that this use of force may be either lawful or unlawful; because the actor is a state actor, even unlawful actions do not necessarily constitute "cyber-crime." Hathaway et al., "The Law of Cyber-Attack", 817-842.

network for a political or national security purpose, violate the criminal law and are committed by means of a computer system or network. Another type of attacks is that produce effects equivalent to those of a conventional armed attack, undermine the function of a computer network for a political or national security purpose, and are violations of the criminal law committed by means of a computer system or network.⁹⁸

1.6 Cyber Weapons

One important matter at hand that need to be discussed is whether the tools used for most cyber warfare activities and attacks are to be considered weapons or not. Such has implications regarding International Law dealing with armed attacks, use or threat to use the force and regulation of hostilities. In this regard two different points of view are to be highlighted. One, tools like hardware equipment or computer code is considered as a weapon on the basis of possibility to cause harm or to allow the execution of an attack by these tools. Hence, “a cyber-weapon is the combination of a propagation method, exploits, and a payload designed to create destructive physical or digital effects.”⁹⁹

According to the second approach, the user’s or designer’s purpose and intention need to be evaluated in order to decide whether the tool (or tools) used are to be considered as a cyber-weapon or not. Hence, a weapon is cyber weapon if “a part of equipment, a device, or any set of computer instructions, used in a conflict among actors both National and non-National, with the purpose of causing (directly or otherwise)

⁹⁸ Hathaway et al., “The Law of Cyber-Attack”, 817-842.

⁹⁹ Trey Herr, “Prep: A Framework for Malware & Cyber Weapons”, *Journal of Information Warfare* 13:1(2013), 23-33, available at, SSRN: <http://ssrn.com/abstract=2343798>, (last accessed: November 15, 2016).

physical damage to objects or people, or of sabotaging and/or damaging in a direct way the information systems of a sensitive target of the attacked subject.”¹⁰⁰ Similarly, “cyber weapons are cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber-operation as an attack.”¹⁰¹ And some authors consider cyber weapon as a subset of weapons and define it as: “computer code that is used or designed to be used with the aim of threatening or causing physical, functional or mental harm to structures, systems or living beings.”¹⁰²

1.7 Challenges Raised by Cyber Warfare

The main concern is that there is only one cyberspace, shared by military and civilian users, and everything is interconnected. Therefore, key challenge is to make sure that attacks are directed against military objectives only and constant care must be taken to protect the civilian population and civilian infrastructure.¹⁰³ Also, the expected incidental civilian losses and damage or collateral damages must not be more than the concrete and direct military advantage anticipated by the cyber-attack. The attack must not be launched without fulfilling these conditions.¹⁰⁴ Another principal issues presented by cyber warfare is difficulty of identifying the attacker, which is essential for effective

¹⁰⁰ Stefano Mele, “Legal Considerations on Cyber-Weapons and Their Definition”, *Journal of Law and Cyber warfare* 3:1(2014), 58-64, available at, <http://www.jlcw.org>, (last accessed: November 15, 2016).

¹⁰¹ Schmidt (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 45.

¹⁰² Ibid.

¹⁰³ Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on A Normative Framework”, *Columbia Journal of Transnational Law* 37(1999), 35-40.

¹⁰⁴ Ibid.

deterrence. To assess this issue, one needs to distinguish between hacking data and destroying data. Since the data is not physically enclosed, secured only by encryption, and codes are designed to scramble a body of electronic data to make it unintelligible can be hacked from anywhere in the world.¹⁰⁵

Inexpensive nature of cyber warfare makes it insidious as it requires no raw materials, like uranium, no processing and no delivery vehicles, like missiles carrying nuclear weapons etc. These challenges compel the states to be extremely cautious when resorting to cyber-attacks.

1.8 Cyber Policing

To ensure cyber security states have adopted different policies.¹⁰⁶ One of such policies is cyber policing. Cyber policing is done by Police force or different government agencies. The policing of cyber-crime or cyber-attack is a very difficult concept. Because the lines of policing the internet becomes blurred within the legal concept as it is not necessarily a crime or attack in the legal sense.¹⁰⁷ Since, criminality is moving online, its volume is increasing, evolves constantly and rapidly, often leaves no clear of its occurrence,

¹⁰⁵ Unless the code is changed constantly (maybe every few seconds), the indispensable defensive response is to detect the hacking promptly and change the code. Stefano Mele, "Legal Considerations on Cyber-Weapons and Their Definition", 58-64.

¹⁰⁶ David S. Wall, "Policing Cyber-crime, Situating the Public Police in Networks of Security within Cyberspace, *Police Practice & Research: An International Journal* 8:2(2010), 183-205, available at, <http://ssrn.com/abstract=853225>, (last accessed: April 26, 2017).

¹⁰⁷ Ibid.

and leaves no scene to be examined.¹⁰⁸ Achieving the policing goals, therefore, presents specific challenges within the context of online crime.¹⁰⁹

Challenge of investigating cyber-crime is that the internet has increased the reach of criminals so they can now strike from thousands of miles away.¹¹⁰ The use of proxy servers, physical distances, international politics, and lack of legislation and national agreement to give up suspects for trial in another country, all make it difficult to investigate cyber-crimes and often impossible to bring the offenders to justice.¹¹¹

Maintaining public order online through cyber policing is also problematic. The police cannot have presence in all online forums all the time.¹¹²

Additionally, to these monitoring of internet is deemed as surveillance and infringement of right to privacy as well as freedom of expression.¹¹³ For example, the cyber-crime bill adopted by Pakistan's parliament last year is the latest one in a series of steps to curtail freedom of expression as well as civilians' right to access information.¹¹⁴ China's Great Firewall and state-sponsored blockages of thousands of dissident web

¹⁰⁸ For details see, Chuck Wexler, "Cybercrime: A New Critical Issue" in *The Role of Law Enforcing Agencies in Preventing and Investigating Cyber-crimes* (USA: Police Executive Research Forum, 2014), 5, available at, visit www.policeforum.org, (last accessed: April 26, 2017).

¹⁰⁹ Wall, "Policing Cyber-crime, Situating the Public Police in Networks of Security within Cyberspace, 183-205.

¹¹⁰ Angie Sapherson, "Policing Cyber-crime and key literature", available at, <https://www.academia.edu>, (last accessed: April 28, 2017).

¹¹¹ Ibid.

¹¹² Wexler, "Cybercrime: A New Critical Issue" 8.

¹¹³ For details see, Anja Kovacs, "Cyber Security, Cyber Surveillance and Online Human Rights", *International Journal of Cyber Warfare and Terrorism* archive 6:2(2013), 32-40, available at, www.gpdigital.org ... [Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights](http://www.gpdigital.org/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights), (last accessed: April 30, 2017).

¹¹⁴ Wall, "Policing Cyber-crime, Situating the Public Police in Networks of Security within Cyberspace, 183-205.

pages in Russia are some of the most blatant censorship projects that either block or criminalize content that opposes the government.¹¹⁵

Therefore, it is argued that to tackle the hurdles in ensuring cyber security via cyber policing different pathways need to be taken.¹¹⁶ For example, one option is to enhance police services abilities to achieve their current objectives in the cyber domain. This would see policing agencies receiving a much greater amount and wider range of resources to be able to detect and prosecute crime. Also, a significant increase of officers skilled in Information Technology, as well as a considerable expansion in the training agenda.¹¹⁷

Conclusions

A century ago, when one nation's army mobilized and massed at another's border, war was imminent. Outbreak of hostilities was a matter of time in such a situation. However, today technology has confused the application of old rules. In cyberspace, where attacks can be launched in milliseconds, a nation might not have enough time to detect an attack and mount a defense. Cyber warfare is all about disrupting, if not destroying, the critical infrastructure which is dependent on information and communications systems. It means trying to know all about an adversary while destroying it the same advantage. It means turning the "balance of information and knowledge" in one's esteem especially if the balance of force is not. It means using knowledge so that less labor and capital may have to be on expenditure. Cyber-attacks are here to stay. Because they provide a low-cost,

¹¹⁵ Ibid.

¹¹⁶ Wexler, "Cybercrime: A New Critical Issue" 15

¹¹⁷ Ibid.

remote, instantaneous, and powerful tactic of coercion or destruction, often without triggering accountability. These attributes guarantee that states and non-state actors will continue to develop and unleash cyber-attacks in the foreseeable future.

CHAPTER 2

CYBER WARFARE AND THE NOTION OF ARMED CONFLICT

Introduction

Some of the International Humanitarian Law topics are proving as problematic in modern warfare as “classification of conflict,” that is the identification of the type of conflict to which particular hostilities amount as a matter of law. Classifying the conflict in question is always the first step in any international humanitarian law analysis as the nature of the conflict determines the applicable legal regime. The current difficulties derive from the advent of hostilities over the past two decades that do not fit the traditional bifurcation of conflict into either State-on-state or purely internal. In future, cyber warfare will further complicate classification. Cyber operations have potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict. They are also inherently trans-border, therefore frustrating any approach to the classification based on geographical factors.

The first and foremost prerequisite for IHL to be applied is the existence of an armed conflict. This fact would lead to question whether a cyber-operation can amount to an armed conflict. In this light, in this chapter the researcher discusses the basic typology of armed conflict under international humanitarian law, the advent of cyber conflict.

Further the researcher explains whether cyber conflicts fit into the ambit of traditional classification of conflicts under IHL or not.

2.1 The Basic Typology

The contemporary history of conflict's classification began in 1949 with adoption of the four Geneva Conventions.¹¹⁸ Earlier treaties regulating conflicts had been silent as to the conditions under which they applied. They were merely assumed the existence of a "war".

Lassa Oppenheim, a renowned Jurist, explained in detail the classic definition of war in his 1906 treatise *International Law*: "War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases."¹¹⁹ The very important element in that definition was that war must be between States. Hence, the law of war would apply only to inter-State hostilities.¹²⁰

The 1907 Second Hague Peace Conference adopted Hague Convention III relative to the Opening of Hostilities in response to the said conflict. In that instrument, State parties agreed that "hostilities between themselves must not begin without previous and

¹¹⁸ Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC I–IV respectively].

¹¹⁹ Lassa Oppenheim, *International Law: A Treatise War and Neutrality* (London: Longmans, 1920), 52.

¹²⁰ Definition of Oppenheim suggested that the existence of a war was a question of fact. This approach was brought into matter by the undeclared war between Japan and Russia in 1905. Intra-State conflict was mostly a matter of domestic concern unless it rose to the level of aggressive behavior. See briefly, Hans-Peter Gasser, *International Humanitarian Law, an Introduction* (Geneva, Henry-Dunant Institute, 1993), 92, available at, <https://books.google.com.pk/books>, (last accessed: July 2, 2016).

explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war.”¹²¹ Sensitive to these realities, the international community took a different approach with the adoption of Geneva Conventions in 1949.¹²² The approach taken in those instruments developed into customary international law recognizes war in both the technical and material sense.

2.1.2 The Notion of Armed Conflict

The term “armed conflict” is not defined anywhere in the Geneva Conventions 1949 or its Additional Protocols.¹²³ In case of International Armed Conflicts, broader view is taken by Pictet’s commentary to the Geneva Convention 1949 provides that:¹²⁴ “Any difference arising between two states and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.”

¹²¹ The war between Russia and Japan which broke out in 1904 without a declaration of war caused a movement for the adoption of some written rules on the commencement of war. The Institute of International Law adopted a resolution to that end in 1906 and the Second Hague Conference of 1907 produced the present Convention. Although this Convention concerns rather the *jus ad bellum* than the *jus in bello*. Consequently, a failure to declare war or the non-recognition of a state of war by a party to the conflict would lead to prevent the application of treaties ruling the conduct of hostilities between states. This approach proved to be fail by later events. For details see, Dietrich Schindler and Jiri Toman, *The Laws of Armed Conflicts* (Boston: Martinus Nijhoff Publisher, 1988), 57-59, available at, www.google.com/books, (last accessed: July 3, 2016).

¹²² Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge: Cambridge University Press, 2010), 81, available at, <https://books.google.com.pk/books>, (last accessed: January 31, 2017).

¹²³ *Ibid.*, In order to avoid the political and legal strife that had occurred over the legal definition war, a police action, or any other form of hostile action the drafters of the convention intentionally remained it undefined.

¹²⁴ ‘Article 2’ in Jean S. Pictet, *the Geneva Conventions of 12 August 1949-I: Commentary* (Geneva: International Committee of Red Cross, 1952), 32, available at, <https://www.loc.gov/Law/pdf/>, (last accessed: July 13, 2016).

Whereas the International Committee of Red Cross (ICRC) embraces an expansive view of armed conflict, stating that in case of cross-border operations, the first shot is considered sufficient to trigger an International Armed Conflict:¹²⁵

By using the words “from the outset” the authors of the Convention wished to show that it became applicable as soon as the first act of violence were to show that it became committed, even if the armed struggle did not continue. Nor it is necessary for there to have been many victims. Mere frontier incidents may make the Convention applicable, for they may be the beginning of a more widespread conflict.

2.2 Categorization of Armed conflict under IHL

There are two types of Armed Conflicts in IHL namely:¹²⁶

- International Armed Conflicts (herein after IAC), opposing two or more States, and Non-International Armed Conflicts (herein after NIAC), between governmental forces and nongovernmental armed groups, or between such groups only. A distinction between non-international armed conflicts in the meaning of common Article 3 of the Geneva Conventions of 1949 and non-international

¹²⁵ Article 6 in Jean S. Pictet, *the Geneva Conventions of 12 August 1949-IV: Commentary* (Geneva: International Committee of Red Cross, 1958), 59, available at, <https://www.loc.gov/law/1949-IV.pdf>, (last accessed: July 13, 2016). See also, ICRC, how is the Term “Armed Conflict” Defined in International Humanitarian Law? 2, <http://www.icrc.org/eng/assets/files/opinion-paper-armed-conflict.pdf>, (last accessed: July 7, 2016).

¹²⁶ Knut Dörmann & Louis Maresca, “The International Committee of the Red Cross and its Contribution to the Development of International Humanitarian Law in Specialized Instruments”, *Chicago Journal of International Law* 5:1(2004), 217-232.

armed conflicts falling within the definition provided in Article. 1 of Additional Protocol II is also established by IHL.¹²⁷

The Geneva Conventions 1949 also recognize two types of armed conflicts- International and Non-international in its Articles 2 and 3, which is “Common” to all four conventions. Later on, two Protocols, additional to the Geneva Conventions 1949 were adopted. Additional Protocol I (herein after- AP I) is related to IAC by reference to Article 2 of the 1949 Conventions.¹²⁸ And the Additional Protocol II (herein after-APII) applies to NIAC. Unlike, Common Article 3 it sets a higher threshold of applicability.¹²⁹

¹²⁷ Ibid.

¹²⁸ The International Committee of the Red Cross (ICRC) held a Diplomatic Conference between 1973 and 7 to “update” international humanitarian law primarily due to post 1949 conflicts. Many States, most particularly the United States, refused to become party to the instrument, in part due to this latter provision. Deiter Fleck ed., *The Handbook of Humanitarian Law in Armed Conflicts* (UK: Oxford University Press, 2013), 43, available at, <https://books.google.com.pk/books>, (last accessed: July 16, 2016).

¹²⁹ The provision is different from Common Article 3 in its requirement that rebellious or other armed forces control territory and its limitation to conflicts involving a State, thereby excluding non-international armed conflicts between organized armed groups. Considering generally, this collection of provisions holds four categories of conflict: 1) International armed conflict between States; 2) International armed conflict involving national liberation movements; 3) Non-international armed conflict between a State and an organized armed group or between organized armed groups; 4) Non-international armed conflict at the Additional Protocol II level. The second and fourth categories are relevant only to application of Additional Protocols I and II respectively for Parties thereto. The first and third are acknowledged as customary categories of conflict. AP II is applicable to all armed conflicts which are not covered by Article 1 of [AP I] and 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. Article 1 specifically excludes “situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts” from the ambit of non-international armed conflict. This exclusion has been broadly accepted as reflective of customary international law in all non-international armed conflicts, a fact evidenced by its adoption in the Statute of the International Criminal Court. For details see, Jenny Döge, “Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime”, *Archiv des Völkerrechts*, 48:4(2010), 486-501, available at, <http://www.jstor.org/stable/25782>, (last accessed: July 17, 2016).

2.2.1 International Armed Conflict

International Armed Conflict defined in the Geneva Conventions is essentially similar to traditional legal concept of 'war' that is an armed conflict between two or more states. Article 2, common to the Four Geneva Conventions 1949, provides that:

... the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.

According to this provision, a conflict is IAC when one or more States have recourse to armed force against another State, regardless of the reasons or the intensity of this confrontation. Even in the absence of open hostilities relevant rules of IHL may be applied. Moreover, no formal declaration of war or recognition of the situation is required. The application of International Humanitarian Law to IAC depends on factual conditions like what actually happens on the ground. For instance, even though one of the belligerents does not recognize the government of the adverse party, the conflict between them be called an IAC.¹³⁰

According to the Commentary of the Geneva Conventions of 1949 "any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the

¹³⁰ "It is irrelevant to the validity of international humanitarian law whether the States and Governments involved in the conflict recognize each other as States". For details see, Fleck, *The Handbook of Humanitarian Law in Armed Conflicts*, 45.

existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place”.¹³¹

Jurisprudence: In *Tadic* case the International Criminal Tribunal for the former Yugoslavia (ICTY) proposed a general definition of international armed conflict. The Tribunal stated that “an armed conflict exists whenever there is a resort to armed force between States”.¹³² Since then this definition has been adopted by other international bodies.

According to one of the international expert, “the existence of an armed conflict within the meaning of Article 2 common to the Geneva Conventions can always be assumed when parts of the armed forces of two States clash with each other. [...] Any kind of use of arms between two States brings the Conventions into effect”.¹³³

Therefore, a conflict is IAC, if it qualifies two basic factual criteria—a conflict between States and hostilities that amount to “armed conflict”.

¹³¹Pictet, Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Whereas if peoples fight against colonial domination or alien occupation and against racist regimes exercising their right of self-determination, as preserved in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations then it could also be concluded as Armed conflict. See, Additional Protocol I, art. 1, para. 4: “armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations”.

¹³² ICTY, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-I-A, 2 October 1995, para. 70, available at, http://www.icty.org/case_tadic/1, (last accessed: July 17, 2016).

¹³³ Gasser, *International Humanitarian Law, an Introduction*, 93.

2.2.2 Non international Armed Conflict

Common Article 3 to the Geneva Conventions of 1949; and Article 1 of Additional Protocol II must be examined to know about NIAC under IHL.¹³⁴

- **Common Article 3 to the Geneva Conventions 1949;** applies to “armed conflicts not of an international character occurring in the territory of one of the High Contracting Parties”.¹³⁵ In such type of armed conflict one or more non-governmental armed groups are involved. Hostilities may occur between governmental armed forces and non-governmental armed groups or between such groups only, depends upon situation. In order to distinguish NIAC from less serious forms of violence, such as internal disturbances and tensions, riots or acts of banditry, the situation must reach a certain threshold of hostility. Usually, two criteria are used for qualification of hostility as NIAC: First, the hostilities must reach a minimum level of intensity. Suppose, this may be the case, when the hostilities are of a collective character or when the government has to use military force instead of police force against the rebels.¹³⁶ Second, non-governmental groups involved in the conflict must possess organized armed forces.
- **Article 1 AP II;** gives a more restrictive definition of NIAC. It applies to armed conflicts “which take place in the territory of a High Contracting Party between

¹³⁴ Ibid.

¹³⁵ For details see, “Conflicts Not of an International Character”, available at, <https://ihl-databases.icrc.org>, (last accessed: July 17, 2016). It has been generally accepted that Article 1(2) of APII contains lower threshold which excludes internal disturbances and tensions from the definition of NIAC. It has been generally accepted that Article 1(2) of APII contains lower threshold which excludes internal disturbances and tensions from the definition of NIAC.

¹³⁶ For a detailed analysis of this criteria, see ICTY, *The Prosecutor v. Fatmir Limaj*, Judgment, IT-03-66-T, 30 November 2005, para. 135-170. It means that these forces have to be under a certain command structure and have the capability to confront military operations. Also see, ICTY, *The Prosecutor v. Fatmir Limaj*, Judgment, IT-03-66-T, 30 November 2005, para. 94-134, available at, <http://www.icty.org/case/limaj>, (last accessed: July 17, 2016).

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".¹³⁷

The Statute of the International Criminal Court (ICC), in its article 8, para. 2 (f), confirms the existence of a definition of a non-international armed conflict not fulfilling the criteria of Protocol II.¹³⁸

Comments of several recognized authors also very clearly suggest that what should be considered as NIAC Dietrich Schindler, Professor of International Law recommends a detailed definition:

"The hostilities have to be conducted by force of arms and exhibit such intensity that, as a rule, the government is compelled to employ its armed forces against the insurgents instead of mere police forces. Secondly, as to the insurgents, the hostilities are meant to be of a collective character, [i.e] they have to be carried out not only by single groups. In addition, the insurgents have to exhibit a minimum amount of organizations. Their armed forces should be under a

¹³⁷ Additional Protocol II, art. 1, para. 1. In this context, it must be reminded that Additional Protocol II "develops and supplements" common Article 3 "without modifying its existing conditions of application". This means that this restrictive definition is relevant for the application of Protocol II only, but does not extend to the law of NIAC in general. Additional Protocol II, art. 1, para. 1. This definition is narrower as compared to definition of NIAC given in common Article 3 in two ways. Firstly, it specifies a requirement of territorial control, by giving that non-governmental parties must exercise such territorial control "as to enable them to carry out sustained and concerted military operations and to implement this Protocol". Secondly, armed conflicts between State armed forces and dissident armed forces or other organized armed groups are expressly regulated by AP II. Unlike common Article 3, the Protocol does not apply to armed conflicts occurring only between non-State armed groups.

¹³⁸ Statute of the ICC, art. 8 para. 2 (f): "It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups".

responsible command and be capable of meeting minimal humanitarian requirements".¹³⁹

Jurisprudence: Case law put forward important elements for a definition of an armed conflict, primarily referring to NIAC in common Article 3 Geneva Conventions 1949. These are not defined expressively. Hence, some light is thrown on the definition of NIAC by ICTY via its Judgments and decisions. The ICTY confirms the existence of a NIAC "whenever there is [...] protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".¹⁴⁰

2.3 Qualification of Cyber warfare as International Armed Conflict

Existence of an Armed Conflict is the first and foremost prerequisite to trigger an application of IHL.¹⁴¹ This fact would lead to very basic question whether a cyber-attack or cyber warfare can initiate an Armed conflict which need to be answered. For this purpose, an analysis will be made, based on the 1949 Geneva Convention and 1977 Additional Protocol II (APII) as well as on the *Tadić* case ICTY which held that "an Armed conflict exists whenever there is a resort to armed force between states or protracted armed violence between governmental authorities and organized armed groups

¹³⁹Dietrich Schindler, "The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols", *Recueil des Cours de l'Académie de droit International* 163:2(1979), 125-162.

¹⁴⁰ ICTY, *The Prosecutor v. Dusko Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para.70. The ICTY thus states the definition of NIAC almost same as that of common Article 3 of Geneva Conventions 1949 which incorporate situations where "several factions [confront] each other without involvement of the government's armed forces". Since then, each judgment of the ICTY has taken this definition as a starting point.

¹⁴¹Schmitt, "Cyber Operations and the Jus in Bello: Key Issue", 87-107. Also see, International Criminal Tribunal for the Former Yugoslavia, *Prosecutor v. Tadić*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-A, A.Ch., 2 October 1995, para. 67, available at, <http://www.icty.org/case/tadic-4>, (last accessed: July 21, 2016).

or between such groups within a state".¹⁴² The criteria to be set out reflect the conditions to be met for the existence of an Armed conflict. Different thresholds have been established by both customary and treaty law for the use of IHL in both types of conflicts.¹⁴³

2.3.1 Threshold of Harm for Armed Conflict

Applying *de minimis* level of intervention, it would appear that computer network attacks could welcome within the ambit of armed conflicts. However, this view is not universally held and the statement regarding the length and intensity of the conflict is not necessarily borne out by the state practice.¹⁴⁴ Further it is by no means clear that most states would regard an isolated incident or exchange of fire as an armed conflict, bringing into operation the full panoply of the Geneva conventions.¹⁴⁵ Moreover, at the same time there are examples of relatively minor incidents where a state has claimed protection of the laws of armed conflict and there have been a number of border clashes and naval incidents which have not been treated as armed conflicts.¹⁴⁶

¹⁴² Ibid., para. 70.

¹⁴³ Janne K. Keßler, "Scope of Application of Humanitarian Law", in Dieter Fleck (ed.), *The Hand Book of Humanitarian Law in Armed Conflicts* (Oxford: Oxford University Press, 2008), 45.

¹⁴⁴ This is also supported by the series of decisions of the Ethiopia/Eritrea Claims Commission. Though controversial and criticized for several reasons, the decisions of the Commission in declaring 12 May 1998 as the start of armed conflict that was the subject of their awards indicates their unwillingness to apply the Laws of Armed Conflict to the border skirmishes that took place in the preceding weeks. For details see, Partial Award, *Jus Ad Bellum—Ethiopia's Claims 1-8*, Decision of 19 December 2005, available at http://legal.un.org/riga/cases/vol_XXVI/457-469.pdf, (last accessed: July 21, 2016).

¹⁴⁵ Ibid.

¹⁴⁶ For instance, during the Dogger Bank Incident of 1904, the Russian navy's North Sea fleet opened fire on the British fishing trawler, believing them to be Japanese warships. The case was closed by payment of compensation to the British government for the lives of the two men lost, the sinking of one trawler and the injury and damage to the other trawlers and crew. Findings of the International Commission of Inquiry organized under Article 9 of the Convention for the Pacific Settlement of International Disputes, of July 29, 1899 (the Dogger Bank Incident). Also see, Keßler, "Scope of Application of Humanitarian Law", 48.

On 8 June 1967, Israeli fighter jets and torpedo boats attacked the USS Liberty¹⁴⁷ in the eastern Mediterranean, killing 34 crew members and wounding 171 more. The officially accepted explanation for the attack has been that it was a tragic mistake and the US accepted apology and compensation for the losses. Contrary to this, when a US Navy pilot was shot down and captured by Syrian forces over Lebanon in 1983, the United States maintained that this incident amounted to an armed conflict and the pilot was given prisoner of war status.¹⁴⁸

A closer look of these incidents reveals that classification of events as an armed conflict appears to be based on the perceived intentions of the other party. Hence, Nils Melzer comments “in the absence of a formal declaration of war, an international armed conflict requires a minimal transgression, which expresses the belligerent intent of the acting state against another.”¹⁴⁹

On the other hand, Non-international armed conflicts are generally accepted to be met a requirement of a certain level of intensity in order to distinguish them from internal disturbances and tensions. Albeit the principle set out in the Article 1 paragraph 2 of the Additional Protocol II, states that the laws of armed conflict do not apply to situations of “internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature. This principle generally applied to all non-international

¹⁴⁷ USS Liberty stands for United States Navy technical research ship, for details see, Israel attacks USS Liberty, available at, <http://www.history.com/tjis-day-in-history>, (last accessed: April 6, 2017).

¹⁴⁸ Several crew members and intelligence official dispute the findings of the official inquiry, stating that the attacks were deliberate. See generally Walter L. Jacobsen, “A Judicial Examination of the Israeli Attack on the USS Liberty”, *Naval Law Review* 36(1986), 69, available at, <http://heinonline.org/journals>, (last accessed: July 14, 2016).

¹⁴⁹ Nils Melzer, *Targeted killing in International Law* (UK: Oxford University Press, 2008), 250, available at, www.google.com/books, (last accessed: July 13, 2016).

armed conflict.¹⁵⁰ In 1995 the appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia in the *Tadic* case considered the term armed conflict by holding that¹⁵¹ “an armed conflict exists wherever there is resort to armed forces between states or protracted armed violence between government authorities and organized armed groups or between such groups with a state.”

The appeals chamber thus took a more inclusive approach to the question, asserting that the threshold for the application of common article 3 is actually relatively low, although it does not apply as widely as Pictet’s commentary would suggest.¹⁵²

The problem lies in application of threshold of harm on cyber-attacks to be called as IAC or NIAC because the consequences of such attacks are non-lethal and non-physical which is contrary to the meaning of attack given in article 49 of AP I (this is explained later on in detail). The researcher opines that there should be some reasonable threshold of harm attached to IAC in case of cyber warfare due to non-lethal and non-physical consequences of cyber-attacks.

2.3.2 The Requirement of Armed Force

Pictet’s definition of armed conflict refers only to hostilities between states. To consider conflicts as IAC and NIAC force or armed violence is the requirement for it according to

¹⁵⁰ Dieter Fleck, “The Law of Non-International Armed Conflicts” in D. Fleck (ed.), *The Handbook of International Humanitarian Law*, 33.

¹⁵¹Prosecutor vs. Dusko Tadic (interlocutory appeal on jurisdiction) (1995) Case No. IT-94-1-AR, International Criminal Tribunal for Former Yugoslavia, Appeal Chamber, para. 70, available at, <http://www.icty.org/x/cases/tadic/ajug/en/tad-aj990715e.pdf>, (last accessed: July 14, 2016).

¹⁵² Lindsey Moir, *The Law of Internal Armed Conflict* (UK: Cambridge University Press,2004), 43, available at, <https://books.google.com.pk/books?id=3ssL3oB>, (last accessed: July 20, 2016).

Tadic case.¹⁵³ Similarly, tribunal also separates the level of violence required for IAC and NIAC by requiring a level of protraction of the violence in conflicts.¹⁵⁴

The notion of 'armed force' is not defined in International Law. Generally, the term armed force is construed broadly and it includes indirect form of support for the application of force.¹⁵⁵ Thus cyber-attack will result in a use of force, if it directly or indirectly, results in injury or death, or deconstruction of physical property.¹⁵⁶ Determination of cyber warfare as a use of armed force will be a factual determination, likely to be established with the passage of time by state practice. However, further research in this field shows that a certain level of physical damage will also be required.

2.3.3 Intervention of the Armed Forces

Pictet's commentary on Common Article 2 of the Geneva Conventions 1949 requires the intervention of the armed forces of a state as a precondition for IAC.¹⁵⁷ This approach raises two problems for contemporary conflicts. First, in modern armed conflict the armed forces of a state may not only actors engaged in its armed conflicts due to privatization of military and outsourcing of the key defense functions by civilians.¹⁵⁸ Second, now-a-days military forces are engaged in other tasks besides armed conflict

¹⁵³ Ibid., it should be noted that there was no question in the *Tadic* case whether there had been such force or violence used against the people of the former Yugoslavia, the case addressed the question of the international or internal nature of the armed conflict that took place in Balakans.

¹⁵⁴ Ibid, this is in keeping with the requirement that the laws of armed conflicts are not to apply to internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of similar nature.

¹⁵⁵ Fleck (ed.), *The Handbook of International Humanitarian Law*, 37.

¹⁵⁶ Schmitt, "Cyber Operations and the Jus in Bello: Key Issue", 87-107.

¹⁵⁷ See Article I(2) Additional Protocol II, available at, <https://treaties.un.org/doc/Publication/PfI/> (last accessed: July 14, 2016).

¹⁵⁸ Dinniss, *Cyber warfare and the Laws of War*, 123.

against other states or groups - for instance, for Aerial Surveillance and investigation.¹⁵⁹ Michael Schmitt, Professor of International Law, opined that a dispute resulting in the involvement of armed forces cannot be considered only criterion for initiation of an armed conflict.¹⁶⁰ Moreover, involvement of the armed forces in a dispute by state signifies that it has reached a sufficient level to be termed as an armed conflict.¹⁶¹

In case of internal armed conflict involvement of the armed forces of a state are not required which makes them more difficult. Common Article 3(CA3) of Geneva Conventions 1949 is silent about the extent of the parties involved in internal armed conflict. While, AP II to Geneva Convention 1949 regulates internal armed conflicts between the armed forces of a state and dissident armed forces or organized armed groups.¹⁶² Thus conflicts between other government agencies and such groups cannot be termed as internal armed conflicts.¹⁶³ In the case of *Akayesu*, the trial chamber entails 'a

¹⁵⁹ Ibid., 124.

¹⁶⁰ Micheal N. Schmitt, "Wired Warfare: Computer Network Attack and the Jus in Bello", *International Review of the Red Cross* 84:846(2002), 369-381, available at, <https://www.icrc.org/pdf>, (last accessed: July 14, 2016).

¹⁶¹ Ibid., 370.

¹⁶² Article 1 Additional Protocol II Geneva Convention 1949 is about material field of application. It states that This Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 2 and 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. 2. This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts. Available at, <https://treaties.un.org/doc/Publication/UN/LS/Vol5/volume-1125-I-17513.pdf>, (last accessed: July 14, 2016).

¹⁶³ An explanatory note inserted into the Report Committee I describes 'armed forces' as: All the armed forces...According to the views expressed by a number of delegations, the expression would not include other government agencies the members of which may be armed; example of such agencies are the police, customs and other similar organizations. This fact may leave grey area in the protocol. For discussion of armed forces in international conflicts. The definition of internal armed conflict given by Appeal Chamber in *Tadic*, reflects the extent of the parties covered by Common Article 3 and applies to prolonged armed violence by any government authority. In contrast to Common Article 3 and the definition covered *Tadic*, Additional Protocol II does not apply to conflicts between armed groups within the territory of a high contracting party. see; Moir, *The Law of Internal Armed Conflict*, 45.

degree of organization within the armed group... such as to enable the armed group to plan and carry out concerted military operations, and to impose discipline in the name of a de facto authority'.¹⁶⁴

Studying Estonia, Georgia and other low level computer network attacks such as those launched by supporters of the website helpisraelwin.com and its variants, the highly dispersed nature of the participants in those attacks shows that a fairly minimal level of organization is required to launch sustained and debilitating attacks against a country's infrastructure.¹⁶⁵ According to Louise Doswald-Beck, Professor of International Law at the Graduate Institute of International and Development Studies, "any computer network attack launched by well-organized group and had done enormous damage is likely to be considered as criminal behavior. Therefore, it should be dealt by agencies rather than military".¹⁶⁶ However, since the recognition of armed attacks by non-state actors this view can no longer be maintained.¹⁶⁷

As discussed, IAC must be both 'armed' and 'international'. Here the problem is that cyber warfare is non-kinetic and do not employ what would in common usage be considered as 'weapons'.¹⁶⁸ Hence, a conflict consisting of only cyber operations would not be considered 'armed'.¹⁶⁹ It is argued that State involved in an exchange of cyber-attacks at this level would be very likely to characterize the situation as IAC, much as

¹⁶⁴ Prosecutor vs Jean- Akayesu (1998) Case No. ICTR-96-4-T, International Criminal Tribunal for Rwanda, para. 626. Available at, https://www.ictc.org/casebook/doc/case-study_ictt-akayesu-case_study.htm, (last accessed: July 14, 2016).

¹⁶⁵ Knut Dormann, Computer Network Attack and International Humanitarian Law, *International Committee of the Red Cross*, 1-12, available at, http://www.ictc.org/Web_Eng_site/eng09.nsf/html/5P2AFL, (last accessed: July 15, 2016).

¹⁶⁶ Duncan B. Hollis, "Why States Need an International Law for Information Operations", *Lewis and Clark Law Review* 1023:11(2007), 1-20, <https://www.scribd.com/document/182669513/Why-States-Need-an-International-Law-for-Information-Operations-pdf>, (last accessed: July 14, 2016).

¹⁶⁷ Dinniss, *Cyber warfare and the Laws of War*, 125.

¹⁶⁸ Jeffrey Carr, *Inside Cyber warfare*(USA: O'Reilly Media, 2010), 47.

¹⁶⁹ *Ibid.*, 48.

another State's non-kinetic biological attack.¹⁷⁰ The official ICRC Commentary to Article 2 provides that

any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.¹⁷¹

The ICRC Commentary to AP I is in accord.¹⁷² Similarly the ICTY has defined armed conflict as the 'resort to armed force between States' without recognizing any threshold for the duration or intensity of hostilities.¹⁷³ These provisions imply the concept of armed as forceful acts at whatever level.¹⁷⁴ For instance, if a State was behind 'Stuxnet' cyber-attack in 2010 against Supervisory Control and Data Acquisition (SCADA) systems upon

¹⁷⁰ Michael N. Schmit, "Classification of Cyber Conflicts", *International Law Studies*, 89(2013), 240.

¹⁷¹ See generally Jean S. Pictet, *Commentary to Geneva Convention III relative to the Treatment of Prisoners of War* (Geneva: International Committee of the Red Cross, 1960), 23, available at, https://www.loc.gov/law/pdf/GC_1949-III.pdf, (last accessed: July 15, 2016).

¹⁷² According to Commentary to AP I: Humanitarian Law . . . covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its intensity, play a role: the law must be applied to the fullest extent required by the situation of the persons and the objects protected by it. Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., *Commentary On the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: International Committee of Red Cross, 1987), 62, available at, http://www.loc.gov/pdf/Commentary_GC_Protocols.pdf, (last accessed: July 15, 2016).

¹⁷³ Schmitt, "Classification of Cyber Conflict", 240.

¹⁷⁴ *Ibid.* It should be noted that an armed conflict can exist even in the absence of uses of force. For instance, Common Article 2 of the four 1949 Geneva Conventions extends to "all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance." Consequently, any cyber operation that amounts to an 'attack' in IHL terms would qualify as armed. Though cyber operations are not violent in themselves, they capably generate violent consequences. To the extent that they result in injury or death of persons or damage or destruction of property, due to this fact they are attacks satisfying the armed criterion of armed conflict. Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", 1-12, available at, <https://www.icrc.org/pdf>, (last accessed: July 20, 2016).

which the power centrifuges at an Iranian nuclear power plant depended, it would meet this threshold because physical damage resulted.¹⁷⁵

However, whether a cyber-attack that does not cause physical injury or damage initiates an armed conflict or not. The ICRC opine, in this regard, that a cyber-operation that 'disables' an object is also an attack even when it does not cause physical damage.¹⁷⁶ Since the operation is an attack, it is also armed in terms of qualification for armed conflict. A *de minimis* standard should be attached.¹⁷⁷

If the lower threshold of harm leads to IAC and includes cyber-attacks resulting in manipulation of data or loss of functionality computer systems, then psychological operations directed against civilians can also initiate armed conflict. Harm in the context of armed must be a violent act instead of being just an act of annoyance.

Also consider a situation in which a State takes control of critical infrastructure in another State, carry out DOS attacks against vital societal services, or begins altering data in a manner that severely disrupts another State's economy.¹⁷⁸ The list does not end here beyond these cases; it is unclear that where the state practices will lead.

¹⁷⁵ The question remains as to whether a State was behind the operation. For details see, John C. Richardson, "Stuxnet as Cyherwarfare: Applying the Law of War to the Virtual Battlefield", *Journal of Computer & Information Law* 29:1(2011), 1-29, available at, <http://papers.ssrn.com/papers189/>, (last accessed: July 16, 2016).

¹⁷⁶ This is a reasonable extension of the notion of damage, at least to the extent repair (as distinct from merely reloading software) of the cyber infrastructure concerned is necessitated. For details see, Gloria Gaggioli, "The Use of Force in Armed Conflicts Interplay Between the Conduct of Hostilities and Law Enforcement Paradigms", available at, <https://www.icrc.org/pub/pdf/>, (last accessed: July 16, 2016).

¹⁷⁷ Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", 303-333

¹⁷⁸ As noted by the ICRC, "[i]t would appear that the answer to these questions will probably be determined in a definite manner only through future state practice" Michael N. Schmitt and Watts S. Sean, "The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare", *Texas International Law Journal* 50(2015) 189-231, available at, <http://www.tilj.org/journal.pdf/>, (last accessed: July 16, 2016).

2.3.4 Requirement of Being International

In addition to being armed, cyber-attacks must be of an 'international' nature to qualify as IAC. The term 'international' indicates actions conducted by, or attributable to a State. By the plain text of the provisions Cited above, those conducted by a State's armed forces qualify as IAC. And cyber-attacks conducted by other organs of a State, such as intelligence or law enforcement agencies, also qualify, though not mentioned in those provisions.¹⁷⁹ In *Tadic* case ICTY states that 'private individuals acting within the framework of, or in connection with, armed forces, or in collusion with State authorities may be regarded as de facto State organs'.¹⁸⁰ Any cyber-attacks launched by them would be treated as if launched by de jure State organs. Cyber-attacks carried out by a person or entity that, although not an organ of the State, 'empowered by the law of that State to exercise elements of the governmental authority.... provided the person or entity is acting in that capacity in the particular instance' would be treated in the same way.¹⁸¹

More problematic to deal with are activities engaged in by individuals or groups that are neither organs of a State nor authorized to act on its behalf. It appears clear that

¹⁷⁹ Herbert Lin, "Cyber conflict and international humanitarian law", *International review of the Red Cross* 94:886(2012), 515-531, available at, http://www.icd.icrc.org/library/docs/DOC_irrc-886-lin.pdf, (last accessed: July 16, 2016). See also, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Commission, 53d Sess., GAOR 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001), reprinted in [2001] 2 Yearbook of The International Law Commission 32, U.N. Doc. A/Cn.4/Ser. A/2001/Add.1 (Part 2). Article 4(2) of the Articles of State Responsibility provides that an "organ includes any person or entity which has that status in accordance with the internal law of the State."

¹⁸⁰ Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, 144 (International Criminal Tribunal for the former Yugoslavia July 15, 1999), <http://www.icty.org/x/cases/tadic/acjag/en/tad-aj990715e.pdf>, (last accessed: July 17, 2016).

¹⁸¹ Article 5 of State Responsibility states that The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance. For details see, International Law Commission, Articles on State Responsibility, available at, <https://www.icrc.org/casebook-doc/case-study-ijc-state-responsibility-case-study.htm>, (last accessed: July 17, 2016). An example would be a private corporation that a State authorizes by law to conduct cyber operations on its behalf, so long as the operations in question are of the sort for which said authorization was granted. Lin, "Cyber conflict and international humanitarian law", 515-531.

cyber-attacks by individuals or groups acting on its own are generally not attributable to a State for the purpose of finding an IAC. The classic example is the ‘hacktivist’ cyber campaign against Estonia in 2007 and moreover, they were no ‘armed’.¹⁸²

Merely providing software or hardware with which attacks are conducted does not suffice to attribute a group’s actions to the State for the purpose of finding IAC (although such assistance may violate certain norms of international law).¹⁸³

The requisite degree of control over the actions of individuals who conduct cyber-attacks without being members of an organized armed group is much higher. In such cases, the State must issue ‘specific instructions or directives aimed at the commission of specific acts’ before attribution of the acts to the State for the purpose of classifying the conflict as international occurs.¹⁸⁴ Absent such instructions, the attacks cannot be attributed to the State for that purpose. Neither would the conflict be non-international since, the individuals do not comprise an organized armed group.¹⁸⁵

¹⁸²However, if a State endorses and encourages the perpetuation of the cyber operations, the individuals or groups involved will be deemed ‘de facto organs’ of the State, such that the activity meets the international criterion. This principle was enunciated (albeit, in the State responsibility context) by the International Court of Justice in the Hostages case and cited with approval by the International Criminal Tribunal for Yugoslavia (ICTY) in *Tadić* when dealing with attribution for the purposes of conflict classification. Schmitt, “Classification of Cyber Conflicts”, 242. See also United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3,74. *Tadić* Appeals Chamber Judgment, supra note 30, 133–37. A scenario in which some relationship exists between a State and the individuals or group conducting the cyber-attacks is more likely. The ICTY addressed this situation head on in *Tadić* when assessing whether the conflict in Bosnia–Herzegovina was international by virtue of the relationship between the Bosnia Serb armed groups and the Serb-dominated Federal Republic of Yugoslavia. In an often-overlooked distinction, the Tribunal took different approaches to the actions of organized armed groups and individuals. For details see, Michael N. Schmitt, “The Law of Cyber Targeting”, *Naval War College Review*, 68:2(2015), 10-29, available at, <https://www.usmc.edu/The-Law-of-Cyber-Targeting>, (last accessed: July 18, 2016).

¹⁸³ Kristen E. Eichensehr, “Cyberwar & International Law Step Zero”, *Texas International Law Journal* 50:2(2015), 357-380, available at, <http://www.tilj.org/content/journal-50-FINAL.pdf>, (last accessed: July 18, 2016).

¹⁸⁴ *Tadić* Appeals Chamber Judgment, supra note 30, 132, available at <http://www.icty.org/pdf>, (last accessed: July 18, 2016).

¹⁸⁵ Eichensehr, “Cyberwar & International Law Step Zero”, 357-380.

Last but not the least, it is sometimes questioned whether attribution to a State is required for qualification of conflicts as IAC. In the Targeted Killing case, the Israeli Supreme Court argued that attribution is not necessary so long as the group in question operates transnationally, that is, the conflict ‘crosses the borders of the state’.¹⁸⁶ In cyber warfare context, this situation is highly probable, for organized armed groups might well launch cyber-attacks from relative safety abroad.¹⁸⁷

2.4 Non-international Armed Cyber Conflict

As it has been already mentioned, two essential conditions apply to all non-international armed conflicts—participation by an organized armed group and a particular level of intensity which may prove problematic for cyber warfare.¹⁸⁸

2.4.1 Requirement of Organized Armed Group

For NIAC organized armed groups must be both ‘organized’ and ‘armed’. Common Article 3 refers to ‘parties to a conflict’, a reference to the requirement of organization.¹⁸⁹

Organization may help them to act in a coordinated manner, probably enhancing the capability to engage in violence. Simply, the criterion of organization suggests that

¹⁸⁶ Catherine M. Grosso, “International Law in the Domestic Arena: The Case of Torture in Israel”, *the University of Iowa Law Review* (2001), 305, available at, <http://digitalcommons.law.uiowa.edu/>, (last accessed: July 18, 2016).

¹⁸⁷ Schmitt, “Classification of Cyber Conflicts”, 242. The US Supreme Court took a contrary approach in *Hamdan*, where it found that the conflict with the Al-Qaeda terrorist organization was ‘not of an international character’ because it was not between States. See briefly *Hamdan V. Rumsfeld* (2006), available at, <https://www.supremecourt.gov/opinions/05pdf/05-184.pdf>, (last accessed: July 18, 2016).

¹⁸⁸ Schmitt, “Classification of Cyber Conflict”, 244.

¹⁸⁹ *Ibid.*, The same is reinstated by ICTY as ‘some degree of organization by the parties that required for establishing the responsibility of superiors for the acts of their subordinates within the organization, as no determination of individual criminal responsibility is intended under this provision of the Statute’. In military operations, such coordination typically involves mission planning, sharing intelligence and exercising command and control.

the actions are best understood as those of a group and not its individual members. And this organizational requirement is important to identify enemy treated as the other party to the conflict.¹⁹⁰

It means that cyber-attacks against a State conducted individually cannot meet the organized criterion. Although a number of hacktivists involved in the cyber operations against Estonia, they lacked the requisite degree of organization and therefore the operations did not amount to NIAC.¹⁹¹ Similarly, consider a case in which a website containing malware and listing potential cyber targets is accessed by large numbers of individuals who are unaffiliated with the creator of the website would not amount to organization criterion. Moreover, collective cyber-attacks occurring in parallel are not considered “organized.”¹⁹²

It is difficult to classify a group that organizes entirely on-line to conduct cyber-attack. Because the members of virtual organizations may never meet nor even know each other’s actual identity. Until and unless such groups, highly organized and act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership.¹⁹³ Suppose, one member of the group might be given task to identify vulnerabilities in target systems, a second might be asked to develop a malware

¹⁹⁰Whether a group is organized is always a fact and context-specific determination. In *Limaj* case, the ICTY looked to such factors as, inter alia, the existence of a formal command structure, the creation of unit zones of operation, the issuance of orders, the establishment of a headquarters and the promulgation of disciplinary orders to find that the Kosovo Liberation Army qualified as an organized armed group in its conflict with the Federal Republic of Yugoslavia.

¹⁹¹ Keiichiro Okimoto, “The Relationship Between a State and an Organised Armed Group and its Impact on the Classification of Armed Conflict”, *Amsterdam Law Forum* 5:3(2013),33-51, <http://ojsl/article>, (last accessed: July 19, 2016).

¹⁹² Ibid.

¹⁹³ Swanson, “The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian Georgian Cyber Conflict”, 303-333.

to exploit those vulnerabilities, a third might be instructed to conduct the operations and a fourth might be in charge of cyber defenses against counter-attacks.

2.4.2 Requirement of Responsible Command

AP II to Geneva Conventions 1949 imposes a requirement that a group be “under responsible command” for a conflict to be called NIAC.¹⁹⁴ This requirement should be construed flexibly.¹⁹⁵ In a virtually organized group, the requirement of an ability to carry out protracted military operations could be met to the extent that cyber operations are linked with military operations. However, imposing this discipline in cyber warfare would be difficult due to the lack of physical control over its members.

Such organization cannot be seen in a virtually organized group as there is no physical connection among them. It must be kept in my mind that since this treaty law requirement is given in AP II, making it applicable to conflicts in which that instrument applies.¹⁹⁶ On the other hand, Common Article 3 contains no such condition. This leads

¹⁹⁴ Additional Protocol II, 1977 art. 1(1) states that this Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and 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. For details see, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, available at, <https://ihl-databases.icrc.org/ihldocument?id=3408>, (last accessed: July 19, 2016).

¹⁹⁵ As noted by the ICRC Commentary to the article, the term ‘implies some degree of organization of the insurgent armed group or dissident armed forces, but this does not necessarily mean that there is a hierarchical system of military organization similar to that of regular armed forces. It means an organization capable, on the one hand, of planning and carrying out sustained and concerted military operations, and on the other, of imposing discipline in the name of a de facto authority’. See briefly, Additional Protocol II Commentary, 4663, available at, <https://ihl-databases.icrc.org/ihldocument?id=3408>, (last accessed: July 19, 2016).

¹⁹⁶ Swanson, “The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian Georgian Cyber Conflict”, 303-313.

to a question whether an analogous customary law norm applies to NIAC other than AP II.¹⁹⁷

Besides the criterion of organization, the group in question must be armed. The meaning of armed in the context of NIAC is the same as that of IAC. Generally, it means the manner in which 'attacks' are carried out.¹⁹⁸ Since NIAC is based on requirement of organized group, therefore, question of attribution of an individual member's conduct to the whole group arises, because it is the group that needs to be armed and must have a purpose of carrying out armed activities.¹⁹⁹ The criterion of armed is not met if individual members of an organized group carry out cyber-attacks individually, not on behalf of the group.²⁰⁰

¹⁹⁷ In this regard, the Commentary to Article 3 notes that the Diplomatic Conference that drafted the 1949 Geneva Conventions considered setting express preconditions for such conflicts. Although the proposal was rejected, the Commentary asserts that they 'constitute convenient criteria'. The first condition was that the 'Party in revolt against the de jure Government possesses an organized military force, an authority responsible for its acts, acting within a determinate territory and having the means of respecting and ensuring respect for the Convention'. It would appear reasonable, therefore, to extend the Additional Protocol II requirements regarding responsible command (*vis-a-vis* enforcing discipline) and an ability to implement international humanitarian law to all non-international armed conflicts. The ICTY adopted this approach in *Boskoski* and it is consistent with the principle of command responsibility in non-international armed conflicts. If valid, the extension to all non-international armed conflicts would preclude virtually organized groups from qualifying as organized armed groups for the purpose of classifying a conflict as non-international connection between the members. See, Commentary On Geneva Convention I for The Amelioration of the Condition of the Wounded and Sick in The Armed Forces in The Field 49 (Jean Pictet ed., 1952). Also see briefly, *Prosecutor v. Boskoski*, Case No. IT-04-82-T, Judgment, 205 (ICTY July 10, 2008).

¹⁹⁸ Okimoto, "The Relationship Between a State and an Organized Armed Group and Its Impact on the Classification of Armed Conflict", 33-51.

¹⁹⁹ *Ibid.*

²⁰⁰ Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian Georgian Cyber Conflict", 303-313.

2.4.3 Particular Level of Intensity

NIAC not only requires a certain degree of intensity but the hostilities must also be protracted.²⁰¹ Several factors like the gravity of the attacks, the collective character of the hostilities, the need to increase forces to deal with the situation, the time over which the hostilities have taken place, and whether the United Nations Security Council has addressed the matter as bearing on whether the intensity threshold is satisfied are quoted by ICTY in its decisions.²⁰² Despite of these facts no clear intensity test exists, nor is there any clear standard for ‘protracted’ conflict.²⁰³ The manner in which cyber warfare is mounted, it might do not have that continuity.²⁰⁴

Consequently, this would preclude many cyber operations from serving for the purpose of finding NIAC. Even highly destructive cyber-attacks would fail to qualify just because they did not occur on a regular basis over time and they would be addressed by criminal law paradigm instead of IHL.²⁰⁵

Another issue that needs to be tackled is the classification status of cyber-attacks conducted by an organized armed group during IAC between two States. If a group ‘belongs to’ a party to the conflict, the conflict would be international in character. The concept of ‘belonging to’ is in Article 4 of GC III 1949, which infers that “at least some

²⁰¹ Riots, civil disturbances or isolated and sporadic acts of violence do not meet the requirement of threshold of intensity. Okimoto, “The Relationship Between a State and an Organized Armed Group and Its Impact on the Classification of Armed Conflict”, 33-51.

²⁰² See, Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, 49 (ICTY, 2008), available at <http://www.icty.org/x/cases/haradinaj/tjug/en/080403.pdf>, (last accessed: July 19, 2016).

²⁰³ In *Abella*, the Inter-American Commission on Human Rights characterized a thirty-hour clash between dissident armed forces and the Argentinian military as non- international armed conflict. *Abella v. Argentina*, Case 11.137, Inter-American Commission and Court of Human rights., Report No. 55/97, OEA/Ser.LAV/II.98, doc. 6 rev. 148, 327 (1998), available at <http://hrlibrary.umn.edu/cases/1997>, (last accessed: July 19, 2016).

²⁰⁴ Dinniss, *Cyber warfare and Law of Armed conflict*, 130.

²⁰⁵ *Ibid.*

may, cyber warfare will make classification of conflict more challenging for States. With regard to IAC, attribution of cyber operations conducted by non-State actors will likely prove even more problematic than the attribution of kinetic actions to state. In the context NIAC, qualification as an organized armed group will prove increasingly complex as the structures are; means and prevalence of virtual organization grow and evolve. Perhaps most importantly, the approach taken for the interpretation of the term “armed” regarding cyber warfare is, although, presently reflecting *lex-lata*, unlikely to survive. Involvement of States and non-State actors, engaged in ever more destructive and disruptive cyber operations and societies, is becoming deeply dependent on the cyber infrastructure, State practice accompanied by *opinio juris* can be expected to result in a lowering of the current threshold. The law of cyber armed conflict is a work in progress and it needs to be sorted out till it’s too late.

CHAPTER 3

APPLICATION OF INTERNATIONAL HUMANITARIAN LAW ON CYBER WARFARE

Some people, no doubt animated by the noblest humanitarian impulses, would like to see zero-casualty warfare. However, this is an impossible dream. War is not a chess game. Almost by definition, it entails human losses, suffering and pain. As long as it is waged, humanitarian considerations cannot be the sole legal arbiters of the conduct of hostilities.²¹⁰

Yoram Dinstein.

Introduction

Cyber warfare is an emerging form of warfare not explicitly addressed by existing norms of IHL. It is argued that legal restrictions should be applied to cyber warfare. However, the international community has yet to reach the consensus that whether IHL applies to this new form of warfare or not. After providing an overview of the cyber warfare and alike terminologies and outlining several cyber warfare scenarios, this researcher argues that violations of the traditional principles of IHL are more likely to occur in cyber

²¹⁰ Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* 1.

warfare than in conventional warfare. States have strong reasons to engage in cyber-attacks. The belligerent will violate core principles of IHL more frequently in cyber warfare than in conventional warfare.²¹¹ Rather than to condemn all uses of cyber warfare, it is argued that IHL should evolve to encourage the use of cyber warfare in some situations and provide states better guidance in the conduct of these attacks.

The first chapter considers the general applicability of the IHL to cyber operations. It then turns to the crucial principle of distinction and military necessity, and assesses how it is to be applied in the cyber context. In particular, this chapter assesses what and who may be targeted (i.e. what constitutes a 'military objective', the issue of 'dual-use' objects in the cyber context and the prohibition on indiscriminate attacks.) The chapter then considers the various ways in which the principle of precaution may be relevant to cyber-attacks

3.1 Application of International Humanitarian Law on Cyber Warfare

The applicability of IHL to Cyber-attacks is under discussion on international platform. According to Mark Shulman, Adjunct Professor Fordham University, 'as[s] with other armed conflict, defensive [information warfare] operations are subject to the restraints of Law of Armed Conflict (LOAC) and its principles of proportionality', despite observing that 'information warfare is neither "armed" in the traditional sense, nor does it

²¹¹ Jeffrey T. G. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review* 106:7 (2008), 1427-451, <http://www.jstor.org/stable/40041623> (last accessed: June 21, 2016).

necessarily involve “conflict”²¹². On the other hand Richard Aldrich, Associate Professor of Law, USAir Force Academy, opines that a physical manifestation such as explosion is required: “‘Armed Conflict’, as presently understood, seems far less likely to be applied to the simple manipulation of bits inside a computer, although this may soon change since the nefarious manipulation of bits could, in some cases, already cause significantly more harm than could a bomb.”²¹³

From the afore-mentioned suggests that the question of applicability of the IHL to cyber- attacks arises in three different scenarios:

1. When cyber-attacks are carried out during ongoing conventional armed conflict;
2. When cyber-attacks are launched on their own;
3. When the use of conventional weapons is insufficient in and of itself to qualify as an armed conflict, but it is accompanied by extensive CNAs.

²¹² Mark R. Shulman, “Discrimination in Laws of Information warfare”, *Pace Law Faculty Publications* 1:1(1999), 1-33, available at, <http://digitalcommons.pace.edu/cgi/viewcontent>, (last accessed: December 14, 2016). It is to be noted that the earlier literature tends to use the term information warfare rather than computer network attacks, the former is a broader term than the later.

²¹³ Richard W. Aldrich, “The International Legal Implications of Information Warfare” *Information Warfare Series* 9(1996), 1-27, available at, www.dtic.mil/cgi-bin/Doc?AD_A0365379, (last accessed: December 14, 2016). Upon analyzing the approaches of these authors it may be said that although the authors do not treat cyber-attacks and other information operations homogenously, they fail to establish a test which either works within the framework of the IHL, or sets out appropriate components of information warfare which should be taken into account (means and results respectively). Other authors have perceived the issue from different angle; for instance, after considering armed conflict to the definition of aggression and using the terms armed force and armed attack synonymously, it is argued that LOAC will apply to CNAs where “consequences of the attack are equivalent to the damage done by traditional weapons”. Furthermore, the LOAC readily apply to CNAs: “in determining the constrains imposed on computer network attack by the law of war the focus of analysis must be the intent and likely results of an attack, not the novel method of attack.” For details see, Emily Haslam, “Information Warfare: Technological Changes and International Law”, *Journal of Conflict and Security Law* 5:2(2000), 157-175, available at, <https://www.deepdyve.com/doc/10.1080/10439862.2000.10555555>, (last accessed: December 14, 2016). But the physical consequences of cyber-attacks are always not immediate and always irreversible.

3.1.1 Application during Conventional Armed Conflict

The conflict between Russia and Georgia in 2008 is generally accepted to be the first incident of armed conflict accompanied by Cyber-attacks.²¹⁴ It may be argued that IHL cannot be applied as GC 1949 was drafted before the advent of the technology in warfare and such attacks.²¹⁵ However, this argument can be rejected on the basis of Martens Clause²¹⁶ and APs of GC 1949 and inclusion of Article 36 of API regarding the development and use of new weapons, means and methods of warfare.²¹⁷ However, it should be noted that cyber-attacks are different from both conventional weapons and

²¹⁴ The 2008 war between Russia and Georgia may represent the first time in history of “a coordinated cyberspace . . . attack synchronized with major combat actions in the other warfighting domains.” The cyber-attacks on Georgia’s military and government networks, including DDoS and website defacements, began three weeks before the physical hostilities and continued throughout the war. Linked to Russia’s “patriotic hackers/cyber militias,” the attacks were timed with the Russian military’s ground, air, and naval combat operations and closely coordinated with the “overall strategic objectives of the Russian government.” By disabling Georgia’s government and news websites, the attackers sowed panic and confusion among the Georgian civilian population because it was unable to communicate with its government. Cyber warfare also prevented Georgia from sending messages to the outside world, delivering Russia strategic communications victory. David Hollis, “Cyberwar Case Study: Georgia 2008”, *Small Wars Journal* (2011), available at, <http://smallwarsjournal.com/jml/art/cyberwar-case-study/>, (last accessed: August 10, 2016).

²¹⁵ Michael N. Schmitt also raises and dismisses a further possible argument that LOAC do not apply to CNA because they are not specifically mentioned in the Conventions.

²¹⁶ The Martens Clause has formed a part of the laws of armed conflict since its first appearance in the preamble to the 1899 Hague Convention (II) with respect to the laws and customs of war on land: “Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.” For details see, “The Martens Clause” available at, <https://www.icj.org/eng/documents/>, (last accessed: August 10, 2016).

²¹⁷ Article 36 AP I states: “in the study, development, acquisition or adoption of a new weapon, means and method of warfare, a high contracting party is under 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.” The same was reinstated by the court in the Nuclear Weapons case in 1996. In nuclear weapons case the court held that: indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the conferences of 1974-1977 left these weapons aside, and there is a qualitative as well as quantitative differences between nuclear weapons and all conventional arms. however, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in questions which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future. Nuclear weapons case, para. 86, available at, http://www.icj-cij.org/doCKET/index_5, (last accessed: December 14, 2016).

nuclear weapons that is the extent and type of damage caused by such attacks that entirely depends on the objective and design of attack. Whereas conventional and nuclear weapons result in physical destruction, injury and loss of life hence may be regulated by IHL. Therefore, problematic is when cyber-attacks may or may not cause physical destruction and indirectly affect civilians.

3.1.2 Cyber-Attack on its Own

The flexibility of the attack medium and delivery of possible consequences of cyber-attacks have raised a further argument against the application of the IHL to such attacks.²¹⁸ Although it is clear that one cannot apply a blanket rule against all computer network attacks, the question must be asked, whether cyber-attack or series of such attacks trigger the application of IHL.²¹⁹ Suppose the objectives of Stuxnet²²⁰ were more than explicit: it not only made uranium centrifuges to run at a different pace, which caused damages to the process of uranium enrichment and the centrifuges itself but also false signals were sent that the system works properly through the usage of certificates of two widely known companies.²²¹

²¹⁸ Helen Wilson & Patrick van Esch, *International Humanitarian Law: Attack of the Binary Bullet?*, *Journal of Politics and Law* 9:4(2016), 110-114, <http://www.ccsenet.org/journal/index.php/article>, (last accessed: December 14, 2016).

²¹⁹ Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks", *Harvard National Security Journal* 6(2015), 474-515, available at, <http://harvardnsj.org/wp-content/2015/06/Chayes.pdf>, (last accessed: December 14, 2016).

²²⁰ In 2010, an unexpected cyber-attack carried out against Iran's nuclear plant with the deployment of a worm called Stuxnet.

²²¹ However, no physical damage in the public domain was reported. Later on, it was said that perpetrators had used much time and resources for the creation of such worm. It is incurred that not only financial and technical means have to be implemented but also significant time and human efforts are needed for the repair of the damage. It is argued whether this would be sufficient to bring IHL into operation. Wilson & Esch, "International Humanitarian Law: Attack of the Binary Bullet?" 110-114. As far as the view of researcher is concerned it would not bring IHL into action because the term attack and

By applying the criteria given in *Tadic* case, Pictet's ICRC commentary and subsequent state practice shows that cyber-attack can initiate an armed conflict. The cyber-attack launched by the attacker that might be a state organ or an armed group may intend to cause, or which actually causes physical damage to life or property. It is perceived that consequences and intentions must be considered.²²² Attribution of cyber-attack to a state actor, ICRC's commentary, interference and manipulation of data results in massive destruction and damage of objects in this case the cyber operation seems to have reached the required threshold of harm.²²³ Based on this analysis, the stuxnet incident could be assumed to trigger an IAC and thus, IHL could be applied.

3.1.3 Computer Network Attacks in Support of Conventional Attacks

The third scenario where the application of IHL is raised when a conventional attack is launched accompanied by extensive number of cyber-attacks.²²⁴ In that case the supporting cyber-attacks would reveal the intentions of the opposing party. And it is believed that this combined tactic will increase the impact of conventional attack.²²⁵ For instance, the impact of conventional attack in a city would be huge if at the same time the city experience water cut off, power shut down along power to traffic signals, hospitals, and the emergency response telephone numbers disconnected. And it is contented that

armed aren't used in ordinary context there must be some severity attached to consequences or harm intended.

²²² This the case where the Pictet's commentary leave the state practice. Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks", 474-515.

²²³ And one can argue that cyber operation targeted computer data on which physical objects are dependent.

²²⁴ Dinnis, *Cyber warfare and The Laws of War*, 160.

²²⁵ *Ibid.*

such a combination of attacks would also be deemed sufficient to trigger an armed conflict and application of IHL.²²⁶

Like any other military operations, the cyber-attack must conform to the core principles of IHL. And the target selected for attack must be legitimate military object. However, the cyber attacks' compliance with the core principles of IHL raised some issues. And the ability to limit the consequences of cyber-attacks has caused commentators to think again over the criteria set forth for the application of principles of IHL.

3.2 Military Necessity

Although cyber-attack may represent a new type of weaponry, the law of war still requires consideration of the principles of necessity. It is one of the most fundamental principles of IHL. Broadly interpreted, military necessity means that armed forces can do whatever is necessary to achieve their legitimate military objectives in warfare but it should not to be unlawful under IHL.²²⁷

The assessment of whether a cyber-attack arose from military necessity will depend on a case-by-case determination. A cyber-attack that targets an adversary's military computer systems satisfies the condition of military necessity by virtue of their exclusive military association.²²⁸ But determining whether a target creates a 'definite

²²⁶ Ibid.

²²⁷ For example, enemy armed forces that have not surrendered or are not hors de combat are always legitimate military targets in themselves and may therefore lawfully be attacked at any time and in any place, irrespective of where they are located or what they are actually doing. For detail see, Kyle Genro Phillip, "The Sufficiency of the Law of Armed Conflict in the Cyber Domain", *Applied Research Journal* 70:3(2013), 70-75, available at, http://alepress.ajhr.edu/Portal/68/Documents/70-75_Phillips.pdf. (last accessed: January 27, 2017).

²²⁸ Daniel Garrie, "What is Cyber warfare and What are the rules?", *Journal of Law & Cyber Warfare: The New Frontier of Warfare*, 1:1(2012), 1-7, available at, <https://books.google.com.pk/books?id=bo504>, (last accessed: April 6, 2017).

military advantage' is complicated. And this requirement would limit cyber-attacks with indeterminate military advantages. The complexity of computer systems makes calculating military advantage a challenge. The value of cyber weapons often lies in its cascade effect on systems that rely upon the initial target. And most attackers do not have sufficient information to predict the indirect effects of an attack.²²⁹

Major Jensen, a Professor of International Law at the US army, asserts that "[t]hough intertwined, a separate look at military necessity and humanity, as they relate to the use of CNA, will illustrate that the current laws of war are sufficient to guide commanders in the use of CNA as a method or means of warfare."²³⁰ Practically, this requirement cannot be so easily met in cyber-attacks. The reason for that is the means of cyber warfare such as viruses, logic bombs or DDoS attacks, designed to reduce unusable network systems, do not have predesigned final outcomes.²³¹

3.3 The Principle of Distinction

The principle of distinction is codified in the Article 48 of AP I, according to which,

[i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between

²²⁹ Ibid., For instance, a cyber attacker that penetrates into the computer systems of an electrical generator might gain a military advantage, but the system may have unseen layers that prevent such an advantage from occurring. In those circumstances, the military advantage is not definite enough to satisfy the conditions of military necessity.

²³⁰ Johann Christoph Woltag, *Cyber Warfare: Military Cross-border Computer Network Operations Under International Law* (Cambridge: Intersentia Publishing Limited), 197.

²³¹ A hostile virus will replicate itself without knowing in advance how and where it will spread; a DDoS attack will render an entire network of botnet computers as 'zombies' but without any antecedent knowledge about which exactly the compromised machines will be. Phillip, "The Sufficiency of the Law of Armed Conflict in the Cyber Domain", 70-75.

the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

Similarly, AP II Article 13(1) touches on the subject by stating that “[t]he Civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations.”²³² Article 51 of AP I states that “[t]he Civilian population as such, as well as individual civilians, shall not be the object of attack.”²³³

According to ICJ, the principle of distinction prohibits ‘means and method of warfare, which would prohibit any distinction between civilian and military targets, or which result in unnecessary suffering to combatants.’²³⁴

The principle further can be found in the Statute of International Criminal Court, which states that ‘intentionally directing attacks against civilian objects, that is objects which are not military objects’ constitutes a war crime in IAC.²³⁵ In the *Tadic* case the Appeal tribunal extended the application of the principle to NIAC.²³⁶

²³² AP II Article 13(1).

²³³ Additional Protocol I, Art. 51(2).

²³⁴ Thus the purpose of the principle is to give effect to the general protection of civilians against the dangers arising from military operations as incorporated in Article 51(1) Additional protocol I. The subsequent targeting rules of Additional Protocol I must therefore be construed in the light of this principle classified as a basic rule of humanitarian law. *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) para. 95. See also, Woltage, *cyber warfare: military cross border computer network operations under international law*, 214.

²³⁵ Article 8(2)(b)(ii), Statute of the International Criminal Court, available at, <https://www.rome-statute.org/english.pdf>, (last accessed: August 3, 2016).

²³⁶ *Tadic* (*Interlocutory Appeal*), paras 112, 127.

3.3.1 Targeting in Cyber Warfare

According to article 52(2) AP I, attacks shall be limited strictly to military objectives, which are further described as objects which by their nature, location, purpose or use offer a definite military advantage by means of their total or partial destruction, capture or neutralization. Article 52(2) of AP I:²³⁷

Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

The challenge lies with the actual implementation of this definition in cyberspace and cyber warfare rather than with the relevance of its basic elements due to qualification of computer data as an object under IHL.²³⁸

3.3.2 Computer Data as an Object

According to the Oxford English Dictionary, in the realm of computing, data means ‘the quantities, characters, or symbols on which operations are performed by a computer, being stored and transmitted in the form of electrical signals and recorded on magnetic,

²³⁷ The definition of military objectives also appears in several subsequent instruments: Additional Protocols II and III, annexed to the 1980 Conventional Weapons Convention, and the second protocol to the Cultural Property Convention. Yoram Dinstein, “Legitimate Military Objectives Under the Current Jus in Bello”, *International Law Studies* 68(2012), 139-173, available at, <https://www.usnwg.edu/legitimate-Military-Objective.pdf>. (last accessed: December 15, 2016).

²³⁸ Because Object is corner stone of IHL and without assessing this in cyber context, it remains difficult to apply IHL on cyber warfare.

optical, or mechanical recording media'.²³⁹ And according to ICRC commentary object refers to something visible and tangible.²⁴⁰ It shows that only material tangible things can be targets.²⁴¹ Hence, cyber-attacks can be excluded from that definition because of their intangible nature. However, at the same time it is clear from the text of the commentary that this definitional point is being made to distinguish the term object as a 'thing' from its use in the sense of 'aim or purpose of an operation', rather than to exclude an intangible object from the definition.²⁴² Therefore, it may be concluded that any computer program, data base, system or virtual network would be considered as a legitimate target.

On other hand, the drafters of the Tallinn manual²⁴³ cited the ICRC Commentary on the Additional Protocols and observed that in this commentary, '[a]n object is characterized ... as something "visible and tangible"'.²⁴⁴ In the light of this interpretative background, data was poised to remain outside of the scope of IHL rules on targeting. The experts argue that 'Data is intangible and therefore neither falls within the "ordinary meaning" of the term object nor comports with the explanation of it offered in the ICRC

²³⁹ 'Data', Oxford English Dictionary, available at, <http://www.oxforddictionaries.com/definition/>, (last accessed: November 15, 2016).

²⁴⁰ Claud Pilloud, et al., *Commentary on the Additional Protocols of 8 June 1977* (Geneva: Martin Nijhoff, 1987), paras 2008-10.

²⁴¹ The notional targets such as 'civilian morale and victory' cannot be deemed as military objectives. for details see, Yoram, *The Conduct of Hostilities Under the Law of International Armed Conflict*, 181.

²⁴² Jack Goldsmith, "How Cyber Changes the Laws of War", *The European Journal of International Law* 24:1(2013), 129-138.

²⁴³ The Tallinn Manual is the result of a comprehensive and rigorous endeavor aiming to identify the rules of international law applicable to cyber warfare. Produced by a group of international experts who were 'carefully selected to include legal practitioners, academics, and technical experts', it purports to reflect their consensus as to the *lex lata* governing cyber conflict derived primarily from 'treaty law directly on point or sufficient state practice and *opinio juris* from which to discern precise customary international law norms'. The Manual identifies a total of 95 rules belonging to general international law, the law on the use of force, and IHL. For details see, Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 127.

²⁴⁴ *Ibid.*

Additional Protocols Commentary.²⁴⁵ This view adopted by majority of the experts of International Law.²⁴⁶ Those who drafted the Article understood objects as those entities that were visible and tangible and used these characteristics to limit the Article's reach.²⁴⁷

The researcher argues that the act of labeling data as an object provides no meaningful clarity to the identification of permissible military targets. This is because if data is an object and qualifies as a military objective, it may be attacked. If it is not an object, then such qualification is meaningless since the prohibition does not apply; it may be targeted and a loss of functionality does not ensue. From the perspective of those planning, approving, executing or commenting on an attack, labeling data as an object provides not a greater clarity than saying it is not data. Before interpreting data as an object it is also important to interpret target, military objective and attack in the context of cyber warfare, because these terms would altogether help in application of the principle of distinction on cyber warfare. And although the system targeted may be physically visible, but in fact the actual target is not that computer system, but its databases and programs running thereon. Therefore, this fact cannot be denied.

3.3.3 Dual Use Object

The term dual use target is not defined in IHL. Generally, a dual-use object is the one that "serves both civilian and military purposes."²⁴⁸ One of the often mentioned examples of

²⁴⁵ Goldsmith, "How Cyber Changes the Laws of War", 129-138.

²⁴⁶ Ibid.

²⁴⁷ Statement of US Representative, 'Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts', Geneva, 7 February 1975, CDDH/III/SR.15, Vol XIV, 119. Professor Yoram Dinstein has noted that '[t]he noun "objects", used in the definition, clearly encompasses material and tangible things. See also, Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict*, 92.

dual-use object is the coalition bombing of the Iraqi electrical grid in the Gulf War 1990-91. The outcome of that campaign was effectively expressed in the following words:

since the electrical grid in Iraq was totally integrated, attacks against it – and its installation- resulted not only in a tremendous military advantages (shutting down radar stations, military computers, etc.), but also extensive damage to civilians: hospital stopped operating, water pumping facilities came to a standstill, etc. from a legal point of view, a ‘dual-use’ of Iraq’s electrical grid did not alter its singular and unequivocal status as military objective. there was as usual with military objective the question of proportionality where collateral damage to civilians is concerned but the extensive damage to civilian was not excessive in relation to the military advantage anticipated.²⁴⁹

Most of the computer technology, hardware and software are of dual-use.²⁵⁰ Like some systems initially projected for military use have become so integrated into civilian society that any interruption caused by cyber-attacks would cause serious effects on civilians.²⁵¹ For instance, global positioning system (GPS) initially military system but now used by civilians as well, in many ways.²⁵² Therefore, spoofing the signal via may lead to massive disruption and possibly put in danger civilian lives.²⁵³

²⁴⁸ Schmitt, “Cyber Operations and the Jus in Bello: Key Issue”, 87-107.

²⁴⁹ Dinestein, *The Conduct of Hostilities Under the Law of International Armed Conflict*, 137.

²⁵⁰ Schmitt, “Cyber Operations and the Jus in Bello: Key Issue”, 87-107.

²⁵¹ Ibid.

²⁵² GPS uses two levels of signals: the military signal(Y-code) is more accurate and encrypted; the less secure civilian code (or P-code) is not and thus makes it more susceptible. the precision timing provided by the GPS system is needed for the accurate routing of information packets through computer networks. <http://www.dictionaty.com/browse/gps/>, (last accessed: December 15, 2016).

²⁵³ Spoofing the signal involves feeding a GPS receiver a fake signal so that it computes the wrong time or location of the receiver. See more at, <http://techartms.com/definition/spoofing/>, (last accessed: December 15, 2016).

Dual-use targets become attractive because the attacker not only benefits from the destruction of the target's military value but also from collective effects on the civilian population.²⁵⁴ The interconnectivity of cyberspace and its usage by the military forces may be indistinguishable from civilian uses. Civilian items could easily become targets by giving a vast number of digital networks or infrastructure that is used by military and civilians simultaneously.

3.3.4 Targeting Civilians Objects

Article 52(1) AP I provides that "civilian objects shall not be the object of attack or reprisals."²⁵⁵ ICJ stated in its Nuclear Weapons Advisory Opinion that 'States must never make civilians the object of attack.'²⁵⁶ Like definition of civilians, civilian objects are also negatively defined as all objects which are not military objectives.²⁵⁷ And in case of doubt regarding the civilian character of a person or an object, the doubt goes in favor of civilian.²⁵⁸ Again, in the case of cyber-attack, the threshold question is whether the attack is intended to, or foreseeably will, cause injury, death, damage or destruction or

²⁵⁴ Dinniss, *Cyber warfare and the Laws of War*, 195.

²⁵⁵ Article 52(1) AP I, https://www.icrc.org/eng/assets/files/other/ferc_0002_0321.pdf, (last accessed: December 16, 2016).

²⁵⁶ Nuclear Weapons Case, para. 78.

²⁵⁷ Article 52(1) Additional Protocol I states that available at, <https://www.icrc.org/eng/assets/pdf/>, (last accessed: December 15, 2016).

²⁵⁸ Article 50(1) states that A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A 1), 2), 3) and 6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian. and 52(3) AP I states that in case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used. For details see, <https://www.icrc.org/eng/assets/pdf/>, (last accessed: December 15, 2016).

not if so, the prohibitions set forth earlier, which undeniably restate existing customary law, apply.²⁵⁹

Unfortunately, the norms, albeit clear at first sight, are subject to interpretative difficulties. The differing standards for distinguishing civilian objects from military objectives are most probably due to interconnectivity of systems or dual-use objects. Indeed, most military networks rely on civilian, mainly commercial, computer infrastructure, such as under-sea fiber optic cables, satellites, routers, or nodes; conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on GPS satellites, which are also used by the military. Thus, it is impossible to differentiate between purely civilian and purely military computer infrastructure easily.

3.3.5 Attacks and Operations

One of the distinctive features of cyber-attacks or CNA is to neutralize or destroy target systems without causing physical damages.²⁶⁰ For example, data may be manipulated, corrupted or deleted to cause massive harm or even complete loss of functionality of a computer system or network without ever causing physical damage to the system, its components or surroundings. This raises an interesting question regarding the legitimate targets of such attacks. The basic rule, thus stated, is general in nature and is set out at the beginning of a series of more specific rules which, *inter alia*, prohibit the targeting of civilians and civilian objects; however, these subsequent rules are phrased in terms of the

²⁵⁹ Schmitt, *Wired warfare: Computer network attack and jus in bello*, 382.

²⁶⁰ Woltag, *Cyber Warfare: Military Cross Border Computer Network Operations under International Law*, 214.

prohibition or restriction of ‘attacks’ rather than operations.²⁶¹ The term ‘attack’ is defined in IHL as “acts of violence against the adversary, whether in offence or defense”.²⁶² The requirement of ‘violence’ in the definition denotes the use of physical force. It is argued that whether cyber operations that do not rise to the level of physical harm are covered by the rules governing the conduct of hostilities or not.

To differentiate between attacks and operations to have any meaning, it must then be determined what constitutes a military ‘operation’ as distinct from an attack. According to the ICRC commentary to API 1977 Article 48, the term “operations’ should be understood to refer to *military* operations (as opposed to political or other kinds of operations) which ‘refers to all movements and acts related to hostilities that are undertaken by the armed forces’.²⁶³ Similarly, the commentary to Article 51 refers to military operations as “all the movements and activities carried out by the armed forces with a view to combat.”²⁶⁴ Thus the notion of an ‘operation’ can be seen as a distinctly broader concept than that of an attack, albeit one that is still closely connected with the conduct of hostilities.

²⁶¹ For example, Article 52 of API 1977 states that ‘civilian objects shall not be the object of attack’ and that ‘attacks shall be limited to military objectives’. And Article 57 provides a list of specific precautions that must be taken ‘with respect to attacks’.

²⁶² See Article 49 of API 1977 available at, <https://www.icrc.org/en/assets/pdf>, (last accessed: December 15, 2016).

²⁶³ Claude Pilloud, et al., *Commentary on the Additional Protocols of 8 June 1977* (Geneva: Martinus Nijhoff, 1987), para 1875, available at, <https://ihl-databases.icrc.org/hl/COM/750001/Document>, (last accessed: September 26, 2016).

²⁶⁴ Indiscriminate attacks are: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction. Pilloud et al., 1987: para. 1936. Similarly, Article 57 says that ‘the term “military operations” should be understood to mean any movements, maneuvers and other activities whatsoever carried out by the armed forces with a view to combat. Pilloud et al., 1987: para. 2191.

The researcher opines that this difference between attacks and operations leaves an inconsistency in the law and the nonlethal potential of Cyber warfare that may lead to more attacks on traditionally protected objects and individuals than occurs in conventional warfare.²⁶⁵

3.3.6 Indiscriminate Attacks

IHL prohibits indiscriminate attacks. This prohibition is established as customary International Law in international and non- international armed conflicts, and is codified in Article 51(4) of API (1977).²⁶⁶ Indiscriminate attacks may result either from the use of a means or method of warfare or that is indiscriminate by its very nature.²⁶⁷ The application of this rule on cyber warfare depends upon the type of means used in it. Particularly two methods of cyber-attacks, viruses²⁶⁸ and worms²⁶⁹ likely to fall into this

²⁶⁵ In providing belligerents a gain in military advantage without an additional threat to civilian lives, cyber warfare is more likely than conventional warfare to lead belligerents to ignore the principle of distinction to attack directly what IHL has traditionally sought to protect.

²⁶⁶ Article 51(4) AP I 1977, available at, <https://ihl-databases.icrc.org/ihl/750065>, (last accessed: August 5, 2016).

²⁶⁷ As it relates to the latter, this means that the weapon concerned either cannot be directed at a specific military objective or that the effects of the weapon cannot be limited as required by IHL, so that it will strike both military objectives and civilian objects without distinction. For details see, Woltage, *Cyber Warfare: Military Cross Border Computer Network Operations Under International Law*, 224.

²⁶⁸ A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. See briefly computer virus, available at, <http://www.webopedia.com/Virus.html>, (last accessed: August 5, 2016).

²⁶⁹ A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of the original code to other computers, causing harm by consuming bandwidth or possibly deleting files or sending documents via email. Worms can also install backdoors on computers. Worms are often confused with computer viruses; the difference lies in how they spread. Computer worms self-replicate and spread across networks, exploiting vulnerabilities, automatically; that is, they don't need a cybercriminal's guidance, nor do they need to latch onto another computer program. As such, computer worms pose a significant threat due to the sheer potential of damage they might cause. A particularly notorious incident occurred in 1988. A computer worm since named the Morris worm caused hundreds of thousands, if not millions, of dollars in damage,

category as their effects are often unlimited. Due to interconnectivity of military and civilian computer networks, computer viruses seem to be difficult to control its effect.²⁷⁰ For instance in February 2009, the so called cyber worm 'Win32/conficker'²⁷¹ infected the computer systems of the French, British and German armed forces, the Manchester City Council, the House of Commons and numerous home computers.²⁷² If it had been a military cyber-attack with physical damages and consequences, it is obvious that the effects are indiscriminate as the worm cannot distinguish between civilian and military targets.

One of the examples of indiscriminate attacks prohibited by IHL is set out in Article 51(5) of API 1977 commonly known as target area bombing.²⁷³ In respect of cyber warfare, the issue is also related to the definition of military objectives and the level of specification at which such definition occurs, like, network system, component or even code are military objective or not. Particularly, in an era of extensive dual- use

and its creator was convicted under the Computer Fraud and Abuse Act. see briefly definition of cyber worm, available at <http://www.pctools.com/security/news/what-is-a-computer-worm/>, (last accessed: August 5, 2016).

²⁷⁰ Schmitt, *Wired warfare: Computer Network Attacks and Jus in Bello*, 389.

²⁷¹ Cyber worm 'Win32/conficker' which infects computers using advanced malware techniques. When the worm takes over a computer it registers it onto a network called the botnet, which is a collection of compromised computers running software under a common command and-control server. Once a hijacked computer is on the botnet, the owner of the botnet can give commands to the hijacked computers and pull data from them. This simplifies the work of cyber criminals and, at the same time, places an unprecedented amount of computing power into the hands of criminals who can conduct Distributed Denial of Service (DDoS) attacks against different targets. DDoS attacks are conducted when the targeted server is bombarded with queries from different sources in such quantities that the available bandwidth for the server is overloaded. The result is that the server cannot process the requests and slows down or goes offline. This can also compromise the server and the data within the computer system. Estimates differ, but the worm could have infected from nine to 15 million computers.

²⁷² Erki Kodar, "Applying The Law of Armed Conflict to Cyber Attacks: From The Martens Clause to Additional Protocol I" *Stanford Journal of International Law* 38(2002), 207-217, available at <http://www.ksk.edu.ec/wp-content/2012/11/Toimetspdf>, (last accessed: August 15, 2016).

²⁷³ It prohibits "an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects." For details see, Article 51(5) of API 1977, available at <https://ihl-databases.icrc.org/ihl/750005>, (last accessed: August 5, 2016).

systems and increasing virtualization of both data storage and services. The law requires that targets must be attacked separately when they are ‘clearly separated’ – has been interpreted by states to mean that the distance ‘be at least sufficiently large to permit the individual military objectives to be attacked separately.’²⁷⁴ In the cyber realm this will be dependent on the type of system or network that is intended.

3.4 Principle of Proportionality

The second types of indiscriminate attacks that are prohibited by API are attacks that breach the principle of proportionality.²⁷⁵ This principle is given in Article 51(5)(b) of API 1977 as “an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”²⁷⁶

The principle of proportionality is similar to distinction between both, concern with the consequences of an attack on civilians and civilian object. Furthermore, the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage caused to civilians and civilian objects is governed by this principle.²⁷⁷ As one of the courts note, the laws of war

²⁷⁴ James A. Green (ed.), *Cyber Warfare: A multidisciplinary analysis* (New York: Routledge Publishers, 2015), 130, available at <https://www.scribd.com/CyberWarfareAnalysis>, (last accessed: August 6, 2016).

²⁷⁵ Heather A. Harrison Dinniss, *The regulation of cyber warfare under the jus in bello* in James A. Green (ed.), *Cyber Warfare: A multidisciplinary analysis* (New York: Routledge Publishers, 2015), 137, available at <https://www.scribd.com/CyberWarfareAMultidisciplinaryAnalysis>, (last accessed: August 6, 2016).

²⁷⁶ Article 51(5)(b) of API 1977, available at <https://ihl-databases.icrc.org/ihl/750065>, (last accessed: August 5, 2016).

²⁷⁷ The Rome Statute incorporates proportionality within its enumeration of particular crimes, Article 8(2)(a)(iv) references “extensive destruction . . . not justified by military necessity” and Article 8(2)(b)(iv) states that “intentionally launching an attack in the knowledge that such attack will cause

“creates a delicate balance between two poles: military necessity on one hand, and humanitarian considerations on the other.”²⁷⁸ The said principle applies to the indirect effects of an attack as well. For instance, a cyber-attack is responsible for the indirect effects on a civilian population caused by an attack on the control system of an electrical generator.

Two major problems raised by cyber operations in relation to proportionality relates to the expected ‘knock-on’ or indirect effects²⁷⁹ on civilians and civilian objects and dual-use technological systems.

3.4.1 Knock-on Effect

Assessing indirect or knock-on effects in cyber warfare may prove to be one of the most difficult issues in applying principle of proportionality.²⁸⁰ It is clear that a commander must consider the direct effects of his cyber-attack. These direct effects are defined as the “immediate, first order consequences, unaltered by intervening events or mechanisms.”²⁸¹ In the cyber domain, this would include the effects on a computer that is shut down by a cyber-attack or the damage to the centrifuges caused by the Stuxnet malware.²⁸²

incidental loss . . . or damage . . . would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.” In Beit Sourik, the court articulated the principle as focusing on “the relationship between the objective whose achievement is being attempted, and the means used to achieve it.”

²⁷⁸ See, HCJ 2056/04 Beit Sourik Village Council v. The Government of Israel [2004], art. 34 (Barak, C.J), available at, <http://www.refworld.org/docid/4374ac594.html>, (last accessed: December 15, 2016).

²⁷⁹ Both 1990-91 gulf war and the NATO action in Yugoslavia illustrated the knock-on effects of targeting the electricity networks.

²⁸⁰ Green (ed.), *Cyber Warfare: A multidisciplinary Analysis*, 139.

²⁸¹ Ibid.

²⁸² Some attacks have such dangerous indirect effects that they are prohibited. As stated in Article 56 of Additional Protocol I, “works or installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations, shall not be the object of an attack, even where those objects are

Knock-on effects are “the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms.”²⁸³ In the cyber domain of war, this would include damage that was not the intent of the attack, but that resulted from elements of the attack. Suppose, in the case of Stuxnet, the malware infected many computers beyond its intended targets within Iran. Here the problem in adopting this principle while carrying out cyber -attack is the nature of computer systems and linkage between military and civilian systems. Therefore, the attacker should be well aware of the mapping of targeted network to know which ancillary networks or systems are connected to the intended target.

3.5 The Principle of Precaution

Parties to an armed conflict should take certain precautionary measures both in carrying out military operations and attacks, and against the effects of attacks as required by IHL.²⁸⁴ These obligations have been recognized by the Appeals Chamber of the ICTY in both the *Tadić* and *Kupreškić* cases.²⁸⁵ The principle of Precautions in attack states that:

I. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.

military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.”

²⁸³ Green (ed.), *Cyber Warfare: A multidisciplinary Analysis*, 146.

²⁸⁴ *Ibid.*

²⁸⁵ *Prosecutor v. Tadić*, case No. IT-94-1-AR72, Decision on the defence motion for interlocutory appeal on jurisdiction of 2 October 1995, paras. 119 and 126-127. In the *Kupreškić* case, the ICTY recognized in particular the customary nature of the requirement to take precautions in attack and the applicability of this norm in non-international armed conflicts. for details see, ICTY, *Kupreskić* case, Judgment, paras. 49 and 132, available at, www.icty.org/x/cases/tadic/acjug/cn/tad-aj990715e.pdf, (last accessed: December 24, 2016).

2. With respect to attacks, the following precautions shall be taken: (a) those who plan or decide upon an attack shall:

(i) Do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;

(ii) Take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;

(iii) Refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . ²⁸⁶

IHL requires that feasible measures should be taken in planning and carrying out attacks. Feasibility has been interpreted by many states to mean 'those precautions that are practicable or practically possible, taking into account all the circumstances ruling at the time, including humanitarian and other considerations'.²⁸⁷ Cyber warfare raises several issues in applying this principle while carrying out cyber-attack.²⁸⁸

²⁸⁶ See article 57 AP I, available at, https://www.icrc.org/eng/assets/files/other/ivrc_002_0321.pdf, (last accessed: December 16, 2016).

²⁸⁷ It should be noted that the standard of feasibility applies to all attacks against targets on land (from whatever platform they are launched); attacks against targets in the air or at sea are subject to 'all reasonable' precautions, which may be interpreted as 'a little less far-reaching' than the feasibility standard. See, Pilloud et al., 1987: para. 2230.

²⁸⁸ Before assessing them it should be noted that, the requirements regarding targeting set out in article 49 and provisions related to precautions in attack refers to 'attack'. on the other hand, the general rule expressed in article 57(1) Additional Protocol I requires that constant care must be taken to spare the civilian population, individual civilians and civilian objects in the course of military operations. therefore, it may be assumed that the specific rules mentioned afore will only to those computer network attacks which result in physical damages injury or death.

3.5.1 Verification of Objectives

Those who plan or decide on an attack are required to do everything 'feasible'²⁸⁹ to verify that the target or targets of the attack are military objectives and that it is not prohibited to attack them.²⁹⁰ This rule is based upon article 57(2)(a)(i) AP I. In cases of a predetermined cyber- attack against a specified target, this obligation does not seem problematic. However, targets of opportunity or automated 'hack- backs' may be problematic because of the danger of hacking back against a target computer that has been spoofed, where the source of the attack has not been accurately attributed (i.e. the source appears to be the attacking computer when in actuality it is not). The fact that most of the cyber- attacks that are in disguise do not make them unlawful by it, however it does mean that those deciding on attacks will need to be particularly vigilant regarding the verification of targets.

²⁸⁹ The legal standard of feasibility appears in several places in the "Precautions in Attack". see, API, supra note 15, arts. 57.2(a)(i)–(ii), 58 and applies to most types of attacks. In various provisions, a commander must do "everything feasible"⁴¹ or "take all feasible precautions." During the ratification process, there was great debate about the term "feasible" and what it meant.⁴³ A number of representatives to the negotiating convention made specific comments about the meaning "feasible" was to have when applied as a legal standard. John Redvers Freeland,⁴⁴ the head of the United Kingdom delegation, through several sessions stated that the words "to the maximum extent feasible" related to what was "workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations. Similarly, S.H. Bloembergen, a delegate from the Netherlands, stated that "feasible" should be "interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time. As a result, "feasible" is generally understood to mean that which is "practicable or practically possible, taking into account all circumstances ruling at the time." See briefly,

²⁹⁰API, 1977: Article 57(2)(a)(i).

3.5.2 Choice of Means and Methods

In order to avoid, and in any event to minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects, attackers are required to take all feasible precautions in the choice of means and methods of attack ²⁹¹

The ability of cyber warfare to achieve its desired effects without causing physical harm to surrounding civilian objects may mean that states with the ability to launch an attack by cyber means should utilize those options instead of traditional kinetic means. However, at the same time interconnectedness of the cyber environment also increases the potential for knock- on effects to cause more collateral damage that may result from a conventional attack. Thus, most probably the assessment will be highly dependent upon facts on both the operation planned and the type of cyber- attack anticipated. For instance, in 2010 the Stuxnet virus was specifically created to deploy its payload only when it reached a particular system containing a set combination of software and hardware operating at particular frequencies. That allowed the attackers to minimize the collateral damage to the surrounding systems, despite of purposely utilizing the civilian gateway targets as their attack vector.

3.5.3 Choice of Targets and Interconnectedness

Article 57(3) of API 1977 states that: “when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be

²⁹¹ It should also be noted that the rule that all feasible precautions must be taken in the choice of means and methods of attack applies independently of the principle of proportionality. That is, the choice of means and methods of attack must be taken even where neither of the methods under consideration would result in excessive damage to civilians or civilian objects such that it would breach the proportionality principle. It is an additional measure designed to minimise the effects of hostilities on the civilian population. API, 1977: Article 57(2)(a)(ii).

that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.”²⁹²

This obligation is particularly important due to large amount of interconnectedness and the high incidence of dual-use systems in the cyber environment.²⁹³ The unique ability of cyber warfare to break down targeted networks and systems into ever smaller components in order to locate and affect precisely the exact military objective required to achieve the desired result.²⁹⁴ Suppose, a targeted system may be neutralized by disabling an essential component of the system so that it is unable to function, by attacking the system as a whole, by attacking the network on which that system resides, or by shutting off the electrical supply to the site containing the targeted system.²⁹⁵ However, in most of the cases, attacking the network as a whole or shutting off the electrical supply, if they are not isolated systems, will also have an impact on civilian portions of the network or other civilian infrastructure.

3.6 Perfidy and Ruses of War

Cyber operations provide an ample opportunity in modern armed conflicts for parties to engage in tactics designed to deceive and mislead the enemy or induce them to act recklessly.²⁹⁶ Ruses are defined in Article 37(2) of API (1977).²⁹⁷ Traditional examples of

²⁹² See, Article 57(3) of API 1977, available at, https://www.icrc.org/eng/assets/002_0321.pdf, (last accessed: December 16, 2016).

²⁹³ Michael, “Cyber-attacks and the Laws of War”, 525-579.

²⁹⁴ Swanson, “The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict”, 303-333.

²⁹⁵ Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law*, 159.

²⁹⁶ Deception and other ruses of war are entirely permissible and have a long and renowned history in warfare, where the deception invites the confidence of the enemy as to the existence of protected status

permissible uses are the use of camouflage, decoys, mock operations and misinformation. Perfidy, is defined in Article 37(1) of API (1977).²⁹⁸ The key difference between deceptions that amount to lawful ruses and those that constitute prohibited perfidy is the exploitation of a deliberately induced trust on the part of an adversary in order to kill, injure or capture.²⁹⁹

In the cyber domain one of the key difficulties in determining the threshold between legitimate ruses and prohibited perfidy is caused by the civilian nature of much of the cyber infrastructure.³⁰⁰ In cyber operations one of the most common tactics is the routing of an attack through multiple 'stepping- stone' hosts (routers, servers and computers, etc.) in order to disguise the origin of the attack. While there is no prohibition on concealing the origin of the attack per se, as most of the hosts will be civilian in nature, there is a risk that the victim of the attack may conclude that one of civilian stepping- stone hosts is the originator of the attack. Where this technique is carried out in such a manner as to invite that conclusion (or the conclusion that it originates from any other host with protected status) and the operation results in the death, injury or capture of the adversary, it will amount to perfidy.

under international law in order to attack them, the act crosses the line into perfidy (or treachery) and is prohibited under the jus in bello. Both the permissibility of ruses and the prohibition against perfidy are reflective of customary international law. Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", 303-333.

²⁹⁷ Article 37(2) API (1977) states that acts which are intended to mislead an adversary or induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law.

²⁹⁸ Article 37(1) API (1977) states that act 'inviting the confidence of an adversary to lead him to believe that he is entitled to, or obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence'.

²⁹⁹ Feigning civilian status in order to mount an attack is a classic example of perfidious behavior. Swanson, "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict", 303-333.

³⁰⁰ Ibid.

Conclusions

It is concluded that like any other military operations, the cyber-attack must conform to the core principles of IHL. And the target selected for attack must be legitimate military object. However, cyber-attacks compliance with the core principles of IHL raised some issues. And the ability to limit the consequences of cyber-attacks has caused commentators to think again over the criteria set forth for the application of principles of IHL, because violations of the traditional notions and cardinal principles of IHL are more likely to occur in cyber warfare than in conventional warfare. States are unlikely to refrain from engaging in some forms of prohibited conduct. Thus, due to potentially lethal nature of cyber weapons, and non-physical consequences of cyber-attacks, the meaning of these principles should evolve to accommodate cyber warfare. Because in some cases, the use of this new and changing method of warfare is encouraged if it adheres to principles of IHL. However, this process would be evolutionary not revolutionary. Such an evolution will allow the rule of law to guide the development of cyber warfare to ensure that civilian lives are protected in the age of cyber warfare.

CHAPTER 4

COMBATANT STATUS, DIRECT PARTICIPATION IN HOSTILITIES AND CYBER WARFARE

Introduction

Since, the beginning of 21st century, the war-fighting capacities of the modern military has gone under several changes.³⁰¹ The most significant changes are range of people involved and the technologies.³⁰² It might be easy to apply IHL on combatants and civilians carrying rifles on front line rather than the status of personnel armed with Central Processing Units (CPUs) and keyboards sitting at a desk far away from battle field.³⁰³ It might be because of two reasons: first it is not clear how the requirements of lawful combatancy will be applied on to the medium where anonymity is the fact and distance and proximity does not matter. Secondly, the initiation of specialist nature of new technologies and increased civilianization of state armed forces.³⁰⁴

This chapter provides an examination of the status of persons involved in cyber warfare in the light of combatant's status and civilian's direct participation in hostilities under IHL, and assesses whether these rules are relevant to cyber warfare or not.

³⁰¹ Charlotte Lülf, "Modern Technologies and Targeting Under International Humanitarian Law", IFHV Working Paper 3:3(2013), 32, available at, http://www.ifhv.de/documents/wp3_3.pdf, (last accessed: August 10, 2016).

³⁰² Ibid.

³⁰³ Sean Watts, "Combatant Status and Computer Network Attack", *Virginia Journal of International Law* 50:2(2010), 391-417,

³⁰⁴ Ibid.

4.1 Combatants

IHL makes fundamental distinction between civilians and combatants.³⁰⁵ The latter can take part in hostilities and may attack, kill and wound enemy combatants and destroy military objects. Contrary to this, civilians are not allowed to participate directly in hostilities. Being a civilian they enjoy protection from the danger arising from military operations and must not be directly targeted.³⁰⁶ However, once a civilian directly participates in hostilities they lose their protected status till their involvement. And they may be punished either via domestic law or international law.³⁰⁷

According to AP I combatants are “[m]embers of the forces of a party to the conflict (other than medical personnel or chaplains...)”; the preceding section establishes that:³⁰⁸

[t]he armed forces of a party consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which ‘inter alia’, shall enforce compliance with the rules of international law applicable in armed conflicts.

³⁰⁵ See briefly *Nuclear Weapons Case*, 257.

³⁰⁶ Lucian Dervan, “Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown”, *Goettingen Journal of International Law* 3:1(2011), 373-396, available at, http://www.gjil.gu.issues/31/21/article_dervan.pdf, (last accessed: December 14, 2016).

³⁰⁷ This definition has proved highly controversial and is one of the reasons behind the states refusal to ratify the protocol. the reason for controversy is the inclusion of armed groups within the definition. Article 43(1) and (2) Additional Protocol I.

³⁰⁸ Article 4(A)(1), (2) (3) and (6) Geneva Conventions III.

It is contended that four of the groups given in Article 4(A) of the Geneva Convention 1949 are known as combatants:³⁰⁹ (1) members of the armed forces of a party; (2) militias, volunteer corps and organized resistance movements belonging to a party; (3) armed forces of parties to the conventions not diplomatically recognized by their enemy; (4) members of *levée en masse*.³¹⁰

According to Article 50 of AP I people who do not fall within the above mentioned categories are known as civilians. However, those persons who are associated to armed forces without actually being a part of it and they are authorized by a party to the conflict and are entitled to prisoner of war status but not combatant's status. In IHL, combatants may be further divided two categories: those people who belong to belligerent party, their specific task may not be related to active hostilities; second, any person who is actively involved in hostilities such person is called unlawful combatant.³¹¹

³⁰⁹ Watts, "Combatant Status and Computer Network Attack", 394.

³¹⁰ The term *levée en masse*, which first became an international legal term at the Brussels Conference in 1874, must be distinguished under the laws of war from an insurrection by a people against its own national government. The *levée en masse* is defined as taking place against foreign troops either invading or occupying a country, restricting the definition to one involving national self-defense. It refers especially to situations in which the populace spontaneously takes up what weapons it has and, without having time to organize, resists the invasion. see *levée en masse*, available at, <http://www.crimesofwar/lev>, (last accessed: August 12, 2016).

³¹¹ Article 4(A)(4) Geneva Conventions III states that: Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model. available at, <https://ihl-databases.icrc.org/ihl/Web/ART/375-590007?OpenDocument>, (last accessed: August 11, 2016). Yoram dinstein, argues that unlawful or unprivileged combatant status can be achieved in one or two ways: either combatant's primary status is that of combatant and they lose their privileged status through lack of compliance with the lawful combatancy; or they are civilians directly participating in hostilities. see generally Dinstein, *The Conduct of Hostilities Under the Law Of International Armed Conflict*, 36.

4.1.1 Requirements of Combatant Status and Cyber Warriors

Yoram Dinstein has raised seven collective conditions for legal combatancy.³¹² The first four conditions are those conditions which are set out by Geneva Conventions for the applicability of lawful combatant and prisoner of war status: being under a command of a person responsible for his or her subordinates; having a fixed distinctive sign recognizable at a distance; carrying arms openly; and conducting operations in accordance with the laws and customs of war.³¹³ Other two conditions may be taken from article 4(A)(2) of Geneva Convention III; organization and belonging to party to conflict. And seventh condition is any person owing a duty of allegiance to a detaining power would not be given prisoner of war status.³¹⁴ Therefore, the status of lawful combatant or prisoner of war will be accorded to the members of armed forces of a party. Application of these conditions with respect to computer network attacks raises several problems.

Literal application of these requirements to cyber warriors is likely to result in the conclusion that some of these actors are not lawful combatants. They are unlikely to wear uniforms; given that they are not part of the armed forces of the State. They are also likely to hide the military nature of computers used in a cyber-operation by employing the outward markings of civilian computer infrastructure, such as a civilian Internet Protocol (IP) address.

³¹² For details see, Dinstein, the conduct of hostilities under the law of international armed conflict,

³¹³ Art 13(2) Geneva Conventions I and II and Art. 4(2) Geneva Convention IV.

³¹⁴ Seventh condition is taken from a case law Public prosecutor v. Koi et al. 1968 Public Prosecutor V. Koi et al. (1968), AC, privy council. The privy council considered that the principle was one of the customary international law. For details see, Rogers, Law on the battlefield (UK: Manchester University Press, 2004), 32.

4.1.2 Distinction

The second and third conditions raise similar problems for cyber warfare.³¹⁵ One of the characteristics of the internet is anonymity, that is impossible to tell who is sitting at any particular computer creates problem in application of IHL on Cyber warfare.³¹⁶ These rules were drafted in an era where warfare involved a certain amount of physical proximity between opposing forces. Combatants and noncombatants could see and can distinguish between each other. Whereas, in case of cyber warfare opposing parties are plainly not in sight of each other and may be half a world away.³¹⁷

Taking an example of troops who are serving abroad or travelling upon vehicles, engines of war, aircrafts, tanks and boats etc. whenever partisans are on board they all are required to be marked with the distinctive sign of the belligerent party.³¹⁸ This can also be applied to computer network attacks from which attack is launched. Scholars have argued that these distinctive requirements are obsolete with respect to cyber operations because cyber operations are launched remotely; the failure of a cyber-warrior to wear a uniform, for example, does not provide him an inappropriate military advantage by appearing to blend with the civilian population.³¹⁹

³¹⁵Haslam, "Information Warfare: Technological Changes and International Law", 157-175.

³¹⁶ Schmitt, "Wired Warfare: Computer Network Attack and the Jus in Bello", 369-381.

³¹⁷ Emily Crawford, "Virtual Backgrounds: Direct Participation in Cyber Warfare", *A Journal of Law and Policy for The Information Society* 9 (2013), 1-19, available at, <http://moritzlaw.osu.edu/pdf/>, (last accessed: January 28, 2017).

³¹⁸ This is in line with the long-established regulations in international law regarding the flag in the case of war at sea. Pictet, *commentary*, 60. Although note that this does not absolve the combatant on board from wearing their personal distinctive emblems once they are separated from the aircraft or other vehicle: Dinstein, *Conduct of Hostilities*, 45.

³¹⁹ Schmitt, "Wired Warfare: Computer Network Attack and the Jus in Bello", 369-381.

4.1.3 Compliance, Organization, Belonging and Allegiance

Some of the CNAs methods like DoS involve more dispersed structure of armed group, allowing group members who are geographically dispersed to play a more active role in organized actions. Therefore, if the group does not have the necessary organization whether in network or hierarchical form and does not maintain discipline and supervision, its members cannot be lawful combatants. In *Akeyesu*, the trial chamber of the ICTR stated that:³²⁰

The armed forces opposing the government must be under responsible command, which entails a degree of organization within the armed group or dissident armed forces. This degree of organization should be such so as to enable the armed group or dissident forces to plan and carry out concerted military operations, and to impose discipline in the name of a *de facto* authority.

Cyber warriors engaged in cyber operations on behalf of non-State groups which are engaged in NIAC are not to be entitled to lawful combatant status because they do not “belong to” a State party to the conflict.³²¹ “Hacktivists,” or non-State actors unaffiliated with either side in an armed conflict who undertake cyber operations out of personal sympathies with a belligerent also do not qualify for combatant status because they lack a relationship with a State party to the conflict. One explanation for the cyber-attacks

³²⁰ *Akeyesu*, para 626, available at, <https://casebook.icrc.org/casebook/doc/case-study-1011-akeyesu-case-study.htm>, (last accessed: August 1, 2016).

³²¹ For example, members of al Qaida have admitted to engaging in “low-level and disruptive” cyber operations including sabotage of political websites and denial of service attacks as part of their organization’s war with the United States. Such individuals, even if part of the armed wing of al Qaida, would not qualify for lawful combatant status. See, Woltag, *Cyber Warfare: Military Cross-border Computer Network Operations Under International Law*, 204.

directed against Georgian websites is that they were launched by the nationalist Russian hacker community, which may have been tipped off by the Russian government about plans to use force in South Ossetia.³²² Such kind of affiliation with the State is improbable to meet the standard for “belonging to a Party” to the conflict because hacktivists are not under the “effective control” of the State.³²³

4.2 Direct Participation in Hostilities by Civilians

Civilians are entitled to protection from the harm arising from the hostilities and may not be targeted until, and for such time as, they take an active or direct part in hostilities.³²⁴

However, when civilians take direct part in hostilities, they lose their protected status for the period of their involvement.³²⁵

³²² Michael N. Schmitt, “War, Technology, and International Humanitarian Law” *Harvard University Program on Humanitarian Policy and Conflict Research, Occasional Paper Series 4*(2005), 1-67, available at, <http://www.hpcrresearch.org/pdf/>, (last accessed: August 1, 2016).

³²³Some scholars have taken the position that anyone who is not a lawful combatant is a civilian. The International Committee for the Red Cross (ICRC) Commentary on Geneva Convention IV (GCIV) indicates that it was the intention of the drafters of the Geneva Conventions to cover everyone within the ambit of the treaties, either as a prisoner of war or as a civilian. For details see, Marco Sassòli, “Use and Abuse of the Laws of War in the ‘War on Terrorism’, Law and Inequality” 22:2(2004), 195-221, available at, <https://archive-ouverte.unige.ch/unige:8494>, (last accessed: August 1, 2016).

³²⁴ The IHL defines the term hostilities as, “...the resort to means and methods of ‘injuring the enemy’, and individual attacks as being directed ‘against the adversary.’ 1. ...the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm), and For an act to be hostile, it must satisfy three tests: 2. ...there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation), and 6 3. ...the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus)²⁴ See CA 3 Geneva Conventions 1949; Article 51(3) Additional Protocol I. Common Article 3 of the Geneva Conventions employs the term ‘active’ rather than ‘direct’ as used in the Additional Protocols. The distinction between active and direct participation was discussed by ICTR in the *Akayesu* case which held that the terms are so similar that they should be treated as synonymous: *Akayesu*, para 629.

³²⁵The law of armed conflict faces issue regarding the question of what actions will amount to direct participation in hostilities. Like now-a-days the use of contractors, in particular, has increased as the combined effects of the technological revolution and ‘privatization through subcontracting’ have been used to ensure military power and reducing costs. For instance, in 2006 over 38,000 contractors were serving

The ICRC Interpretive Guidance provides that a civilian directly participates in hostilities when he when he (1) engages in an act that directly causes (2) harm of a sufficient gravity with (3) the intent of aiding a belligerent party.³²⁶ Application of each of these terms to cyber warriors raises difficult legal questions.

It is suggested that the persons involved maybe divided into following categories according to their functions:³²⁷

1. those who design and write the programs used for offensive or defensive Cyber warfare operations;
2. those who install these programs on the computer systems, act as service administrators ('webmasters') and provide technical maintenance for them; and
3. those who actually operate the computer programs in a cyber warfare.
4. Computer technicians, technical maintenance personnel and others who perform similar tasks.
5. 'Patriotic hackers' or 'hacktivists'.³²⁸

with coalition forces in Iraq in support functions from cleaners and cooks, with an additional 30,000 providing security for both the military and other contractors and guarding convoys and military installation. For details see, Michael N. Schmitt, "Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees", *Chicago journal of International Law* 5:2(2004), 511-525.

³²⁶ After six years of expert discussions and research, the ICRC has published the "Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law", which aims to clarify the meaning and consequences of direct participation in hostilities under international humanitarian law (IHL). Note that the Interpretive Guidance limits its interpretation of the notion of direct participation in hostilities for the purposes of the conduct of hostilities only. It does not address the consequences of direct participation in hostilities for detention and trial. See generally, ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, available at, <https://www.icrc.org/en/publication-interpretive-guidance-notion-direct-participation-hostilities>, (last accessed: August 2, 2016).

³²⁷ Crawford, "Virtual Battlefields: Direct Participation in Cyber Warfare", 121-143.

4.2.1 DPH in the Context of Cyber warfare

Apparently standards set by ICRC Interpretive Guidance shows that any civilian engaged in proactive, offensive cyber-attacks would no doubt be directly participating in hostilities. However, application of these standards seems difficult in reality.³²⁹

The notion of “hostility” is interpreted widely enough to encompass a large variety of acts. According to the ICRC’s Guidance:³³⁰

there was wide agreement that the causation of military harm as part of the hostilities did not necessarily presuppose the use of armed force or the causation of death, injury or destruction but essentially included “all acts that adversely affect or aim to adversely affect the enemy’s pursuance of its military objective or goal.

In other terms, “hostilities” is not synonymous to attack and cyber military operations that are below the threshold of an attack and could be considered as “hostilities”. According to the Tallinn Manual: “There is no requirement for physical damage to objects or harm to individuals. In other words, actions that do not qualify as a cyber-

³²⁸ People who are not part of their State’s armed forces but on their own initiative carry out attacks against perceived ‘enemy’ computer systems, without the authority and outside the control of their government but in pursuance of common political ends, it is suggested that the Russians who hacked into Estonian and Georgian websites in 2007–08 were ‘hacktivists’, as the Russian Government denied that they acted on its instructions. Schmitt, “Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees”, 511-525.

³²⁹ Crawford, “Virtual Battlefields: Direct Participation in Cyber Warfare”, 121-143.

³³⁰ Niels Melzer (ed.), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva: ICRC, 2009), 85.

attack will satisfy this criterion as long as they negatively affect the enemy militarily.”³³¹ From this point of view, it can be concluded that a wide range of cyber operations may fall under the scope of “hostilities.”

The interpretation of the expression “for such time” in a cyber-context is challenging, in particular, and needs to be clarified. Indeed, should we consider that civilians could be targeted only when they “press” the button or can they only be targeted when the cyber-operation is under-way.

4.2.2 Specific Cyber Warfare Activities as DPH

Table 2: Specific Cyber Warfare Activities as DPH³³²

CW activity undertaken by a civilian	Threshold of harm	Direct causation?	Belligerent nexus?	DPH?
Research for the development of CW programs generally	No—the research is in abstract.	No—no harm is actually Caused	No—the research is not tied to any particular conflict	No

³³¹ Michael N. Schmitt (ed.), *Tallinn Manual on the international Law applicable to Cyberwarfare* (New York: Cambridge University Press, 2013), 197, available at, <https://www.peacepalacelibrary.pdf>, (last accessed: January 28, 2017).

³³² David Turns, “Cyber warfare and the Notion of Direct Participation in Hostilities”, *Journal of Conflict & Security Law* 2012, available at, <http://jesl.oxfordjournals.org>, (last accessed: January 25, 2017).

Design/writing of a specific CW program	No—any eventual harm that might result is too remote	No—any eventual harm that might result is too remote	Yes, potentially, if research takes place with a specific future target or conflict in mind	No
Installation of a CW program on a computer system	Yes—the program cannot be used to cause the harm unless it is installed	No—any eventual harm is too remote from the installation	Yes, if imminent use is intended	No
Exploitation of a vulnerability on a target State system by introduction of a hostile agent that does not damage it immediately but that can be directed to cause damage subsequently	Yes—introduction of the hostile agent is what eventually causes the harm; time lapse irrelevant	No, if separate autonomous action is required to activate the agent; yes, if activation is pre-programmed by the same person; time lapse relevant	Yes—intention is clearly hostile	No/ Yes
Dictation or written provision, to a combatant, of the precise set of commands needed to activate the hostile agent	Yes—harm would not occur but for provision of the commands	Yes—activation is caused directly by the input of the commands	Yes—intention is clearly hostile	Yes

Personal entry, by the civilian, of the precise set of commands needed to activate the hostile agent	Yes—activation of the agent causes the harm	Yes—activation is caused directly by the input of the commands	Yes—intention is clearly hostile	Yes
--	---	--	----------------------------------	-----

These cyber situations can be categorised in the following cyber warfare scenarios:

1) **A civilian who is contracted by the armed forces of another party to the conflict to write malicious code or otherwise engage in a Cyber warfare:** This scenario strongly resembles the case in where civilians are used to pilot drones in targeted killing strikes.³³³ The ICRC IG addresses this topic on civilians and DPH stating:

...as long as they are not incorporated into the armed forces, private contractors and civilian employees do not cease to be civilians simply because they accompany the armed forces and or assume functions other than the conduct of hostilities that would traditionally have been performed by military personnel A different conclusion must be reached for contractors and employees who, to all intent and purposes, have been incorporated into the armed forces of a party to the conflict, whether through a formal procedure under national law or de facto by being given a continuous combat function . . . Such personnel would be

³³³ David S. Cloud, "Combat by Camera: Civilian Contractors Playing Key Roles in U.S. Drone Operations," *The Los Angeles Times*, December 30, 2011.

members of an organised armed force, group or unit under a command responsible to a party to the conflict and . . . would no longer qualify as civilians.³³⁴

2) Civilians Engaged in Cyber-Attack Independently: Civilians who are engaged individually in hostile cyber-attacks without instruction of the armed forces or another party to the conflict would DPH if it amount to an attack under IHL. Because any act carried out by such persons with the “intent or effect of rendering the targeted networks vulnerable or inoperative”³³⁵ have directly participated in the same way as if they were conducting a “traditional” attack for instance, hampering a military base, aircraft, navy vessel or any other military target. However, in case of cyber-attacks on Georgia in 2008 would not amount to DPH as they were carried out merely for disrupting networks and gathering information.³³⁶

3) A civilian who writes malicious code or another malware program and gives it to the armed forces or some other party to the conflict: This scenario can be related to the acts done by someone who creates the mechanism through which a destructive act is executed but is not involved beyond the construction phase. Therefore, it would not amount to DPH, because the “causation test” would not be fulfilled. And ICRC IG states that “individual conduct that merely builds up or maintains the capacity of a party to harm its adversary . . . is excluded from the concept of direct participation in hostilities . .

³³⁴ Nils Melzer. “Interpretative Guidance On the Notion of Direct Participation in Hostilities Under International Humanitarian Law”. *International Review of the Red Cross* 90:872(2008), 1010-1011.

³³⁵ Crawford, “Virtual Backgrounds: Direct Participation in Cyber Warfare”, 1-19.

³³⁶ Ibid., this scenario can be related to IAC between Georgia and Russia in 2008. The cyber-attacks that happened there were mostly for the purposes of disrupting networks and gathering information.

. . . Examples of non-DPIH include scientific research and design, as well as production and transport of weapons and equipment.”³³⁷

4) **A civilian who writes or deploys malware for criminal use only:** No need to mention that all cyber-attacks are not targeted towards an armed conflict. Some hackers hack banks and financial institutions for money or they target sites and networks for the purpose of recreation.³³⁸ In such a case it is dealt via domestic law and not IHL. However, this situation can be quite complicated when a civilian engaged in a cyber-attack during an armed conflict, as his attacks would be hard to distinguish from attacks being conducted by civilians who do have a nexus with the conflict and will put himself at risk of being targeted.

5) **A civilian who affords technical support to a person involved in cyber hostilities:** It means a civilian who is involved in cyber hostilities and is confronted with a technical problem that he or she could not solve might ask for help from someone else, for example

³³⁷Melzer, “Interpretative guidance On the Notion of Direct Participation in Hostilities Under International Humanitarian Law”, 1021-1022. However, the IG stated that there were many discussions on this topic and that opinions were divided as to civilian scientists and weapons experts could always be considered to be taking no direct part in (cyber) hostilities in such a way as described above. Some of the experts argued that constructing explosive devices could be considered to a measure that is “preparatory to a concrete military operation”. It wouldn’t just be pure capacity building, it would’ve exceeded that and would go on to constitute as an integral part of a military operation. However, the other experts argue that such a strict criterion would prevent the criterion in becoming too broad. The approach of the IG was still to require direct causation of harm in the strict sense but to extend that perspective with regard to causing the harm. So instead of focussing solely on the specific act carried out by the civilian, it was pointed out that direct causation still existed when the required harm was directly caused by a concrete and coordinated military operation of which that act contributed in integral part. The act in question must thus be a part of the military operation and not merely a contribution to it. The threshold of harm can be reached if the program also really intends - and is designed - to cause harm but the harm that could bring it would be too remote unless if the person who writes the code also conducts the attack; then there would be no intermediary between the code and its activation. For details see, Turns David. “Cyber warfare and the notion of direct participation in hostilities.” *Journal of Conflict and Security Law* 17:2(2012), 295-310.

³³⁸CNN.com, “Timeline: A Forty Year History of Hacking,” CNN Tech, <http://edition.cnn.com>, (last accessed: January 28, 2017).

an external contractor. Whether such a contractor is participating in hostilities as well or DPH applies automatically when the contractor's hands touched the computer or after he or she has fixed the technical problem or only if the civilian who is engaged in the cyber hostilities mentioned to the contractor what he or she was doing. And only after that explanation mean that the contractor was directly contributing in cyber hostilities.³³⁹ The answer to all these queries is NO! Because such a person will not fulfil cumulative criteria required for the DPH given by the ICRC.

Other actions that could amount to DPH in cyber warfare are the exploitation of a vulnerable targeted State's cyber system by introducing a hostile agent that damages it directly, a dictation of the precise set of commands needed to activate the hostile agent and personal entry by a civilian of the precise set of commands to activate the hostile agent.³⁴⁰ Some military thinkers assert that a cyber-attack is considered as DPH in cyber hostilities when a civilian used a cyber-attack to shut down an air defence station. Such a person may deliver the weapon through the host country's internet or possible "beam" the

³³⁹ When looking at the ICRC guidance and the ruling of the Israeli Supreme Court on the Targeted Killings case it would conclude that such a support, be it technical or logistics, would be too remote to amount to direct participation in (cyber) hostilities. Even if the contractor would know about the civilian's cyber-attack and was even on board about engaging in a cyber war and even if he or she encouraged the civilian to destroy as much what was possible then still the contractor would be a mere enthusiastic supporter shouting from the (war infused) sidelines. He or she would not fulfil cumulative criteria required for the DPH-test as formulated by the ICRC. This in turn was agreed by other scholars that conduct like this would be too remote for the purposes of the threshold of harm and the criterion of causation.³³⁹ That is because computers require technical support and for a long basis of time. Simply because of their technical nature, they need on-going maintenance. Even when there is no conflict going on. The contractor's conduct could amount to: "...individual conduct that merely builds up or maintains the capacity of a party to harm its adversary . . . [and thus] is excluded from the concept of direct participation in hostilities." However not all scholars agree with the ICRC on this point. Some scholars have argued that direct participation includes not only activities involving the delivery of violence, but also acts such as described in this scenario; aimed at protecting personnel, infrastructure, or material. See for example, François Quéguiner, "Direct Participation in Hostilities under International Humanitarian Law," International Humanitarian Law Research Initiative Briefing Paper", November 2003, available at: <http://reliefweb.int/pdf/>, (last accessed on January 27, 2017).

³⁴⁰ David, "Cyber warfare and The Notion of Direct Participation in Hostilities", 295-310.

weapon to the target directly from an aircraft. Proper execution of such a cyber-strike would be the same as a bombing raid.³⁴¹

Hence, it can be argued that Computer technicians, technical maintenance personnel and others who perform similar task qualify under the inclusion of the category of “persons who accompany the armed forces without actually being a member thereof”.³⁴² Civilians who write codes and do research for the development of cyber war programs in general would also not fall under the notion of DPH. There would be no causal harm and there will be no point of reaching the threshold of harm.³⁴³

Similarly, the mere installation of a cyber-war program on a computer system would also not amount to DPH. Here the direct causation criterion would also not be fulfilled; it would be too remote for the installation. Just the identification of vulnerability in a targeted state’s system would in itself cause no harm and it still requires more action to exploit the vulnerability before the real harm can be done. It however does have a nexus with the conflict so if imminent exploitation would be intended then this situation could amount to DPH.³⁴⁴

Furthermore, if one considers the cyber-attacks on Estonia in 2007 and the cyber-elements of the Russia–Georgia conflict in 2008 (assuming in both cases that they were

³⁴¹ Kelsey, “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in The Age of Cyber Warfare”, 1434-1449.

³⁴² Because they keep the machines in order and they themselves don’t undertake the attack nor can they be held accountable for it because of the direct causation criterion. It would in itself cause no harm and routine maintenance does not in itself cause any direct harm nor would it have a nexus with the conflict: routine maintenance is irrespective of its use in conflict. Schmitt, “Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees”, 511-525.

³⁴³ Simply researching would not be tied to any particular conflict; the research itself has been done *in abstracto*. Schmitt, “Humanitarian Law and Direct Participation by Private Contractors or Civilian Employees”, 511-525.

³⁴⁴ Woltag, *Cyber Warfare: Military Cross-border Computer Network Operations Under International Law*, 207.

perpetrated by civilians and not members of the Russian armed forces), it must be concluded that in neither case the acts in question would have amounted to DPH as they would have failed to meet criteria mentioned in ICRC Interpretive Guidance.³⁴⁵ On the other hand, the apparent use of the Stuxnet worm to target Iranian centrifuges used for the enrichment of uranium in 2010 would have amounted to DPII (had it occurred in a situation of armed conflict, which it did not), because it resulted in physical damage to the centrifuges.³⁴⁶

Conclusions

It is concluded that the increased civilization along with high-tech means and methods of warfare has raised some interesting challenges in determining combatant status under IHL, particularly, the law requiring distinction between civilian and combatant. One of the reasons for it may be the decreased relevance of time and distance to the battle field and the other is creation of virtual environment. As far as application of DPH to cyber warfare is concerned, it is observed that the three constitutive elements of DPH are cumulative and the threshold for reaching all three is quite high. The easiest of these

³⁴⁵ As to generalities, the 'military harm' required by the 'threshold of harm' criterion is explained broadly as including 'essentially any consequence adversely affecting the military operations or military capacity of a party to the conflict'. Absent specific military harm to the adverse party, 'a specific act [constituting DPH] must be likely to cause at least death, injury or destruction'; thus, the causing of mere inconvenience, however unpleasant, would not be sufficient. It should of course be remembered that in the Estonian case there was no actual situation of armed conflict under IHL, whereas in Georgia there was. The attacks on Estonian computers caused large-scale inconvenience in what is one of the most 'wired' countries in Europe, due to administrative, financial and social chaos when vital public computer systems went down, but there is no evidence that a single person died or was injured, or that any property was damaged or destroyed, as a direct result. In Georgia the impact was somewhat less, largely because the country is less computer reliant than Estonia for its public administration and banking systems; it appears to have been largely limited to propaganda effects (the website of the Georgian Presidency was defaced, for example). It would therefore have been a fortiori the case that in this instance there was no DPII.

³⁴⁶ Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield", 1-29.

elements to satisfy is belligerent nexus, which is because cyber warfare is such a specialized activity that almost any act, it naturally causes, would be intended to support an intended cyber-attack. While the hardest to satisfy is direct causation. The most adjustable element but in practice likely to be the crucial one, is the threshold of harm. However, despite of these challenges, the need of the time is that a view must be reached as to the delineation of a fine line between legitimate and direct participation. So that civilians not mistakenly surrender their rights to protection.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

Almost all IHL treaties are mentioned as “One war behind reality” due to that reason massive suffering and injuries occurred in history of mankind. In plain words, since 150 years of IHL, almost all treaties were stipulated after occurrence of war or armed conflict. There is neither binding legal instrument to govern and deal with cyber warfare nor any organized legal framework under International Law to punish the alleged perpetrators of cyber warfare. As a result of this gap, the international community so far witnessed several cyber incidents that could be cited as good indicators of how the issue is becoming a serious concern of the world community coupled with lenient and unregulated law on cyber warfare.

It appears that cyber-attacks have not yet been used to cause direct, physical destruction and loss of life like other autonomous weapons. However, example of cyber-attacks shows that it could continually infiltrate lives of civilians. Because if cyber-attack could alter the speed of centrifuges to take them out of commission, then it is not unrealistic to think that they may have started an internal fire, potentially causing widespread loss at the facility.

Major findings of the research reveals that one of the challenges that States face in the cyber environment is the scope and manner of IHL's applicability to cyber warfare and characterization of it as armed conflict.

The dichotomous division of armed conflict is complicated by cyber warfare, which, by its very nature, defies the concepts of national borders, territorial control and traditional military organization. The international/ non international distinction is also problematic in the cyber realm, where anonymity is the rule: difficulties in identifying the actor behind a cyber-operation present an obstacle to attributing the relevant hostilities to a State or non-State actor. Furthermore, whether or not the threshold of armed conflict has been reached is complicated by cyber operations, which have far reaching but non-physical consequences.

The principle of distinction presents some immediate problems for cyber warfare. Firstly, there is a serious extent to which much of the internet is dual-use, and is used by both military and civilian actors. It would therefore be impossible to adhere to the principle of distinction whilst attacking aspects of internet infrastructure. Secondly, the use of viruses and worms can be inherently indiscriminate, due to their uncontrollable behavior (despite attempts to control this in worms like Stuxnet). Thirdly, it is difficult to discriminate between military attacks and non-military attacks, without over burdening military forces with the use of identifiable IP address so as to indicate that they are legitimate targets.

Respect of the principle of proportionality amounts to evaluating the 'collateral damage' caused by an attack, ensuring the protection of civilians and civilian objects. This thesis focused on two aspects. Firstly, cyber-attacks can have indirect effects as well

as unexpected consequences, which can be hard to predict. Secondly, the “dual-use” functions of the internet, such that it is both military and civilian.

The use of cyber means to conduct an armed attack can be less harmful, compared to traditional kinetic methods: in contrast to regular weapons that destroy the military target, a cyber-attack may simply ‘turn it off’, or prevent it from operating properly. Principle of precaution faces three main challenges when applied to cyber warfare. Firstly, due to the interconnectivity of the cyber realm, it is difficult for commanders to maintain situational awareness to take the necessary precautions. It can also be difficult to suspend or cancel an attack if there is a risk that it will affect civilians. Secondly, the ‘perfect cyber weapon’ would take years to create, and would be usable only once. There are further challenges as to the possibility of properly testing cyber weapons in an accurate, reliable testing space, in order to properly ascertain their effects. Lastly, due to the interconnectedness of the internet, a party to an armed conflict would have difficulties segregating military objects and civilian objects and to protect civilian objects.

As far as application of combatant’s status and civilians DPH is concerned in the context of cyber warfare, they need particular interpretation. And same is the case with perfidy and principle of military necessity due to complex nature of cyber realm, thus, making IHL ill-adapted to cyber warfare.

Recommendations

To Academia

- There should be a comprehensive and well organized International legal machinery to govern cyber warfare. At the same it is necessary to provide a valid and universal definition to the concept of cyber warfare and cyber-attack that can trigger application of IHL. And to do this on a legal standpoint, it is necessary to identify the purpose of its use, the context in which it is used, the subject/object that offends, and of course the target of the attack.
- The notion and bifurcation of armed conflict under IHL need to be reviewed and interpreted to accommodate new forms of conflicts. Particularly requirement of the level of intensity and organized armed group due to non-physical and covert nature of cyber-attacks.
- Since large part of IHL is based on the provisions of the Geneva Conventions and their customary counterparts so that some of the fundamental principles like principle of military the principle of distinction and the principle of proportionality and combatants' status be amended or revised to accommodate cyber warfare in IHL expressly. Thus, the researcher recommends that the notion of object, attack, military objectives and damage should be interpreted in the light of non-physical consequences of cyber-attacks for application of IHL on cyber warfare. And with regard to objects having dual purpose that is military as well as civil use effective assessment should be made in light with principle of proportionality to minimize the potential impact on civilians.

- With regard to targetable individuals, the status of cyber combatants and the notion of direct participation in cyber hostilities are underdeveloped legal concepts and need particular interpretation in the context of cyber operations. For this “Functional continuous combat test” should be used to ascertain the challenge of civilian’s participation in hostilities. And to check whether certain civilians are part of armed forces by the nature and purpose of their activities or not.
- Rules should be established for cyber warfare to be used in disputed situations for instance interconnected networks that are both military objectives and necessary for survival of population.

To The World Governments

- First, the world’s governments to come together, affirm international cyber-security norms that have emerged in recent years, adopt new and binding rules and get to work implementing them. Second, governments around the world should pursue a broader multilateral agreement that affirms recent cyber-security norms as global rules. Just as the world’s governments came together in 1949 to adopt the Fourth Geneva Convention to protect civilians in times of war, we need a Virtual Geneva Convention that will commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace and conflict. Such a convention should commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property. Similarly, it should require that

governments assist private sector efforts to detect, contain, respond to and recover from these events.

To Monitoring Organs

- From monitoring organs point of view, there are no centralized monitoring mechanisms to govern cyber warfare so far only NATO have come with Tallinn manual to govern it but follow up its respective regions and members. There should be United Nation Special body for Cyber Affairs to come up with centralized monitoring organ.

To Technical Experts

- Increased cooperation and information sharing at the technical level could also indirectly help solve one of the most challenging issues in the cyber security realm, namely the problem of attribution which would ultimately help in categorization of cyber warfare as armed conflict. Correctly identifying the author of a cyber-attack is extremely complex, and in many cases may not be possible at all. Much has been said, especially in military circles, about developing a system that will promptly locate the perpetrators of an attack, but it seems unlikely that a technical solution will appear anytime soon.

ANNEXTURE

Selected Case Studies

Lithuania 2008

Massive cyber operations were carried out against Lithuania in June 28, 2008 by using communist symbols and anti-Lithuanian speech to damage at least 300 private and government websites. On the same an amendment prohibiting the use of several soviet and communist symbols was to be adopted by Lithuanian Parliament.³⁴⁷ This provoked the strong pro-Russian opposition, thus, suspicion was raised towards Russia being responsible for the cyber operations. The effects of the attack were not grave since most of the websites were restored within four days.³⁴⁸ It has to be investigated whether these cyber operations, could have qualified as or triggered an AC due to absence of existing armed conflict. Any analysis in this case should be based on the harm that could have been caused. To proceed further the very first thing would be to see whether the cyber operations amounted to a cyber-attack since the element “armed” is the common criterion between an IAC and a NIAC. In the absence of any damage, destruction of object, injury, death or severe suffering of individuals, it is submitted that the threshold of harm is not

³⁴⁷ Kaska Encken. Tikk, “International Cyber Incidents: Legal Considerations”, *Cooperative Cyber Defence Center of Excellence* (2010), 51-65, available at, <https://cedcoe.org>, (last accessed: July 20, 2016).

³⁴⁸ Döge, Cyber Warfare. “Challenges for the Applicability of the Traditional Laws of War Regime”. 486-501.

met.³⁴⁹ Moreover, the means of the cyber operations, like the defacement of websites, merely substitution of the content of a website and, therefore, in the Lithuanian case it must have caused mere inconvenience which by itself is not adequate to claim that a cyber operation amounts to a cyber-attack. Hence, it is observed that the Lithuanian cyber operations do not amount to a cyber-attack and one of the criteria for existence of an IAC or a NIAC is not met. Since they have to exist all together thus, there is no need to investigate the rest of the criteria.

Georgia 2008

Georgia faced cyber campaign in August 2008.³⁵⁰ These cyber operations were launched just before the Russian military invasion in South Ossetia and Georgia as a result of Georgian attack against separatist groups acting in South Ossetia.³⁵¹ The President's website was disrupted for a whole day. Government and all pro Georgian websites were disrupted for information and defaced on August 8. The perpetrator of it is unknown as Russia ruled out its involvement but, nevertheless, computer experts claimed to have witnessed the installation of multiple bots³⁵² within one month of its initiation the cyber operations were brought to an end.³⁵³

³⁴⁹ Furthermore, the hackers were reportedly aiming at simply trying to instigate individuals to spread the campaign and not cause any kind of harm. government websites remained unaffected due to strong defenses. Eneken. Tikk, "International Cyber Incidents: Legal Considerations", 51-65.

³⁵⁰ Ibid., 52.

³⁵¹ Ibid.

³⁵² Bots "in the context of cyber warfare refers specifically to a parasitic program that hijacks a networked computer and uses it to carry out automated CAs on behalf of a hacker", for more information, Cyberwarfare: A Glossary of Useful Terms, available <https://www.stratfor.com/analysis/cyberwarfare-glossary-useful-terms>, (last accessed: July 21, 2016).

³⁵³ John Markoff, "Before the Gunfire, Cyber Attacks", <http://www.nytimes.com/2008/08/13/13>, (last accessed: July 21, 2016).

It seems that the threshold of harm is not met in the given case. Firstly, the most prominent means of cyber operations was the defacement of websites which, as pointed out in the Lithuanian case, does not cause irreparable damage or destruction of an object nor causes any other required results. One could not neglect the fact that defacement of the websites could contribute to the severe mental suffering of the population. At the same time, it has to be underlined that only 7 percent of the Georgian population had access to Internet during this time which shows that such society is not dependent on the Internet.³⁵⁴ In conclusion, the cyber operations against Georgia cannot qualify as a cyber-attack. Thus, there is no need to investigate the rest of the criteria of IAC or NIAC since they have to exist side by side.

Stuxnet 2010

In 2010, Iran's nuclear power plant was attacked with the deployment of a worm called Stuxnet. It was a unique piece of malware due to its unique structure and aspects.³⁵⁵ Stuxnet could be activated only when a number of specific circumstances were present and its objectives were more than explicit: on the one hand, it instructed uranium centrifuges to run at a different pace, which caused damages to the centrifuges and the process of uranium enrichment. On the other hand, it sent false signals that the system works properly through the usage of certificates of two widely known companies.³⁵⁶ To

³⁵⁴ Linaki, "Cyber warfare and International Humanitarian Law: "A Matter of Applicability", 175.

³⁵⁵ Jerrard Shearer, W32.Stuxnet, http://www.symantec.com/security_response/writeup.jsp?docid=071400, (last accessed: July 21, 2016).

³⁵⁶ For more details, Jeremy Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?", *Fordham International Law Journal* 35 (2012), 849-852.

get know how of the perpetrators, several clues, such as the time and resources are needed for such a complex worm to be created.³⁵⁷

Large scaled damage of around 1000 centrifuges was observed, a fact which shows that not only financial and technical means have to be employed for the repair of the damage but also considerable time and human effort are needed for the repair of the damage.³⁵⁸ Besides that, the graveness of the damage can be proved by its long-term effect since it is estimated that the completion of Iran's nuclear power program was delayed approximately for two years.³⁵⁹ Moreover, the cyber operation targeted computer data on which physical objects were dependent. Interference with and manipulation of such data resulted in a large scaled damage and destruction of objects. It can be assumed that the given cyber operation seems to have reached the required threshold of harm.

Although no one has openly claimed responsibility for the Stuxnet cyber-attack, but such worm could not have been created without the support and involvement of one or more states. Based upon this analysis, the Stuxnet incident could be assumed to trigger an IAC.

US 2013

In 2013, a set of cyber operations against US energy companies was reported but were intended only for information gathering.³⁶⁰ No damage was reported but, according to US officials, the hackers could have manipulated physical equipment and the

³⁵⁷ Ibid.

³⁵⁸ Richardson, "Stuxnet as Cyberwar: The Law of War and the Virtual Battlefield", 1-29.

³⁵⁹ Ibid.

³⁶⁰ Siobhan Gorman and Danny Yadron, "Iran Hacks Energy Firms, U.S. Says" *The Wall Street Journal*, (2013), available at, <http://online.wsj.com/10802>, (last accessed: July 21, 2016).

information gathered might be used in future operation to cause great damage.³⁶¹ Moreover, US officials are quite sure that Iran has provided the hackers with support and instruction. Perhaps, it will be interesting to see the evolution of such cyber operations since, in combination with the Stuxnet case; it could constitute the only case of an IAC triggered.

³⁶¹ Yadron, "Iran Hacks Energy Firms, U.S. Says".

- Goldsmith Jack, "How Cyber Changes the Laws of War". *The European Journal of International Law* 24:1(2013), 129-138.
- Gosnell, Handler S. "The New Face of Battle: Developing A Legal Approach to Accommodate Emerging Trends in Warfare". *Stanford Journal of International Law* 48(2012), 233-250.
- Hathaway, Oona A and Rebecca Crotof. "The Law of Cyber-attack". *California Law Review* 100 (2012), 817–885.
- Herr Trey. "Prep: A Framework for Malware & Cyber Weapons". *Journal of Information Warfare* 13:1(2013), 23-33.
- Jensen Talbot Eric. "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations". *American University International Law Review* 18(2002–2003), 1149-1250.
- Kelsey, Jeffrey T. G. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare". *Michigan Law Review* 106(2008), 1439.
- Kerschischnig. *Cyber threats and International Law*. The Hague: Eleven International, 2012.
- Kilovaty Ido. "Cyber warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare". *National Security Law Brief* 5:1 (2014), 91-124.

Kodar Erki, "Applying The Law of Armed Conflict to Cyber Attacks: From The Martens Clause to Additional Protocol I". *Stanford Journal of International Law* 38(2002), 207-217.

Kovacs Anja. "Cyber Security, Cyber Surveillance and Online Human Rights". *International Journal of Cyber Warfare and Terrorism archive* 6:2(2013), 32-40.

Lin Herbert. "Cyber Conflict and International Humanitarian Law". *International Review of the Red Cross* 94:886(2012), 515-531.

Luff Charlotte. "International Humanitarian Law in Times of Contemporary Warfare: The New Challenge of Cyber-attacks and Civilian Participation". *Journal of International Law of Peace and Armed Conflict* 26:2(2013), 74-82.

Melzer Nilz. "Cyber Operations and Jus in Bello". *Disarmament forum* 4(2011), 3-18.

Michael Gervais. "Cyber-attacks and the Laws of War". *Berkeley journal of international law* 30:2(2012), 525-579.

Papanastasiou Afroditi. "Application of International Law in Cyber Warfare Operations". *Social Science Research Network* 3(2010), 31-57.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on A Normative Framework". *Columbia Journal of Transnational Law* 37(1999), 35-40.

_____. "Classification of Cyber Conflicts", *International law Studies*, 89(2013), 240-258.

- _____. "War, Technology, and International Humanitarian Law". *Harvard University Program on Humanitarian Policy and Conflict Research, Occasional Paper Series 4* (2005), 43-60.
- _____. "Wired Warfare: Computer Network Attack and Jus in Bello". *International Review of the Red Cross* 84:846(2002), 367-377.
- Sean David S. "Policing Cyber-crime, Situating the Public Police in Networks of Security within Cyberspace". *Police Practice & Research: An International Journal* 8:2(2010), 183-205.
- Solce Nathasha. "The Battlefield of Cyber Space: The Inevitable New Military Branch – The Cyber Force". *Albany Law Journal of Science and Technology* 18 (2008), 293-300.
- Swanson Lesley. "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict". *Loyola of Los Angeles International and Comparative Law Review* 32:2(2010), 303-333.
- Taddeo Mariarosaria. "Information Warfare: The Ontological and Regulatory gap". *APA Newsletter on Philosophy and Computers* 14:1(2014), 13-20.
- Todd, Graham H. "Armed Attack in Cyberspace: Detering Asymmetric Warfare with an Asymmetric Definition". *The Air Force Law Review* 64(2009), 65-102.
- Watts Sean. "Combatant Status and Computer Network Attack", *Virginia Journal of International Law* 50:2(2010), 391-417.

Books

- Andres Jason, Winterfed Steve. *Cyber Warfare: Techniques, Tactics and Tools for Security*. Boston: Syngress/Elsevier, 2011.
- Banks, William C. *New Battlefields, Old Laws: Critical Debates on Asymmetric Warfare*. New York: Columbia University Press, 2011, 308.
- Brown Ian. *International Law and the Use of Force by States*. UK: Clarendon Press, 1969.
- Carr Jeffery. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Cambridge: O' Reilly Publishers, 2009, 7.
- Crowe Jonathan. *Principles of International Humanitarian Law*. UK: Edward Elgar Publisher, 2013.
- Deibert, Ronald RohozinskiRafal. *Cyber Space and Coming Crises of Authority*. Oxford: MIT Press, 2011.
- Dinniss Harrison Heather. *Cyber warfare and the Laws of War*. UK: Cambridge University Press, 2012.
- Green A James. (ed.). *Cyber Warfare: A multidisciplinary analysis*. New York: Routledge Publishers, 2015.
- Pilloud Claud. et al. *Commentary on the Additional Protocols of 8 June 1977*. Geneva: Martin Nijhoff, 1987.

Saxon Dan. *International Humanitarian Law and the Changing Technology of War*. Brill: Martinus Nijhoff, 2013.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge, 2013.

Wexler Chuck. "Cybercrime: A New Critical Issue" in *The Role of Law Enforcing Agencies in Preventing and Investigating Cyber-crimes*. USA: Police Executive Research Forum, 2014.

Woltag, Johann Christoph. *Cyber Warfare: Military Cross-Border Computer Network Operations Under International Law*. Cambridge: Intersentia Publishing Limited, 2014.

Statutes and Treaties

Charter of United Nations Organization 1945.

Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949.

Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea 1949.

Geneva Convention (III) relative to the Treatment of Prisoners of War. Geneva, 1949.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War. 1949.

Hague Regulations (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.

Protocol Additional to the Geneva Conventions 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 1977.

Web Links

<http://isis-online.org/isisreports/detail/djd-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>.

<http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace>.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001794.

<http://www.cfr.org/international-law/hague-conventions-1899-1907/p9597>.

http://www.esoonline.com/article/216991.Coleman_The_Cyber_Arms_Race_Has_Begun?page.

<http://www.fas.org/sgp/crs/natsec/RL3J787.pdf>.

<http://www.iipreport.com/default.asp?Mode=Show&A=1421&R=VI>.

<http://www.merriam-webster.com/dictionary/war>.

http://www.unidir.org/files/publications_pdfs/confronting-cyberconflict-en-317.pdf.

<https://www.icrc.org/en/international-review/article/editorial-quest-humanity-150-years-international-humanitarian-law-and>.

<https://www.icrc.org/en/war-and-law/treaties-customary-law/geneva-conventions>.

www.jesl.oxfordjournals/content/short.