INTERNATIONAL HUMANITARIAN LAW ON CYBER WARFARE AND PAKISTAN'S LEGAL REGIME

A Thesis submitted in partial fulfillment of the requirement for obtaining the degree of
MASTER OF LAWS
(LLM International Law)

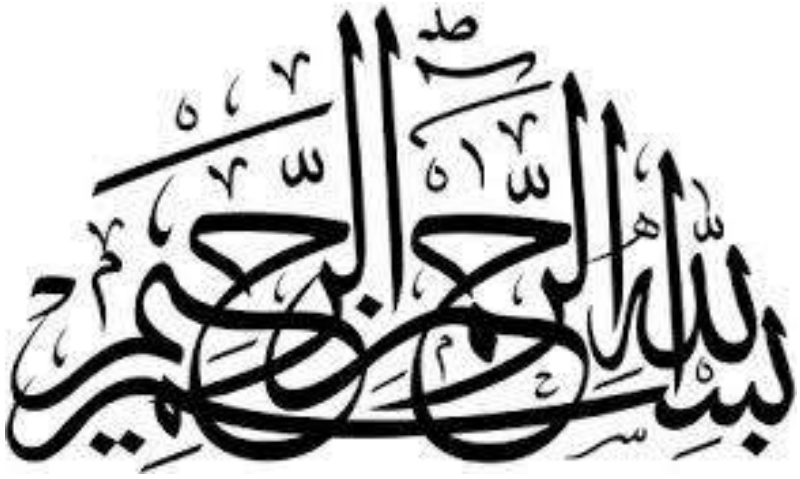
By

KHALIDA BIBI
Registration No: 407-FSL/LLMIL/S20
Degree Program: LLM International Law

Supervisor:
DR. AMBREEN ABBASI
Lecturer in Law

Department of Law
Faculty of Shariah and Law
International Islamic University Islamabad

November 2023


بسم الله الرحمن الرحيم

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD

FACULTY OF SHARIAH AND LAW

****

FINAL APPROVAL

It is certified that we have read and evaluated the Thesis titled as "**International Humanitarian Law on Cyber Warfare and Pakistan's Legal Regime**", submitted by **Ms. Khalida Bibi (Reg No. 407-FSL/LLMIL/S20)** as a partial fulfillment for the award of the degree of **Masters of Law (LLM International Law)**. This Thesis fulfills the requirements in its scope and quality for the award of the degree.

Dr. Ambreen Abbasi
Lecturer in Law
International Islamic University Islamabad _____
(Supervisor)

Ms. Beenish Aslam Sheikh
Lecturer in Law
International Islamic University Islamabad _____
(Internal Examiner)

Dr. Adnan Khan
(External Examiner) _____

DECLARATION

I hereby declare that this thesis titled as "**International Humanitarian Law on Cyber Warfare and Pakistan's Legal Regime**", is my own work, and further that, it contains no such text or material which had already been published by some other person previously, nor a substance already approved for the award of any degree of any university of institute for a Higher Learning, provided that a reference has been made in the paper.

Khalida Bibi

FORWARDING SHEET

The thesis entitled as "**International Humanitarian Law on Cyber Warfare and Pakistan's Legal Regime**," submitted by **Ms. Khalida Bibi**, for the partial fulfillment of the requirement of the degree of **Master of Laws (LLM International Law)** has been completed under my guidance and supervision. I am contented and greatly satisfied with the quality of student's research work and therefore recommend its submission.''

Dr. Ambreen Abbasi

DEDICATION

This thesis is dedicated to my beloved father Tahir shah, mother Raffat Tahir and my husband Sheraz Ahmad, for their endless love, support, and encouragement, without which I could not achieve this milestone.

ACKNOWLEDGMENT

Firstly, praises be to Allah S.W.T for His showers of blessings during my whole research. I thank my supervisor Dr. Ambreen Abbasi, Lecturer in Law Department of Law, Faculty of Shariah and Law, International Islamic University, Islamabad, for providing me this important opportunity to carry out my research and her guidance that has made my research possible. It was indeed a great advantage for me to work and study under her supervision. I am very much thankful for all her help and guidance. I am thankful to all my college fellows at International Islamic University, Islamabad for their suggestions and feedbacks. Finally, I pay thanks to my family and specially my husband who encouraged me during my whole research.

Khalida Bibi

ABSTRACT

Cyberwarfare is an increasingly common and dangerous feature of international conflicts. But right now the combination of an ongoing cyberwarfare arms race and a lack of clear rules governing online conflict means there is a real risk that incidents could rapidly increase and become out of control. In the 21st century, cyber-warfare joined to war terminology and described as a fifth combat zone. Even though there are many definitions for cyber-warfare since there isn't any peace treaty for it, it's hard to describe which malicious activities are considered as cyber-warfare. The most critical uncertainty is the edge for seeing a digital episode as the use of power. Pakistan current cyber-security framework is not sufficient to tackle the emerging threats of cyber warfare and to protect the state from these attacks. Pakistan is particularly vulnerable to cyber threats and ranks 14 out of 18 states in the Asia-Pacific region. The existing Electronic Transaction Ordinance, PEC Act are insufficient to overcome cyber-defense capabilities so, in order to improve Pakistan cyber- security and its defense system some legislation on domestic and international level needs to be formulated. There is a need of improving digital literacy across Pakistan so that individuals can protect their own data from cyber-attacks by signifying that the data belongs to them only. Cyber-warfare is although a new but not entirely separate component of a multidimensional conflict environment. In cyber-warfare victory and defeat are recognizable in. Subsequently, the same rules of international humanitarian law can be applying to it also as it cannot be distinguishing from other physical domain conflicts as it is not a discrete phenomenon, meaning thereby that cyber-warfare must be conducted and inhibited by the values, rules and norms of a state and by those prohibitions that a state apply to conventional warfare.

ABBREVIATIONS

AP	Additional Protocol
APT	Advanced Persistent threat
CCU	Cyber Capacity Unit
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIHL	Customary International Humanitarian Law
CISA	Cybersecurity and Infrastructure Security Agency
COE	Council of Europe
CW	Cyber Warfare
CYCON	International Conference on Cyber Conflict
ETO	Electronic Transection Ordinance
FBI	Federal Bureau of Investigation
FIA	Federal Investigation Agency
GCI	Global Competitiveness Index
IAC	International Armed Conflict
ICRC	International Committee of Red Cross
ICT	Information and Communication Technology
IHL	International Humanitarian law
IISS	International Institute for Strategic Studies
ISC2	International Information System Security
ISP	Internet service providers
ISR	Interrupt Service Routine
IT	Information Technology
ITU	International Telecommunication Union
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
NCCS	National Center for Cyber Security
NCSA	National Cyber Security Agency
NCSC	National Cyber Security Center
NDU	National Defense University
NIAC	Non-International Armed Conflict
NR3C	National Response center for Cyber Crime
NSA	National security Agency
PECA	Prevention of Electronic Crimes Act
PISA	Pakistan Information Security Association
POD	Point of Delivery
PTA	Pakistan Telecommunication Authority
UN	United Nations
WMD	Weapon of Mass Destruction

TABLE OF CONTENTS

THESIS STATEMENT

Pakistan is bound by existing humanitarian law on cyber-warfare but certain loopholes in its cyber-security system exists which need to enforce a new mechanism to tackle the emerging threat of cyber warfare.

INTRODUCTION

Cyber-technology has witnessed uncontrolled growth in recent years becoming the primary tool to manage global infrastructure for economic, social, political and subsequently military activity. Though assisting rapid development, cyberspace at the same time has given rise to new means and methods of warfare. It puts the security of all States at risk, raising internal and external concerns.[1] Such threats can lead to cyber warfare which, as generally understood, materializes when hostilities in situations of armed conflict between States or between organized armed groups are conducted in cyberspace. Cyber-warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks, for example, computer viruses or denial- of-service attacks. The end of cyber warfare is the same as those attributed to kinetic use of force, for example for weakening the military might of another State, or to press one's own advantage. Moreover, like kinetic warfare, cyber-warfare is governed by the law of nation or public international law.

[1] Muhammad Imad Ayub, "CYBER-WARFARE: IMPLICATIONS FOR THE NATIONAL SECURITY OF PAKISTAN." NDU Journal (2019), available at: https://www.semanticscholar.org/paper/CYBER-WARFARE%3A-IMPLICATIONS-FOR-THE-NATIONAL-OF-KhanAyub/86c35bac291369a493393db129b3cb5e451d956e#citing-papers

A cyber-attack is a concern for International Humanitarian Law, hereinafter called (IHL) only where such an attack could be categorized as, a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. Furthermore, where kinetic or physical attacks are launched against belligerent cyber facilities it would not amount to a cyber-attack, but physical damage or destruction may be caused from a cyber-operation. Cyber-warfare, just like kinetic warfare, can be of different natures[2]. However, where parties to the armed conflict, whether during an international armed conflict hereinafter (IAC), non-international armed conflict, hereinafter (NIAC) or trans-boundary hostilities, remain easily identifiable in the physical world, cyberspace changes all that. In modern times, any number of individuals regardless of physical location or affiliation may easily engage in activity that would qualify as cyber-warfare. These persons may use proxies to hide the origin of the cyber-attack and may also devise it in such a way to put blame on any other State thus leading to the complexity in attribution of the act.

Cyber-warfare is one of the contemporary technologies which raise problems of compliance with IHL. Hereinafter, the application and compatibility of IHL to cyber warfare is deliberated upon, with simultaneous analysis of the subject at hand in the context of Pakistan. Public International Law constitutes both jus ad bellum and jus in Bello. Jus ad bellum regulates the legality of resorting to threat or use of force. Thus, it governs situations among States prior to the engagement in hostilities. On the other hand, jus in Bello, commonly referred to as IHL, is that branch of law which comes into effect once an

[2] Sadia Rasool, "Cyber security threat in Pakistan: Causes, Challenges and Way forward." *International scientific online journal* 12 (2015): 21-34, available at: https://d1wqtxts1xzle7.cloudfront.net/98368540/21_34_Sadia_Rasool_Cyber_security_threat_in_Pakistan_causes_challenges_and_way_forward-libre.pdf

armed conflict has been initiated. It focuses to limit the effect of war and to minimize humanitarian cost of attacks, thereby protecting those individuals and objects that do not take direct participation in conflict. Although both these branches of international law raise fundamental questions in respect to cyber warfare, for the purposes of this study, Jus in Bello, i.e. IHL shall be the main point of concern with a special focus on Pakistan.[3]

Cyber warfare is often confused with cybercrimes and cyber-terrorism due to some shared features between them; owing primarily to the common domain through which these are conducted, i.e., cyberspace. Moreover, as it is sought to evaluate the subject at hand in the context of Pakistan, domestic legislation and/or jurisprudence shall be referred to as available. Cybercrimes are based on acquiring personal, wrongful gain by causing physical or psychological injury to another individual; cyber-terrorism is geared more towards political goals as part of its agenda. Cyber-terrorists, operating upon a political, religious or sectarian ideology, in addition to undermining internal order, also seek to shake the peoples' trust in the State's ability to protect them by targeting civilians. This may be differentiated from cyber warfare which theoretically does not allow civilians to be made the object of attack.[4]

Cyber-warfare, just like kinetic warfare, can be of different natures. However, where parties to the armed conflict, whether during an international (IAC), non-international (NIAC) or trans-boundary hostilities, remain easily identifiable in the physical world, cyberspace changes all that. In modern times, any number of individuals

[3] Rafay Baloch, "Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan." *Journal of Development Policy, Research & Practice (JoDPRP)* 3, no. 1 (2019): 23-43, available at: https://journals.sdpipk.org/index.php/JoDPRP/article/view/15

[4] Aamna Rafiq, "Challenges of securitising cyberspace in Pakistan." *Strategic Studies* 39, no. 1 (2019): 90-101.available at: https://www.jstor.org/stable/48544290

regardless of physical location or affiliation may easily engage in activity that would qualify as cyber-warfare. These persons may use proxies to hide the origin of the cyber-attack and may also devise it in such a way to put blame on any other State thus leading to the complexity in attribution of the act, as discussed later.

Applicability of IHL to Cyberwarfare

Cyber warfare raises certain legal questions regarding both branches of Public International Law, i.e., jus ad bellum and IHL. Regarding the former category, the prohibition under Art. 2(4) of the UN Charter apply in cyberspace just as it does in kinetic operations. Similarly, the only justification to engage in such activity would be founded on either Art. 42 or Art. 51 of the Charter. Furthermore, once hostilities are engaged into, IHL becomes applicable. This latter category comprises of numerous Conventions and their Protocols, as well as CIHL derived from State practice and Opinio juris.[5]

However, the law itself is not entirely sufficient because it causes certain complexities. Owing to the differing dynamics of cyberspace from that of physical geography, it makes some rules of IHL somewhat absurd in their application, as discussed later. Nevertheless, the Red Cross and Red Crescent Movement (the Movement) opines that even though new technologies pose difficulties for IHL they are governed thereunder. The opinion that a technology is not specially addressed in the existing body of law does not conclude that it would remain or in any way could operate without restrictions. In

[5]Muhammad Fahim Khan, Dr. Aamer Raza, Dr. Noreen Naseer, "Cyber security and challenges faced by Pakistan." *Pakistan Journal of International Affairs* 4, no. 4 (2021) available at: https://doi.org/10.52337/pjia.v4i4.408

relation to cyberspace, since most of IHL is designed to be an adaptive body of law it is, thus, designed to include new weapons.

This is deduced from Art. 36 of AP I, which reads that: In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party. Therefore, under the authorities cited above, it may be inferred that new and emerging technologies are bound by existing laws regardless of whether they are directly addressed thereunder or not.

As for the third assertion that IHL deals with attacks that are physical in nature, it may be dispensed with by a simple understanding of an armed conflict, i.e., the act which triggers the application of IHL. An armed attack is not merely limited to kinetic use of force, rather any attack constituting violence, against the adversary, whether in the offensive or the defensive. Moreover, the whole of IHL attempts to protect persons not directly engaged in the conflict and to minimize the effects thereof. Thus, exclusion of attacks that are not physical in nature would defeat the purposes of IHL. This logic may also be derived from the ban on biological and chemical weapons; which though not physical means of attacks, fall within the ambit of IHL.

Pakistan Cyber Laws and The IHL Paradigm

Studying and analyzing cyber warfare in the context of Pakistan poses a greater mystery as compared to other countries. While some explicit legislation and State practice is witnessed

by other States at the international level concerning issues in cyberspace, the same is almost non-existent in Pakistan.

At the domestic level, the Electronic Transactions Ordinance, 2002, hereinafter (ETO) which is still in force, primarily deals with cyber activity.[6] The ETO remains limited in scope as it concerns issues related to economic commerce. The emergence of novel cybercrimes emphasized the need for a more comprehensive framework leading to the adoption of the Prevention of Electronic Acts hereinafter called (PEC Act). However, it is mostly silent on cyber warfare, and provides only a rudimentary framework even for the issues it does address, leaving a lot to be resolved.[7]

Be that as it may, it would still be an amateur suggestion that Pakistan is not bound by international norms when it comes to developing cyber offence and defense capabilities. Though, the State lacks substantial domestic framework on the matter, and is not a party to Additional Protocols of 1977, it must adhere to existing IHL as this responsibility arises from Art. 1 of The Hague Convention, 1907 and Common Art. 1 of Geneva Conventions, 1949 to which Pakistan is party. Moreover, these provisions, like most of IHL are derived from customs, and have attained the status of customary IHL themselves most prominent amongst which is the Martens Clause therefore their importance and applicability to the State of Pakistan cannot be denied.

[6] THE ELECTRONIC TRANSACTIONS ORDINANCE, 2002, available at: https://pakistancode.gov.pk/pdffiles/administratordbc98dd49f2df3b1d07bb986dcceb9a3.pdf

[7] Rashida Zahoor, Muhammad Asif Safdar, Waqas Rafiq, Farhana Aziz Rana, Cyber War in a Cyber-Led World and Legislative Measurements taken by Pakistan, *Competitive Social Science Research Journal*, *3*(2), 151–158. Available at: https://cssrjournal.com/index.php/cssrjournal/article/view/250

Furthermore, the ICRC, CIHL Study makes it evident that domestic legislation falls among constituent elements of verbal acts for discerning a State's practice with regard to any rule thereunder. Therefore, ETO and the PEC Act are vital in understanding the Pakistani practice on issues within cyberspace and accordingly shall be used for guidance hereinafter.

Significance of the Research

The existing international humanitarian law is applicable to cyber warfare but there still exists some difficulties that should need to be addressed. The major problem in this regard is to identify the perpetrator of such attack and categorizing the nature of the armed conflict. In order to resolve this challenging problem it would be ascertained that the fundamental principle of IHL is to be practically replicated in cyberspace. If some where there is loopholes in existing laws or treaties than a new treaty regime is suggested to be implemented. But to time taking process of ratification of states to a treaty it is necessary to see it in principle of humanity and recognize such rules for it through universal consensus and evolving state practices. Yet cyber warfare is no humanitarian consequences but ultimately it will happen if the threat grows further and the risk will be increase. Keeping in view the legal framework of Pakistan there is no clear rules regarding cyber warfare, like other nations Pakistan still not exists any rules, the only act enforced at domestic level are insufficient to tackle the emerging threat of cyber warfare.

Aims and Objective of the Study

a) To distinguish cyber warfare from other cybercrimes.

b) To highlight the role of IHL in cyber warfare. And whether cyber warfare effect the principles of IHL.
c) To analyses that whether Pakistan's legal frame work is with in pace with modern technology.
d) To identify in which way cyber warfare different from other war fighting domain. States must be made aware of their legal duty to comply with IHL while adopting new means and methods of warfare and to establish internal mechanisms of reviewing such weapons and techniques prior to their adoption or development.
e) To establish a cyber- defence system while identifying the loopholes in the existing laws and acts.

Literature Review

For the purpose of research, I have thoroughly read the following articles and books, they are very handy as the authors comprehensively described cyber warfare, its nature and difference between cyber warfare and other war fighting domain. It also discussed many laws dealing with cyber warfare on international level and elaborate different mechanisms adopted by states to tackle the emerging threats of the fifth generation war. The main focus of my research is that how International humanitarian law applies to cyber warfare and what regime is adopted by Pakistan to challenge this issue. So the articles and books are very handy but my main focus is on Pakistan which does not specifically discussed the situation of Pakistan. So the basic purpose of my research is to see if any such laws are incorporated in domestic legal regime of Pakistan.

Cyber warfare and cyber terrorism

Andrew Edarik and Andrew M. colarik in their book cyber warfare and cyber terrorism defined the cyber warfare as a planned attack by nations or their agents against information and computer system, computer programs and data that result in enemy losses. They say that cyber terrorism and cyber warfare are becoming new and important threats against information technology resources and must be a part of the overall planning, design and implementation process aimed at providing overall protection. They gave the idea to secure all assets from all parties by giving high restrictive access and set a rationale foundation to decide the basic priorities and any subsequent decisions based on that rationale they also emphasize on the defense mechanism that it must be implemented in an organized way. Meaning thereby that every organization should set up a plan on how to develop and implement security measures. And information security policy plays a key role in it. By dealing with cyber-warfare attacks the most effective mode of operation is the system approach, when all major decisions are done from the point of overall advantage to the whole of an organization.[8]

Cyber warfare: techniques, tactics and tools for security practitioners

Janson Andress and Steve Winterfeld in their book "cyber-warfare: techniques, tactics and tools for security practitioners" they state that till date no nation has declared a cyber-war but the threat of its existence is always there but none have stated they suffered from an act of war. The two talked about events are the 2007 cyber-attacks against Estonia and in 2008 integrated cyber and kinetic attack against Georgia. These both involve nation's states and

[8] Lech Janczewski, and Andrew Colarik, eds. Cyber warfare and cyber terrorism. IGI Global, 2007, available at: https://scholar.google.com/citations?user=ojfOMFkAAAAJ&hl=en&oi=sra

call on military actions. There are so many other incidents occurred but they are not on the record.[9]

Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats

James A Lewis in his paper looks at one set of issues those related to cyber-terrorism and cyber-attacks on critical infrastructure and their implications for national security. Much of the literature on cyber-terrorism assumes that the vulnerability of computer networks and the vulnerability of critical infrastructures are the same, and that these vulnerabilities put national security at a significant risk. Given the newness of computer network technology and the rapidity with which it spread into economic activity, these assumptions are not surprising. A closer look at the relationships between computer networks and critical infrastructures, their vulnerability to attack, and the effect on national security, suggests that the assumption of vulnerability is wrong. A full reassessment is outside the scope of this paper, but a brief review suggests that while many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable.[10]

Cyber Warfare: Issues and Challenges

Michael Robinsona, Kevin Jonesb, Helge Janicke in their paper examine the most basic question of what cyber warfare is, comparing existing definitions to find same ground or disagreements. They find out that there is no properly adopted definition and that the terms cyber war and cyber warfare are not well enough defined to be differentiated. To tackle these issues, the authors present a definition model to help define both cyber warfare and

[9]Andress, Jason, and Steve Winterfeld. Cyber warfare: techniques, tactics and tools for security practitioners (Elsevier, 2013);324.

[10] Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. (Washington, DC: Center for Strategic & International Studies, 2002).

cyber war. The paper then identifies nine research challenges in cyber warfare and analyses contemporary work carried out in each. Also a conclusion is made at the end by making suggestions on how the field may best be progressed by future efforts. Hence the clear cut definition of cyber warfare and cyber war will provide a better idea of understanding deeply this issues and will provide a pathway for researchers to formulate new questions of research.[11]

The limitation of cyber warfare under humanitarian law

This article focuses mainly on the controversy about how current international legal frameworks, especially International Humanitarian Law (IHL), applies to such conduct in cyberspace, most notably in the context of armed conflict. Because one of the fundamental principle of the IHL is to protect civilians from the impact of armed conflict, it is critical to explore the norms of IHL that regulate such operations. This article will be likely to discuss about cyber warfare in the term of armed conflict. This article also review the rules and principle that applies during the cyber warfare.[12]

[11] Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." Computers & security 49 (2015): 70-94.

[12] Zuhra, Amalia, and Laila Almira. "THE LIMITATION OF CYBER WARFARE UNDER HUMANITARIAN LAW (Pembatasan Perang Siber dalam Hukum Humaniter)." terAs Law Review: Jurnal Hukum Humaniter dan HAM 3, no. 1 (2021): 1-10.

A brief primer on international law and cyber space[13]

International law structures relations among states and other international stakeholders most notably international organizations through various prohibitions, requirements, and permissions. As such, it has provided a path for regulating global governance issues from arms control to trade to the environment. As states give increased attention to the governance of cyberspace the technical architecture that allows the global internet to function and governance in cyberspace how states, industry, and users may use this technology, the role of international law in the cyber context has gained increasing prominence.

Research Questions

a) Whether cyber-warfare and other cyber-crimes the same things?
b) What are the strategies of Pakistan to the new emerging threats of cyber warfare? Whether Pakistan's legal framework is in pace with the developing technology while identifying the shortcomings in its existing legal system?
c) Whether International humanitarian law comply with the development of new means and methods of warfare and how much cyber warfare affects the principles of international humanitarian law?

Research Design

For the purpose of research under title stated above, the mixed research methods are used in which the data available is to be studied deeply which is available in the form of books,

[13] Hollis, Duncan. "A brief primer on international law and cyberspace." Carnegie Endowment for International Peace, dostupno na: https://carnegieendowment. org/2021/06/14/briefprimer-oninternational-law-and-cyberspace-pub-84763, приступљено 15 (2021): 2022.

research articles and secondary data. The data in hand has been analyzed to reach the conclusion. Hence the research methodology used in this thesis research is based on doctrinal and analytical research techniques.

Summary of Chapters

The first chapter of the research delineates about cyber warfare and differences of cyber warfare with other war fighting domain. It provides a thorough knowledge that how cyber warfare is different in nature from other cybercrimes. Second chapter discuss the strategies of Pakistan to the new emerging threats of cyber warfare and applicability of international humanitarian law to cyber warfare. Third chapter highlight the principles of IHL in the context of cyber warfare and also discuss shortcomings in the existing legal system of Pakistan. The conclusion of thesis includes a short summary of thesis discussion and some recommendations based on the research.

CHAPTER 1

CYBER WARFARE AND DIFFERENCE BETWEEN CYBER WARFARE & OTHER WAR-FIGHTING DOMAINS

1.1 Introduction

The use of cyber technology to govern the world's infrastructure for economic, social, political, and ultimately military action has grown unchecked in recent years. Cyberspace has helped to accelerate growth while at the same time creating new ways to wage war. It causes both internal and exterior worries and jeopardizes the security of all Nations.[14] A nation-state or international organization may engage in cyber warfare by attacking and attempting to harm the computers or information networks of another country using methods like computer viruses or denial-of-service attacks.[15] The goal of cyber warfare is the same as those associated with the use of physical force, namely to reduce another State's military power. Cyber warfare is also subject to national or public international law, just as kinetic combat.

The branches of international law jus ad bellum and jus in Bello, for example International Humanitarian Law raise fundamental questions regarding cyber warfare, but the main focus of this study is the application of IHL to cyber warfare. International humanitarian law is that branch of law which deals with wagging of war, it minimizes

[14] Muhammad Imad Ayub Khan, "Cyber-Warfare: Implications for The National Security of Pakistan." *NDU journal* (2019):101 available at http://111.68.99.125/website/ndu-journal/pub-new/06-Cyber-Warfare.pdf (last accessed: Nov 6, 2022).

[15] Jane McCall ion, "What is cyber warfare?" https://www.itpro.co.uk/security/28170/what-is-cyber-warfare (last accessed: Nov 6, 2022).

humanitarian cost and comes into effect when an armed conflict has been initiated. The existing IHL is applicable to cyber warfare but there are certain lacunas which need to be addressed. The main issue in the application of IHL to cyber warfare is in the classification of an act to be recognized as an attack, or what acts in cyberspace would amount to an attack, thus triggering an armed conflict and once the nature of attack is determined it remains to be ascertained that how the principles of IHL would be practically implemented.

The Shanghai Cooperation Organization's definition of cyber warfare may only be used in relation to cyber conflicts and cyber hostilities that would be considered armed conflicts under IHL. The International Committee of the Red Cross hereinafter (ICRC) understands cyber warfare to denote those means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL. A cyber-attack is also only a concern under IHL if it falls under the definition of a cyber-operation, whether offensive or defensive, that is reasonably likely to inflict injury or death to individuals or damage or destruction to things. Likewise, although physical harm or destruction may result from a cyber-operation, kinetic attacks directed against hostile cyber infrastructure would not constitute a cyber-attack.

Another definition of cyber warfare is put forward by Cornish et al. (2012): Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial, or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.[16]

[16] Michael Robinson, Keven Jones, Helge Janicke, "Cyber warfare: Issues and challenges", Ma, Computers & Security 49:70-94, DOI:10.1016/j.cose.2014.11.007 rch 2015, Computers & Security 49:70-

1.2 Cyber warfare as a fifth combat zone

Due to the 21st century's substantial reliance on networks, cyberspace is becoming a more important and hotly contested area for the use of military force. In reality, many countries have publicly identified cyberspace as the fifth dimension of warfare in their different military strategies. This transformation in the nature of warfare over the past few decades is undoubtedly the most significant and fundamental one. Networks are becoming the battlefields of the future, where cyber weaponry will engage in electronic attack and defense at lightning-fast speeds.

Cyberwarfare is now included in war vocabulary as a fifth fighting zone in the twenty-first century. Yet, since there is no agreement on what constitutes cyberwarfare, it is difficult to define. Cyber war is an extension of policy by actions taken in cyber space by state or non-state actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security. So, Cyber warfare as activities taken by a nation state to break into the computers or networks of another country with the intention of causing harm or disruption.

According to the Cambridge Dictionary, cyber warfare is the practice of attacking a nation's computers over the internet in an effort to disrupt its water, power, and communication infrastructure. It basically means that it is an attack that originates in electronic systems but has the potential to do harm in the real world. That is a key component of the definition, indicating that a straightforward attack on a website belonging

94, DOI:10.1016/j.cose.2014.11.007 Jeffrey L. Caton, "The Land, Space, and Cyberspace Nexus: Evolution of the oldest Military Operations in the Newest Military Domains" https://www.jstor.org/stable/resrep17662

to the government would not be classified as a kind of cyberwarfare but rather as a cyberattack. Several wars were won without doing enough damage or disrupting state-important infrastructure or buildings, which can do more real harm than the actual fighting itself. When states engage in cyber warfare, defined and proportionate force is used against specific targets, such as military and industrial targets, in order to advance political, economic, or territorial objectives.[17] Many of the characteristics of physical conflict are also present in cyberspace since it serves as a supporter of that conflict. Weapons used in cyberwarfare are primarily military in nature as opposed to dual-purpose, opponents can be tracked and dissuaded, the terrain is predictable, defense is the best position from which to operate, and aggressive actions expose the user to vulnerability as a single operation on the battlefield. In cyberwarfare, success and failure are obvious. Since cyber warfare is not a distinct phenomenon, it cannot be distinguished from other physical domain conflicts. As a result, cyber warfare must be conducted and restrained in accordance with the values, laws, and norms of a state as well as the restrictions that a state imposes on conventional warfare.

1.3 Instances of cyber attacks

In the spring of 2007 Estonia fell under a cyber-attack campaign lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. Estonia requested NATO to intervene but cyber-attacks were not recognized by NATO as an armed attack, however the notion was changed in 2014 without detailed analysis on what constitutes a cyber-attack.[18]

[17] Zen, Chang, "Cyberwarfare and International Humanitarian Law." Creighton Int'l & Comp. LJ 9 (2017): 29. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4262971 last accessed: Nov 10,2022).

[18] Rain Ottis, "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." In *Proceedings of the 7th European Conference on Information Warfare*, p. 163. Reading, MA:

On 9 August 2008, Russian and Turkish servers, allegedly controlled by the Russian hackers, were used to direct major Georgian Internet traffic. Although on the same day some Georgian Internet traffic was temporarily redirected to Germany, the Georgian traffic was soon again diverted to Moscow.

Different variants of Stuxnet targeted five Iranian organizations, with the probable target widely suspected to be uranium enrichment infrastructure in Iran; Symantec noted in August 2010 that 60 percent of the infected computers worldwide were in Iran. It was the first cyber-attack with actual physical damage.

1.4 Difference Between Cyber Warfare and Other War Fighting Domain

In this subsection, various forms of cyber threats are briefly explained to differentiate them from cyberwarfare. This distinction is important because cyberwarfare is often confused with cybercrimes and cyberterrorism due to some shared features between them. There are a few minor distinctions between conventional and unconventional types of warfare and cyberwarfare. In addition to the more conventional battlefields of land, air, sea, and space, cyberspace has expanded the realm of the battlefield and is considered the fifth battlespace.[19] The claim that cyberspace is a legitimate battlefield in and of itself modifies our current concept of cyberwarfare. Simply said, cyberwarfare is a brand-new but not wholly distinct element of a multifaceted battle environment. In general, cyberwarfare

Academic Publishing Limited, 2008, available at: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[19] Jeffrey L. Caton, "The Land, Space, and Cyberspace Nexus: Evolution of the oldest Military Operations in the Newest Military Domains" https://www.jstor.org/stable/resrep17662 (last acceesed: Nov 12,2022).

shouldn't be viewed as a separate or impartial phenomenon. Few of the aforementioned activities would result in a big triumph on their own, and as Alex Michael points out: What remains unremarked in the popular narrative is a constant ongoing background level of cyber-attack as part of a holistic, coordinated programmed to achieve the political, economic and social aims of nation states.

State-sponsored or non-state groups play a force-multiplier role in cyberattacks, although they are but one element of a larger strategic mix used in these attacks. Warlike challenges combined with other forms of coercion and hostility are more likely to arise in cyberspace. But there's no denying that cyberwarfare is distinct from these other tactics. It challenges the conservative notion of the state as the primary actor in the international system and the decisive effect on warfare, in contrast to diplomacy, military force, and economic warfare. Although nation-states are more likely to use cyber methods and means to accomplish their goals and have already recognized its defensive and offensive potential, cyberspace has made it possible for non-state actors, commercial organizations, and even individuals to obtain the means and motivation for warlike activity. Nation-states have far greater access to the capabilities, resources, and budgets needed to carry out significant and well-directed cyber-attacks.[20]

Similar to kinetic combat, cyberwarfare can take on various forms. Cyberspace, however, completely alters the physical world, where parties to an armed conflict, whether during an international (IAC), non-international (NIAC), or trans-boundary hostilities, remain plainly identifiable. In the present era, anyone, regardless of physical location or

[20] Paul, Cornish, David Livingstone, Dave Clemente, and Claire Yorke, "On cyber warfare", (London: Chatham House), 2010. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security (last accessed: Nov 8, 2022).

affiliation, can readily engage in action that qualifies as cyber-warfare. By utilizing proxies to conceal their identity and the source of the cyberattack, these individuals complicate the act's attribution. They may even design the attack to place the blame on any other State.

The PEC Act, inadvertently blurring the line between cybercrime and cyberwarfare by making unauthorized access, copying, transmission, or interference with essential infrastructure illegal, blurs the line between these two activities. Critical infrastructure is defined by this Act as Assets, facilities, systems, networks, or procedures that are essential to infrastructure and the loss or breach of which might have a significant impact on national security, national defense, or the government's ability to function. It should be noted that interference or illegal access with such infrastructure that affects national security may not just result in cybercrime but may also be considered to be use of force under the United Nations Charter, raising concerns about cyber security.[21]

1.4.1 Point of Distinction Between Cyber Warfare & Cybercrime

Due to significant similarities between them, particularly the shared area in which they take place, or cyberspace, cyber warfare is frequently conflated with other cybercrimes. Cybercrimes focus on obtaining personal, unjust gain by physically or psychologically harming another person, whereas cyber terrorism has more of a political aim. In addition to damaging internal order, cyberterrorists that follow a political, religious, or sectarian ideology aim to undermine the public's faith in the government by targeting civilians. This can be distinguished from cyberwarfare, which in theory prohibits using civilians as targets

[21] Dan-Iulian Voitaşec, "Applying International Humanitarian Law to Cyber-Attacks" *Lex ET Scientia International Journal*, 2015, no.1 (2015): 124 https://ro.vlex.com/vid/applying-international-humanitarian-law-761920869 (last accessed: Nov 14, 2022).

for assault. The fact that cybercrime is an intelligence gathering activity rather than a necessarily destructive one sets it apart from cybernetic attacks.[22]

Both cybercrime and cyberwarfare involve destructive actions committed over computer networks or the internet, although there are significant distinctions between the two: International conflicts now frequently include deadly elements of cyber warfare. But at the moment, there is a genuine risk that events might quickly spread and spiral out of control due to the continuous arms competition in cyber warfare and the absence of clear guidelines for online combat.[23] Several elements determine whether an assault qualifies as an instance of cyber warfare. These contain the attacker's name, what they are doing, how they are doing it, and the amount of harm they cause. Cyber warfare is typically defined as a battle between states, not between individuals, similar to traditional types of warfare. The attacks must be of considerable scope and severity to qualify.

Cyber actions that are part of or resemble armed combat are referred to as cyberwarfare. Such cyber operations, which entail the creation and transmission of computer code from a source computer to a target computer, can either be intended to infiltrate a computer system in order to collect, export, destroy, modify, or encrypt data, or to start, alter, or otherwise manipulate processes that are managed by the infiltrated system.

Internet combat Even if such procedures are aimed at computers rather than people, they may still result in a great deal of human suffering. There are legitimate reasons to be

[22] Emerald M. Archer, "Crossing the Rubicon: Understanding Cyber Terrorism in the European Context" *The European Legacy 19*,no. 5(2014):621https://philpapers.org/rec/ARCCTR (last accessed: Nov 12, 2022).

[23] Kamile Nur Sevis, Ensar seker, "Cyber warfare: terms, issues, laws and controversies", July 2016, Conference: 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security, DOI:10.1109/CyberSecPODS.2016.7502348 (last accessed: Nov 16, 2022).

concerned that cyber operations would be used to obstruct the operation of infrastructure required for the supply of resources and services that are vitally important to the civilian population, particularly during times of armed conflict. Power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems, hospital systems, railroads, and air traffic control are just a few examples of critical installations that heavily rely on computer systems that are vulnerable to hacking and manipulation by cyber operations. Because civilian and military computer infrastructure are so interconnected and dependent on one another, it can be very difficult to tell them apart, increasing the danger that civilians and civilian objects would be harmed as a result of cyberwarfare. As a result, it is quite possible that an attack on a computer system used by the military will also harm computers used by civilians. The provision of certain public services, such as the supply of water and electricity or the transfer of assets, may depend on these.

1.5 Intent

Nation-states or state-sponsored entities frequently engage in cyberwarfare with the intention of disrupting or harming the resources or infrastructure of another nation. On the other side, cybercrime is committed by people or organizations for monetary gain or personal gain. Only if the cyber operations engaged are attributable to a state and they amounted to the use of armed force against another state would cyber warfare be considered an international armed conflict.[24] Given its rising reliance on information systems in general and Internet connectivity in particular, critical infrastructure functions is becoming

[24] Eiten Diamond, "Applying International Humanitarian Law to Cyber Warfare", Law and National Security, Selected Issues, Institute for National Security Studies (2014), http://www.jstor.com/stable/resrep08957.8 (last accessed: Nov 16, 2022).

significantly more susceptible to cyber-attack. Secretary of Defense Leon Panetta is among those sounding the alarm, declaring that When it comes to national security, I think this i.e., cyber warfare represents the battleground for the future. I've often said that I think the potential for the next Pearl Harbor could very well be a cyber -attack. If you have a cyber-attack that brings down our power grid system, brings down our financial systems, brings down our government systems, you could paralyses this country.[25]

Cyber warfare is altering the nature of contemporary conflict: In the foreseeable future, achieving the ultimate goals in wars and confrontations will be brought about not so much by the destruction of enemy groups of troops and forces, but rather by the suppression of his state and military control systems, navigation and communication systems, and also by influencing other crucial information facilities that the stability of controlling the state's economy and Armed Forces depends on.[26]

Like the absence of research on the dynamics of nuclear weapons in the 1950s, the highly acclaimed International Institute for Strategic Studies (IISS), based in London, views cyber warfare as an intellectually immature topic. IISS Director-General and Chief Executive John Chipman recently stated that "usage of so-called asymmetric strategies may characterize future state-on-state conflict. The employment of cyberwarfare may be the most important of these.[27]

[25]Dr. Andrew F. Krepinevich, Jr., "Cyber Warfare a "Nuclear Option?" *Centre for strategic and Budgetary Assessments,* 2012.

[26] Ibid

[27] Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence" *Journal of Strategic Security* 4, no.2 (2014):12 https://digitalcommons.usf.edu/jss/vol4/iss2/2 (last accessed: Nov 6, 2022).

1.5.1 Target

Cybercrime targets specific people, companies, or organizations, whereas cyberwarfare is often focused at other nation-states or their vital infrastructure. There are many different aspects to the information revolution. It is based on the growth and widespread adoption of ICTs, which have an impact on many aspects of our everyday lives, including working, engaging with others, traveling, and vacation planning. Because of the fundamental changes brought about by the information revolution, the spread of ICTs has significant philosophical ramifications. The information revolution creates a change that elevates the non-physical realm to parity with the physical one in importance and value. One of the most compelling examples of such a shift is cyber warfare; it demonstrates the existence of a new environment in which physical and non-physical entities coexist and are valued equally, in which states must establish their authority, and in which new forms of warfare are being developed especially for use in such a new environment.

1.5.2 Scope

Large-scale attacks on vital infrastructure, like power grids, communication networks, and banking institutions, are a common feature of cyber warfare. In contrast, smaller-scale attacks like obtaining personal information or carrying out fraudulent transactions are more common in cybercrime.

The transition to a non-physical world creates the foundation for the universality of cyberwarfare. This is a complex issue that is easier to understand when traditional and cyber warfare are contrasted. Traditional warfare is the use of state violence by the state's armed forces to establish the terms of rule over a particular territory. It is a violent

phenomenon that inevitably results in the loss of human life and the destruction of both military and civilian infrastructure. When engaging in traditional warfare, the challenge is figuring out how to minimize such damages while yet securing victory. It appears that cyberwarfare is distinct from traditional warfare in that it is not always violent and destructive. A computer virus that may impair or prevent access to the enemy's database could be used in cyberwarfare to severely harm the adversary without using physical force or violence. The same is true for cyberwarfare, which does not always include people. In this context, a computer virus may carry out an act of war by attacking other artificial agents or informational infrastructures, such as a database or website.[28]

1.5.3 Impact

While cybercrime can lead to financial losses and reputational harm, cyberwarfare has the potential to have a significant influence on national security and public safety. Cyberwarfare is a threat that should be feared just as much as traditional warfare because it can take many different forms and can vary in degree of ferocity. Think about the effects, for instance, if a cyberattack targeting a military aerial control system resulted in an aircraft crashing.

As was already mentioned, the key characteristic of this phenomenon, the feature that distinguishes it most from traditional warfare, and the feature that generates the ethical issues posed by Cyber warfare is the transversely of this phenomenon with respect to the levels of violence, the nature of the agents, and the waging domain. Cyber warfare appears to avoid human sacrifice and violence, relieving political authorities of the

[28] Mariarosaria Taddeo, "An analysis for a just cyber warfare." In 2012 4th international conference on cyber conflict (CYCON 2012), pp. 1-10. IEEE, 2012. (last accessed: Nov 6, 2022).

responsibility of defending military activities to the public. Israel launched an unidentified airstrike on a nuclear plant in Syria in 2007 and used a cyberattack to disable the country's air defense systems. Similar to this, it is said that in 2008, during its conflict with Georgia over South Ossetia, Russia made strategic use of internet.[29]

In general, cyber-warfare is an activity that is supported by a nation-state with the goal of harming the resources or infrastructure of another nation. On the other hand, cybercrime is an illegal activity that is done for monetary or personal advantage, and the impact is typically restricted to the people or organizations who are directly impacted.

1.6 Conclusion

The majority of superpowers today have dedicated military cyber warfare departments, making cyberwarfare a very real threat. Despite the fact that there haven't been many organized cyberattacks against physical targets, we don't need a crystal ball to see that they will continue to rise. Governments, political parties, criminal gangs, businesses, and individuals can all now engage in cyber-espionage, cyber-warfare, and cyber-terrorism. We now live in a world where all forms of conflict can be carried out successfully, yet virtually invariably, the results will have an impact on the physical world. Cyber warfare and other cyber-crimes are conflated sometimes because of the shared features between them. Once an act is identified it would be easy to fall in the specific category of conflict. If real conflict between governments is the best way to define cyberwar, many of the attacks that are frequently and inaccurately referred to be cyber warfare will be excluded. Individual or even collective hacker attacks are typically not regarded as cyber warfare unless they are

[29] Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies", Working Paper CISL# 2017-10 May 2017, https://cams.mit.edu/wp-content/uploads/2017-10.pdf (last accessed: Nov 18, 2022).

supported and coordinated by a state. There are still a lot of grey areas in the murky domain of cyber warfare, though, and it is frighteningly common for states to encourage hackers in order to fabricate justifications for their own acts.

Applying IHL to this new kind of combat presents substantial issues because the legal landscape surrounding it is still developing. Application of IHL to cyber warfare raise so many questions which need to be address while keeping in the domestic and international laws on cyber warfare. The attribution of an attack is very difficult leading to a great deal of anonymity to an attacker. The absence of geographical boundaries in the cyber space makes it very easy for the attackers to attack regardless of their identification. The advantages of cyberspace and technologies are substantial as everyone rely on it and cannot be disputed. So, this makes the cyber-domain more operational for the combat.

CHAPTER 2

STRATEGIES OF PAKISTAN TO THE NEW EMERGING THREATS OF CYBER WARFARE AND APPLICATION OF IHL TO CYBER WARFARE

2.1 Introduction

Since the 1990s warfare is dominated by technology, and with the passage of time and evolution of technologies it has emerged different legal structures and different ways and is thus considered as a new domain of war. Generally, War has been fought on four main stages: land, sea, and more recently, air and space. But now a fifth stage is introduced with the increased development of information and technology.[30] Thus, the age of information technology increased occurrence of electronic attacks and has introduced a fifth stage called cyberspace.[31] When defining cyberwarfare, state actors are typically included, but non-state actors including terrorist organisations, businesses, political or ideological extreme groups, hacktivists, and transnational criminal organisations are also included. Hence, neither a virtual world nor a universe from science fiction exists in the world of

[30] Pierluigi Paganini, "NATO and definition Rules For Cyber Warfare," *Cyber Defense Magazine*, March 21,2013, available at: https://www.cyberdefensemagazine.com/nato-and-definition-rules-for-cyber-warfare/ (last accessed 1st Dec,2022)

[31] Richard J. Harknett and Max Smeets, "Cyber campaigns and strategic outcomes", *Journal of Strategic Studies*, Volume 45, Issue 4(2022): 534-567, available at: https://doi.org/10.1080/01402390.2020.1732354 (last accessed: Dec 1,2022)

modern new technologies. According to Kellen Berger, these new weapons have the potential to kill people, harm infrastructures, and even start military conflicts.

According to Amy Chang, research associate at the Centre for a New American Security, Cyber warfare is a great alternative to conventional weapons. It is cheaper for and far more accessible to these small nation-states. It allows these countries to pull off attacks without as much risk of getting caught and without the repercussions when they are.

The accountability of the attackers is exceedingly difficult to establish when cyber weapons are deployed. Because they employ many proxies while infiltrating systems, cyber attackers and other hostile hackers and organisations are particularly difficult to identify and track back. Even if the attack is confirmed, the lack of a legal system makes it challenging to identify him as a war criminal. There are no set guidelines for putting a cyber-offender in jail or accusing a country of waging war on purpose. The current issue is that people are ill-prepared for these new threats, which have the potential to paralyse Internet service providers (ISPs) at the global level across national borders and disrupt communications and network traffic to and from websites. We live in a highly technologically advanced world of uncertainty. Therefore, the fundamental need of the modern world is to identify the new threats that constantly pose a security threat to the state, as well as to properly train the populace on how to handle cyber security issues and cyber war, as well as how to reduce risks and minimise damage, to the greatest extent possible, should the need arise.[32]

If Internet security cannot be controlled, it's not an exaggeration to say the effects could be no less than a nuclear bomb," said General Fang Fenghui, Chief of General Staff

[32] Daniel Brecht, "Cyber Warfare and Cyber Weapons, a Real and Growing Threat", *InfoSec Resources*, (January 15, 2015):75-105, available at https://resources.infosecinstitute.com/topics/general-security/page/45 (last accessed: Dec 15,2022)

of the People's Liberation Army of China, in April 2013. In the same year, the Secretary of State John Kerry responded to a cyber-security question during his confirmation hearings in January 2013 by saying, I guess I would call it the 21st-century nuclear weapons equivalent.[33]

2.2 Application and Compatibility of International Humanitarian Law to Cyber Warfare

International Humanitarian Law (IHL) and Customary International Humanitarian Law (CIHL) are applicable in order to reduce suffering and limit the effects of war throughout armed conflicts of all kinds, both international and non-international. Both soldiers and non-combatants must abide by these laws. The 1949 Geneva Conventions, 1977 addenda, various international treaties on particular themes, and numerous local manuals and case laws were developed to distinguish between civilian and military personnel and to specify their rights during armed conflicts.

Cyberwarfare and computer network attacks are not officially included in the Geneva Conventions, nor are they covered by any of their supplemental protocols. Nonetheless, the current principles and regulations controlling the means and methods of combat set forth in these treaties are not limited to the circumstances present at the time of their implementation. IHL foresaw technological advancements in weapons and the creation of new ways to wage conflict. In accordance with Article 36 of Additional Protocol I of 1977, a High Contracting Party is under an obligation to determine whether the

[33] Pierluigi Paganini, "Cyber Warfare: From Attribution to Deterrence". *InfoSec resources* (October 3, 2016) available at https://resources.infosecinstitute.com (last accessed: Dec 15, 2022)

employment of a new weapon, means, or method of warfare 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.[34]

The parties to the conflict must first determine if the use of cyberwarfare, which is regarded as a new weapon and a fifth domain of war, is illegal under IHL if it causes damage No specific definition is given for Cyber-attack in the statutes. But according to Article 49(1) of the Additional Protocol-I, Attack means acts of violence against the adversary, whether in offence or in defense. [35] So, there must be use of force to deter or prevent violent conduct for cyber warfare to be considered legal. This means that a cyber-operation just causes physical harm or object destruction, injury or death, and excruciating pain or illness. Only then it may be governed by IHL.

2.3 Pakistan Cyber Laws and the IHL Prototype

Comparatively to other nations, Pakistan presents a higher mystery when it comes to studying and analyzing cyber-warfare. While other States at the international level have some specific legislation and State practice on challenges in cyberspace, Pakistan has essentially none of either. There is currently no institution or entity wholly dedicated to the nation's cybersecurity. Pakistan requires a fully functional organization to defend the nation from cyberattacks. For -instance, Israel has Unit 8200 or the National Cyber Security Authority referred as (NCSA) and the United States has the Cybersecurity and Infrastructure Security Agency (CISA). The National Response Centre for Cyber Crime

[34]"Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977", available at https://ihl-databases.icrc.org (last accessed: Dec16,2022)

[35] "Protocols additional to the Geneva Conventions of 12 August 1949", available at https://www.icrc.org/en/doc/assets/files/other/icrc_002_0321.pdf (last accessed 3rd Dec, 2022)

(NR3C), a division of the Federal Investigation Agency (FIA), The Federal Investigation Agency (FIA) is a counter-intelligence, criminal investigation and security agency of the Islamic Republic of Pakistan which was established in 1975. The Economic Crime Wing (ECW) of the FIA has the mandate to protect the Intellectual Property Rights (IPR) of the people of Pakistan.[36] So, it deals with cybercrimes in Pakistan; but, due to a lack of resources, staff, and facilities, it is unable to protect the nation's vital national infrastructure.

2.3.1 Domestic Cyber Laws of Pakistan

The Electronic Transactions Ordinance, 2002, hereinafter called (ETO), which is currently in effect domestically, largely addresses online activities. The ETO's reach is still constrained because it only addresses issues pertaining to commercial commerce with the rapid increase in cybercrimes, government passed Prevention of Electronic Crime Ordinance (PECO) in 2007 and Prevention of Electronic Crimes Act (PECA) in 2016, which dealt with advanced cybercrimes, data theft, online frauds, forgery, cyber-harassment, and cyberterrorism.[37] The Prevention of the Electronic Crimes Act of 2016, hereinafter called PEC Act was passed because the rise of new cybercrimes highlighted the need for a more comprehensive framework. There are still many difficulties to be handled because it is largely silent on cyberwarfare and only offers a basic foundation for the problems it does address.[38]

---

[36] Ghalib khan, Sobia Bashir, Faisal Shahzad, and Saeed Ullah Jan. "Federal investigation agency against the crime of book piracy in Pakistan." *Library Philosophy and Practice* (2021): 1-13.

[37]Muhammad Nadeem Mirza, Muhammad Shahzad Akram. 3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare. Strategic Studies, 2022, 42 (1), pp.62-80 available at: ff10.53532/ss.042.01.00134ff

[38] "THE ELECTRONIC TRANSACTIONS ORDINANCE, 2002", *Pakistan code,* (11 Sep, 2002) Available at, https://pakistancode.gov.pk/pdffiles/administratordbc98dd49f2df3b1d07bb986dcceb9a3.pdf (last accessed: Dec 16, 2022)

Whatever the case, it would still be naive to argue that Pakistan's cyber-offence and defense capabilities are not subject to international standards. Although the State lacks a comprehensive domestic legal framework and is not a party to the Additional Protocols of 1977, it is nonetheless required to uphold existing IHL by Common Art.1 of the 1949 Geneva Conventions and Art.1 of the 1907 Hague Convention, both of which Pakistan is a party. The Martens Clauses the most notable of these rules, which, like the majority of IHL, are developed from traditions and have earned the status of customary IHL themselves. As a result, it is impossible to dispute their significance and applicability to the State of Pakistan. The Martens clause, which is related to an accepted IHL principle, states that when a situation isn't covered by a global agreement, civilians and combatants stay under the protection and authority of the principles of jurisprudence derived from established custom, from the principles of humanity, and from the dictates of public conscience even though IHL doesn't specifically mention cyber warfare.[39]

Furthermore, the ICRC, CIHL Study makes it clear that domestic law is one of the essential components of verbal actions for determining how a State actually practices any regulation under it. ETO and the PEC Act are therefore essential for comprehending Pakistani practice on matters relating to cyberspace, and as such, they will be utilized as examples in the following.

2.3.2 UN Charter and Cyber Warfare

Regarding jus ad bellum and IHL, as well as both areas of public international law, cyber warfare creates several legal issues. According to the text, the prohibition under UN Charter

[39] Muhammad Riaz shad, "Cyber threat landscape and readiness challenge of Pakistan." *Strategic Studies 39, no. 1 (2019): 1-19*, available at: https://www.jstor.org/stable/48544285

Article 2(4) is illegal under public international law. All Members should refrain from using threats of force or the use of force in their international dealings against the political independence or territorial integrity of any state, or in any other manner inconsistent with the purposes of the United Nations.[40] So, just like they do in kinetic operations, these laws also hold true in cyberspace. Similar to that, only one of Articles 42 or 51 of the Charter would serve as the basis for such behavior. Additionally, IHL is applicable as soon as hostilities start. CIHL arising from State practice and opinion juris are included in the latter group, together with various Conventions and their Protocols.

Unfortunately, because of its inherent complications, the law is not totally sufficient. Several IHL regulations become somewhat nonsensical in their implementation due to the different dynamics of cyberspace compared to physical geography, as detailed later. Even while new technologies complicate IHL, according to the Red Cross and Red Crescent Movement, they are nonetheless subject to its rules.

2.4 Effect of the Existing Laws on the Emerging Technologies

The idea that a technology would stay or in any manner be able to operate without constraints does not follow from the view that it is not specifically addressed in the body of existing law. Since IHL is primarily intended to be an adaptable body of law, it is therefore intended to accommodate new weapons in connection to cyberspace. This can be inferred from Article 36 of AP I, which states: A High Contracting Party is under an obligation to determine whether the employment of a new weapon, means, or method of

[40] BeomChul SHIN, " An Inquiry on the Interpretation of Article 2(4) of the UN Charter and Its Implications for the Jus Ad Bellum" (Final Draft for the S.J.D. Dissertation May 2010)available at, https://repository.library.georgetown.edu/bitstream/handle/10822/1060419/shin_beomchul_sjd.pdf (last accessed: Dec 17, 2022)

warfare 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. [41]Hence, based on the aforementioned authorities, it can be assumed that new and emerging technologies are subject to existing laws, whether or not they specifically address them.

Any attack that involves violence, aggression, hurt, destruction, or that stirs up hostility towards the enemy, whether it is carried out in a defensive or offensive manner, qualifies as an armed attack or conflict. This includes both offensive and defensive actions. IHL's primary goal is to safeguard those who are not directly involved in the conflict and to lessen its effects. The objectives of IHL would be defeated if non-physical attacks were excluded. Since IHL only applies in the context of armed conflict, the first thing that must be determined when determining whether a particular cyber operation is subject to IHL is whether the operation in question was conducted in the context of and with a nexus to an armed conflict. This logic may also be derived from the prohibition on biological and chemical weapons, which although are not physical means of attack, fall within its ambit. Anytime states use force against one another, there is an international armed conflict. Hence, cyber warfare would only be considered an international armed conflict under IHL. A state is responsible for the related cyber operations, which amounted to using force against another state. When a circumstance is deemed to be an armed conflict, both IHL's permissive and restrictive clauses come into effect. IHL tolerates the level of incidental harm to other categories of people and objects known as collateral damage, which would all be prohibited by law applicable outside of armed conflict. This includes the intentional

[41] George H. Aldrich, "Prospects for United States Ratification of Additional Protocol I to the 1949 Geneva Conventions." *American Journal of International Law* 85, no. 1 (1991): 1–20. doi:10.2307/2203556 (last accessed: Dec 17, 2022)

use of lethal force against certain categories of people such as enemy combatants and civilians directly participating in hostilities and the intentional destruction of certain categories of property military objectives. So, there may be compelling reason for those who want to limit the use of force that is permitted by law to favor a stricter definition of when using armed force in cyberspace. In any case, it is still unclear whether, and if so, under what circumstances, cyber warfare can be deemed to constitute the use of armed force, even when it does not result in immediate physical destruction, in the absence of state practice or clarification of states legal positions.[42] When there is prolonged armed violence, or armed violence of a specific severity, between governmental authority and organized armed organizations or between such groups within a state, there is a non-international armed conflict. In other words, for a circumstance to qualify as a non-international armed conflict, it must involve armed conflict involving at least one non-state actor, where the parties engaged meet a minimal standard of organization, and the armed conflict meets a certain standard of intensity. Applying these standards to cyber warfare, however, presents a number of challenges. Hence, while claiming that cyber operations that interfere with the operation of things in the real world are attacks is rather simple, the position is far less obvious when it comes to operations meant solely to interfere with communication in cyberspace. The IHL principle that states that civilians should be safeguarded and that their way of life and the environment in which they live should not be targeted provide fundamental advice for dealing with these new forms of warfare, according to the ICRC. The complexity of armed conflict is increased by cyber warfare,

[42] Ido Kilovaty, "ICRC, NATO and the U.S. – Direct Participation in Hacktivities Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law", *DUKE LAW & TECHNOLOGY REVIEW* 15 (2016): 1-38, available at https://scholarship.law.duke.edu/dltr/vol15/iss1/1/ (last accessed: Dec 18, 2022)

which could raise new issues for IHL.[43] IHL must therefore be reinforced as the primary body of law that can govern this kind of combat. Cyber warfare can and must adhere to the standards of international humanitarian law that address topics including the use of indiscriminate force, distinguishing between military and civilian targets, proportionality, and perfidy.[44]

Cyberspace is an intangible space. But, through this intangible space, modernism has linked the four basic spheres of the material world land, air, sea, and outer space. Attacks on cyberspace can therefore seriously harm the real world. The majority of IHL guidelines are adaptable enough to be used in cyber warfare. The law of differentiation is useful, for instance, in cyberwarfare. This would merely indicate that cyberattacks could only be focused on military targets. But, due to the unique features of cyberspace and associated circumstances, it is now difficult to combat the entire phenomenon of cyberwarfare using only the IHL rules that already exist. The phenomenon's novelty creates a gap in accepted IHL. Treaty laws should take on the task of controlling cyber warfare by enacting new regulations in the absence of customary international humanitarian law. Recognizing the predicament, the international community has taken on the task of preventing cyberwarfare through provisions in treaty law. One attempt to regulate cyber warfare is the Tallinn Manual on the International Law Applicable to Cyber Warfare.[45]

---

[43] Hemen Philip Faga, "THE IMPLICATIONS OF TRANSNATIONAL CYBER THREATS IN INTERNATIONAL HUMANITARIAN LAW: ANALYSING THE DISTINCTION BETWEEN CYBERCRIME, CYBER ATTACK, AND CYBER WARFARE IN THE 21ST CENTURY" *Baltic Journal of Law & Politics* 10, no.1 (2017): 1–34, available at: http://www.degruyter.com/view/j/bjlp DOI: 10.1515/bjlp-2017-0001 (last accessed: Dec 18, 2022)

[44] Nishat Subah Maliha, "Cyber Warfare: Challenges In The Application Of International Humanitarian Law To Virtual Conflict"(Research monograph, Department of Law University of Dhaka august 30,2020) available at https://www.researchgate.net/publication/343979992Cyber_Warfare_ChallengesIn_The_Application_Of_International_Humanitarian_Law_To_Virtual_Conflict ' (last accessed: Dec 18,2022)

[45] Denagamage, PL, Thalpathawadana,TRMYSB. "International Humanitarian Law and Cyber Warfare: Sufficiency of International Humanitarian Law in Combating Cyber Warfare as a New

2.5 Strategies of Pakistan to The New Emerging Threat of Cyber Warfare

Governments must focus more on the emerging issue of cyber warfare since it is not an easy one to resolve. Today, millions of dollars are spent on both developing attack tactics and defending against potential attacks. Cyberwarfare seems to be a ticking time bomb that no one can predict when it will detonate. There isn't yet a piece of legislation that addresses cyberwarfare. Whether or not there has been a formal declaration of war and regardless of whether the parties engaged acknowledge the state of armed conflict, international humanitarian law is applicable to all instances of armed conflict.[46]

2.6 Tallinn Manual on The International Applicable to Cyber Warfare

The Tallinn Manual, an academic, non-binding study on how IHL applies to cyberwarfare, is the most thorough study on this topic. When we refer to cyber warfare, we are solely referring to tactics and techniques of conflict that involve cyber activities that are comparable to, or carried out in the course of, an armed conflict as defined by IHL. It does not apply to all types of what is commonly referred to as cyber-attacks. Of all international organizations to date, the Council of Europe has taken the most direct approach to regulating a portion of the cyber security issue, specifically cybercrime.

Phenomenon", South Eastern University Arts Research Session 2015, available at https://www.seu.ac.lk/researchandpublications/seuars/2015/Book%20of%20Abstracts%20%20Page%2058.pdf (last accessed: Dec 19, 2022)

[46] Dan-Iulian VOITAȘEC. "APPLYING INTERNATIONAL HUMANITARIAN LAW TO CYBER-ATTACKS", *LESIJ-Lex ET Scientia International Journal* 22, no. 1 (2015): 124-131. available at http://lexetscientia.univnt.ro/download/530_LESIJ_XXII_1_2015_art.010.pdf (last accessed: Dec 19, 2022)

2.6.1 Council of Europe Convention on Cyber-Crime

The 2001 Council of Europe Convention on Cyber-crime, or "Cybercrime Convention," promulgated a common criminal policy aimed at protecting society against cybercrime, primarily through legislation and international cooperation. It was the first international treaty on crimes committed using the Internet and other computer networks.

2.6.2 Geneva Conventions 1949

IHL still applies to all actions taken by parties during an armed conflict and must be observed notwithstanding the fact that means and methods of war have changed since the 1949 text of the Geneva Conventions. But, it cannot be ruled out that when cyber technologies advance or their humanitarian impact is more recognized, it may be necessary to develop the law further to ensure that it offers the necessary protection to the civilian population. How effective would such a legal instrument (in the form of a convention, rule, or treaty) be would be the question. As was already stated, technological advancements frequently precede legal advances, and international dialogue is far too slow and unwilling to reach a consensus. Also, it is just outside the scope of the various interests. Sadly, politics plays a significant part in the legal resolution of such a well-known case of present and future significance.[47]

The NATO Cooperative Cyber Defense Centre of Excellence hereinafter referred as (NATO CCD COE), an international military organization based in Tallinn, Estonia, and accredited by NATO in 2008 as a Centre of Excellence, invited an independent

[47] Andrew F. Krepinevich. "Cyber Warfare: A "Nuclear Option"?, (*Centre for Strategic and Budgetary Assessments,* August 24, 2012) available at https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option/publication/1 (last accessed: Dec 20, 2022)

International Group of Experts to produce a manual on the law governing cyber warfare in 2009. The Tallinn Manual is the outcome of this process, which was expert-driven and aimed to create a non-binding agreement, the Tallinn Manual on the International Law Relevant to Cyber Warfare is the most thorough analysis of the legal notion of cyber warfare. The manual was created by more than 30 international law experts from around the world and was created under the watchful eyes of NATO, US Cyber Command, and the Red Cross International.

2.7 Rules Regarding Sovereignty and Jurisdiction in Cyberspace

Tallinn 2.0, the second edition of the Tallinn Manual, was released in 2016. The fundamental basic concerns of the Tallinn Manual are jus ad bellum (the law governing the use of force) and jus in bello (IHL). There are 95 regulations in the two halves of the Tallinn Manual. The titles of the components are international cybersecurity law and cyber armed conflict law. State and cyberspace and the use of force are among the first part's subtitles, while the law of armed conflict, hostilities conducted, specific individuals, things, actions, occupation, and neutrality are the second part's subtitles. First 5 Rules outlines the concepts of sovereignty and jurisdiction while attempting to define a line for cyberspace based on cyber infrastructure within state borders.

The crux of the rules mentioned there is that a state may exercise control over cyber infrastructure and activities, it will also be liable under international law and in case of violation of treaty or commission of unlawful act done than cyber retaliation will be

observed against the offending State.[48] A state may employ its inherent right of self-defense if the operation falls within the ambit of armed attack.

The scope and impact of a cyber-operation determine whether it qualifies as an armed attack. Cyber-attacks are operations that injure or kill people or damage or destroy objects, according to the Tallinn Manual, which also addresses the definition of these operations and document that applies existing law to cyber warfare. Although it is not a legally binding protecting civilians. The concept of differentiation is applicable to cyber-attacks. Civilians as a whole and particular shall not be the target of cyberattacks.[49]

According to Gary Solis: If there is a circumstance in armed conflict that was unforeseen (and unforeseeable) by the 1949 Geneva Conventions, it is cyber warfare. Still, cyber warfare can be dealt with using traditional law of war tools, recognizing that today's jus ad bellum cyber war questions can instantly ripen into jus in Bello issues. Cyber-attacks are not per se LOAC violations. They are another strategy or tactic of warfare when considering their effect or use, they may be thought of as being similar to kinetic weapons.[50]

As William Boothby commented that 'the law of armed conflict contains no ad hoc rules which permit, prohibit, or restrict the lawful circumstances of use of cyber weapons as such? Nonetheless, it is evident that the same laws that govern the use of weapons more generally under international humanitarian law must also apply to cyber weapons. Attacks carried out through the use of cyber operations would be subject to the principles of distinction, proportionality, and military necessity. Cyber operations must abide by the

[48] ERIC TALBOT JENSEN, "THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS", *GEORGETOWN JOURNAL OF INTERNATIONAL LAW*, Vol. 48(2017):735, available at: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf (Last accessed: Dec20, 2022)

[49]Kamile Nur Seviş, Ensar Seker, "Cyber Warfare: Terms, Issues, Laws and Controversies", Conference*: 2016 International Conference On Cyber Security and Protection of Digital Services (Cyber Security) At: IEEE*, available at DOI:10.1109/CyberSecPODS.2016.7502348, (last accessed: Dec 21, 2022)

[50] Marco Sasoli. "IMPLEMENTATION OF INTERNATIONAL HUMANITARIAN LAW: CURRENT AND INHERENT CHALLENGES", *Yearbook of International Humanitarian Law*, Volume 10(December 2007): pp. 45 – 73, DOI: https://doi.org/10.1017/S1389135907000451, (last accessed: Dec 20, 2022)

pertinent principles of international humanitarian law as a type of remote warfare, including the ban on assaults that are indiscriminate or likely to result in needless suffering or harm. The secrecy surrounding cyber operations, the lack of openness around the conduct of attacks, and the lack of a treaty particularly addressing the regulation of cyberwarfare, however, pose obstacles to guaranteeing compliance with such regulations.

IHL would apply once the threshold of armed conflict is reached at high level there are different views exist on the characterization of cyber operations. According to Noam Lubell:

> Cyber operations are a classic example of an attempt to fit things into the laws of armed conflict where in fact they should not be addressed through these laws at all. The default classification of cyber operations, on one view, is that they amount to an armed conflict and so the laws of armed conflict apply. However, it is also argued that since such operations do not adhere to the definition of attack under international humanitarian law, the restrictions on attacks, imposed by the principle of distinction, do not apply One of the main challenges is to identify which type of operation should be addressed under the laws of armed conflict and which type should not.

The classification of each circumstance should be influenced by the intent and objective of this body of legislation: the protection of armed conflict victims. This will help determine which operations should be covered by IHL. This would be in violation if lowering the bar for using fatal force made the relevant legal safeguards less effective, placing those impacted in a more precarious situation. Michael Schmitt asserts that "new rules will emerge to handle events that have so fundamentally changed that the present classification architecture show classificatory vacuum" in the ongoing development of IHL. According to him, "certain components of conflict classification are likely to slip into desuetude while other aspects will likely be reinterpreted to meet emerging, unanticipated settings of armed conflict." If cyber operations are to be accommodated, this must be done

in a way that maintains the validity of the notion of armed conflict as it pertains to IHL, consistent with its object and purpose.[51]

2.8 Status of Pakistan in the Array of Cyber Security Context

Since gaining their independence, Pakistan and India have had a rocky relationship. There is several long-standing, unsolved disputes between the two countries, including those over Kashmir, Siachen issues, the border issues, Sir Creeks, and many others. This is the cause of their strained relationship. As Pakistan and India declared their possession of nuclear weapons, the threat paradigm was further complicated to include both kinetic and non-kinetic threats. The threat has transformed and taken on a new form as a result of increased interdependence and globalization. Iftekhar Ahmad, a spokesman for the Pakistan Interior Ministry, told the press at the time, "The reason for forming the national response center for cyber-crime (nr3c) is to stop the abuse of the Internet and pursue individuals included in cyber recognized crimes. It is noteworthy that nr3c only handles minor concerns, and that this tool needs to be improved to be more effective in containing the digital danger. In order to raise awareness regarding electronic crimes, Nr3c has organized more than fifty different seminars as of today, in 2014. Also, it has received 68 complaints from its zonal cybercrimes section. The Independent Groups of Experts and the International Committee of the Red Cross have planned to write a third manual in addition to the two Tallinn manuals they worked on. They wanted to investigate how current international legal norms and principles applied to the cyberspace environment. Brad Smith, the president of

[51] Anthony Culle. "The characterization of remote warfare under international humanitarian law." (In *Research Handbook on Remote Warfare*): pp. 110-132. Edward Elgar Publishing, 2017, available at, https://doi.org/10.4337/9781784716998.00013 , (last accessed: Dec 21, 2022)

Microsoft, even urged nations to sign a fresh "Digital Geneva Convention" to govern their conduct online.[52]

2.8.1 Cyber Security Strategy of Pakistan

The Senate Defense Committee's Function Edward Snowden, a contractor for the CIA, has revealed a U.S. secret about how it is used to monitor various nations. Edward Snowden said that the American National Security agency was snooping on Pakistan through the internet and online communication technologies, with 13.5 billion pieces of email, phone, and fax communications collected. Pakistan is reportedly the second-largest target of the U.S.

2.8.2 Six-Point Budget Proposal

In this regard, Senator Mushahid Hussain Syed, the chairman of the Senate Standing Committee on Defense, convened a significant meeting at which a delegation from the Pakistan Information Security Association (PISa), led by Ammar Jaffri, met with Mr. Syed in Parliament House to discuss cyber security strategy. In his Six Point Budget proposal, Senator Mushahid Hussain Syed stated: "Funds should be allocated in the budget for a cyber-Security Strategy since Pakistan is a victim of cyber warfare and cyber aggression. Given the security threat posed by the US through their secret agencies like CIA and NSA especially of Pakistan which is the second highest in their list of countries being spied online. This should be left in the hands of a cyber-security task force that has been specifically established for the aim of coming up with countermeasures and dealing

[52] DUNCAN HOLLIS. "A brief primer on international law and cyberspace." *Carnegie Endowment for International Peace,* 15 (2021) available at, https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 (last accessed: Dec 22, 2022)

with new developing threats that disturb both national security and tranquilly of the country.[53] The Ministry of IT should house its Secretariat. All participants enthusiastically agreed to this suggestion. First, it was determined to collaborate for the cyber security of defense, economy, and civilians during the discussion of the agenda items below. Second, it was decided to introduce a Private Bill in the Senate and National Assembly on August 14, 2013. Finally, the Pakistan Information Security Association and the national response of computer crimes centre would work together to develop the bill after extensive consultation on the matter. Also, it was determined that PISA would design the cyber security policy strategy. Fifthly, Senator Mushahid Hussain Syed argued that professional individuals with the necessary skill sets, background, and experience should be hired by various security groups. Finally, the Government needs to step up and take responsibility for putting international norms for cyberspace protection into practice.

2.9 Cyber Security Threat to Pakistan

In order to address security challenges relating to the internet, the Senate committee on defense and defense production organized a policy conference on Defending Pakistan through Cyber Security Strategy[54] in collaboration with the Pakistan Information Security Association hereinafter referred as (PISA). In his opening remarks, Senator Mushahid Hussain, the chairman of the Senate Committee on Defense and Defense Production, emphasized the threat posed by cyber security and how it may affect Pakistan's national

[53] Ms. Afeera Firdous, "Cyber Warfare and Global Power Politics*". CISS Insight Journal* 8, no.1 (2020):71-93. Available at http://journal.ciss.org.pk/index.php/ciss-insight/article/view/137 (last accessed: Dec 22,2022)

[54] Ms. Afeera Firdous, "Formulation of Pakistan's Cyber Security Policy: Comparative Approaches". *CISS Insight Journal* 6, no.1(2018):70 – 94, available at http://journal.ciss.org.pk/index.php/ciss-insight/article/view/32 (last accessed: Dec 23, 2022)

security, intelligence, diplomacy, nuclear and missile programed, economy, energy, education, civil aviation, and industrial and manufacturing units in both the public and private sectors. "Our cyber security must consist of three essential components. Mushahid Hussain stated that Pakistan's digital infrastructure must be able to withstand attacks, cyber penetration, and disruption. It also needs to be able to defend against new cyber threats, whether they are sponsored by states or not, and be able to take appropriate regional measures of retaliation. In response, Senator Mushahid Hussain stated that the committee has already taken the initiative to establish a Joint Task Force for Cyber Security, with the technical assistance of PISA to give recommendations and scenario assessments. He stated that the Senate Defense Committee is putting out the following 7-point action plan for a cyber-secure Pakistan: first, cyber security legislation that will be used to preserve, protect, and advance Pakistan cyber security must be introduced. Second, the group will work with several ministries to ensure that the Government of Pakistan accepts and recognizes it as a new threat and that the threat from cyberspace is dealt in a manner similar to how terrorism and military aggression are treated. Lastly, Pakistan needs to create a national team for computer emergency response. In order for Pakistan to take action against this newly emerging threat and create a cyber-security strategy for the country, a cyber-Security Task Force with affiliation with the Ministries of Defense, IT, Interior, Foreign Affairs, and Information as well as our security organizations is required. In order to manage cyber security and cyber-defense for the Pakistani military forces as well as for civilian departments, an Inter-Services cyber command should be established. Sixth, to prevent these nations from engaging in cyberwarfare against one another, Pakistan should use the SAARC platform and take the initiative to initiate discussions with other SAARC

members, particularly India. Seventhly, the Senate Defense Committee will host a special media workshop in collaboration with the Pakistan Information Security Association (PISA) to raise public awareness of the subject of cyber security and instruct opinion leaders.[55]

2.10 Progress of Pakistan in The Cyber Domain

Cyberwarfare and information warfare are currently two of 4GW's most important instruments. In this battle, intelligence, surveillance, and reconnaissance are crucial. The military will gain from this in understanding 4GW and developing tactics and procedures. In order for the operations that are to be undertaken to be carried out in a more sophisticated manner, Pakistan should also incorporate and become involved in both of these wars. The traditional military should use non-kinetic measures or unconventional tactics to combat 4GW, including land forces, psychological warfare, cyberwarfare, the internet, and information. Pakistan, a nuclear power, faces the same danger as other nuclear powers. The Credible Minimum Deterrence hereinafter referred as (CMD) nuclear doctrine of Pakistan is clearly a thorough set of guidelines that addresses all choices linked to the perception of a conventional threat, but it has not been revised to reflect the evolving nature of threats. Nuclear assets are also at risk from a single motivated attacker, in addition to the banking sector, educational institutions, and governmental websites. Pakistan continues to fall behind in this area, having nothing in the way of actual risk management policies. Compared to other traditional threats, the cyber domain is significantly complex.

[55] MUHAMMAD BAQIR MALIK, "Pakistan and India Cyber Security Strategy*", Defense Journal* 17, no.11 (2014):59 available at https://www.researchgate.net/profile/BaqirMalik/publication/325825535_South_Asia_Security_Paradigm_An_Introductory_Analysis/links/5b27d66745851509895c8c26/South-Asia-Security-Paradigm-An-Introductory-Analysis.pdf (last accessed: 12 Dec, 2022)

Technology is one of Pakistan's most underdeveloped industries, but India is investing heavily in its high-tech sector with the goal of dominating the cyber sphere and outwitting rivals in the area.

Pakistan needs to intensify its revolutionary efforts in order to both advance its technological growth and raise its position in the global innovation index. Pakistan may find it extremely difficult to protect against cyber-threats against key infrastructure with the current resources at its disposal.[56]

2.11 Conclusion

The threat of cyberwarfare is said to have increased along with the expansion of information and technologies. Pakistan is one of the nations exposed to the new, growing dangers of cyberwarfare and faces cyber security challenges. Pakistan has adopted various domestic legislation as well as various international cyber regulations to address this issue. These rules, however, are not enough to stop the new, developing threat that the internet poses. As a result, Pakistan needs to establish new laws, strategies, and policies to deal with cyber threats in a more effective manner. Information, the internet, and media are now additional traditional and new tools of influence. Yet, up until recently, Pakistan's national security decision-makers focused mostly on kinetic threats, but non-kinetic problems are now slowly but surely becoming more and more of a factor. From Pakistan's perspective, it is currently a field, and bluntly speaking, Pakistan is not prepared to respond strongly if any cyberattack occurs. National Response for Computer Crime Centre and the function of

[56] Rizwan Naseer, Musarat Amin. "Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security", *Research Journal of South Asian Studies* Vol. 33, No. 1 (January – June 2018):35 – 48, available at http://journals.pu.edu.pk/journals/index.php/IJSAS/article/viewFile/3133/1327 (last accessed: Dec 23,2022)

the Pakistan Senate Defense Committee are two alternative ways to discuss Pakistan's cyber security strategy. Pakistan established a cybercrime department in 2007, this was the result of a few things. First of all, it's because more governmental and private institutions rely on the internet. Second, terrorists increasingly communicate over the Internet. Thirdly, India as well as other countries are becoming more adept at using cyber weapons. Fourthly, it aids in gathering intelligence on IT security issues and monitoring worldwide security issues. Last but not least, handle and look into cybercrime to enforce current laws to combat computer-related crimes and to protect customers and Internet users. Yet, the purpose of this center is to halt minor harm and further struggles need to be done in the field of cyber warfare to combat this issue.

CHAPTER 3

PRINCIPLES OF IHL IN THE CONTEXT OF CYBERWARFARE AND SHORTCOMINGS IN THE EXISTING LEGAL SYSTEM OF PAKISTAN

3.1 Introduction

The laws of the world have not been able to keep up with the rapid development of cyberspace due to the cross-sector, multi-jurisdictional, and multi-geographical character of the infrastructure and services offered there. Even when our objectives are in line with one other, the laws that already exist overlap and cause conflict. Governments from all across the world have recently announced that cyberspace is the fifth realm of combat, joining space, land, sea, and air. William J. Lynn III, US Deputy Secretary of Defense, affirmed that as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare which has become just as critical to military operations as land, sea, air, and space[57].

This public acknowledgment by the US government is very significant since it relates to the creation of a new generation of technology and instruments to safeguard the country in the perilous internet realm. Several official and expert reports have been released in the previous few years, including: The Tallinn Manual on the International Law Applicable to Cyberwarfare. This manual was created by an independent

[57] Amit Maitra, "Offensive cyber-weapons: Technical, legal, and strategic aspects*", Environment Systems and Decisions* 35, no.1(2014):169-182, available at: DOI:10.1007/s10669-014-9520-7 (last accessed: Jan 2,2023)

"International Group of Experts" who were invited by the NATO Cooperative Cyber Defense (CCD) Centre of Excellence (COE). It pays particular emphasis to the jus in bello, the international law governing the conduct of armed conflict also known as international humanitarian law, and the jus ad bellum, the international law governing the use of force by States as a tool of their national policy.

Whether war is declared or not, and regardless of whether the parties to an armed conflict recognize one another or not, the laws of armed conflict apply to all instances of armed conflict. The conclusion that IHL applies to cyberwar is not without controversy, despite the fact that the aforementioned statement like many other parts of law related to cyberwar seems ambiguous. This is due to the absence of explicit provisions that specifically address cyberwarfare and other space-related offence.

Currently, the International Committee of the Red Cross the majority of international experts, and many States have come to the conclusion that when there is an armed conflict, IHL also applies to cyber-attacks. Except for the Tallinn manual, which was recommended by several international experts, there is no clear definition available that expressly deals with how IHL shall apply to cyberwar and cyber warfare. Consequently, one must first consider the fundamental ideas and goals of IHL before analyzing specific IHL principles in the context of cyberwarfare.[58]

[58] CDR Peter Pascucci, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution" *Minnesota Journal of International Law* ,26 (2017):419, available at: https://scholarship.law.umn.edu/mjil/257, (last accessed: Jan st,2023)

Cyber warfare has been a hot issue especially after the events in Estonia in 2007 and the discovery of Stuxnet.[59] Cyber-attack incidents that have come up recently, proved that cyber-attacks can cause a devastating effect on the systems that are free from internet and closed to the outside world[60]. To encourage cooperation, the twenty-first century requires new legislation. Data ownership, data processing, data protection and privacy, evidence collection, incident handling, monitoring, and traceability, as well as the rights and obligations linked to data breaches, data transfers, and access to data by law enforcement or intelligence agencies, should all be covered by these laws. The International Court of Justice observed in the Nuclear Weapons advisory opinion[61] The established principles and rules of humanitarian law applicable in armed conflict have an intrinsically humanitarian nature, which permeates the entire law of armed conflict and applies to all types of warfare and weapons, past, present, and future.

3.2 The Meaning of Distinction in International Humanitarian Law

The fundamental idea of differentiation establishes the framework for international humanitarian law. This principle has been referred to as a cardinal principle of international humanitarian law and one of the principles of international customary law by the International Court of Justice.[62] Article 48 of Additional Protocol I, outlines the

[59] Janne Valo, "Cyber Attacks and the Use of Force in International Law", Master's Thesis 2014, University of Helsinki, available at: https://core.ac.uk/download/pdf/19524871.pdf (last accessed: Jan 3,2023)

[60]Andrew N Liaropoulos, "13th European Conference on Cyber Warfare and Security, University of Piraeus, 2014" available at: https://www.academia.edu/7665555/13th_European_Conference_on_Cyber_Warfare_and_Security_University_of_Piraeus_2014 (last accessed: Jan 3,2023)

[61] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1. C.J. Reports 1996, p. 226, available at: https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-EN.pdf (last accessed: Jan 4,2023)

[62]Ahmed, Syed Ghayyur, "Cyberwarfare and the Applicability of the Principle of Distinction" Social Sciene Research Center (December 15, 2018). Available at SSRN: https://ssrn.com/abstract=3301834 (last accessed: Jan 4,2023)

basic principle of distinction: In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[63]

The 1977 Additional Protocol I to the Geneva Convention "Additional Protocol I" illustrates the principle of distinction: A technical term in the laws of armed conflict intended to protect civilian persons and objects. Under this principle, parties to an armed conflict must always distinguish between civilians and civilian objects on the one hand, and combatants and military targets on the other.[64] Civilians and civilian-related objects are prohibited from becoming the targets of attacks under Additional Protocol I. The treaty forbids belligerents from destroying items necessary for the life of the civilian population, like as food, animals, agricultural crops, drinking water supply, and irrigation systems. Therefore, States must never employ weapons that cannot discriminate between military and civilian targets.

3.3 Cyber Warfare and Principle of Distinction under IHL

When a cyber-operation uses cyber means or methods of warfare that produce or are reasonably anticipated to produce violent effects, it qualifies as an attack under Article 49(1) of Additional Protocol I. If a cyber-operation results in or is likely to result in a loss

[63] "1949 Additional Protocols and-their Commentaries", Available at; https://ihl-databases.icrc.org/en/ihl-treaties/geneva-conventions (last accessed: Jan 4,2023)

[64] PROTOCOL ADDITIONAL TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, AND RELATING TO THE PROTECTION OF VICTIMS OF INTERNATIONAL ARMED CONFLICTS (PROTOCOL I), OF 8 JUNE 1977, available at: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf

of life, personal injury or more substantial material damage to property, it is considered an attack, and the law of targeting, including the principle of distinction, is fully applicable.[65]

It is the responsibility of belligerents to take all precautions possible to minimize the loss of human lives and damage to civilian property while conducting military operations. Attacks must be limited by military leaders to just attacking military targets, which are defined in the treaty such as those objects that 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. It is the responsibility of the belligerents to use extra caution while pursuing their objectives in order to protect the environment and works and installations that contain dangerous forces, such as dams and nuclear power plants, among other things. Additionally, it is against the law for belligerents to launch attacks with the primary intent of terrorizing the civilian populace. The principle of differentiation will probably play a significant role in defining the military operation in actions carrying higher chances of civilian casualties, such as the strike on an air defense network. IHL mandates that military leaders must not only be aware of the target of an attack but also be able to foresee all potential outcomes.

The principle of distinction would require the commander to determine whether such a strategy was the best way to achieve the expected military advantage while minimizing the loss of civilian lives if the commander believed that the false messages and targets sent to an air defense network could more risk relief planes or commercial aircraft.

[65] Marco Roscini, "The United Nations Security Council and the Enforcement of International Humanitarian Law" *Israel Law Review*, Vol. 43 (2010)pp. 330-359, Available at SSRN: https://ssrn.com/abstract=1767983 (last accessed: Jan 5,2023)

Again, the principle would probably need a modification to the operation's scope to eliminate the threat to civilians. In other words, a cyberattack that is the "direct and intentional cause of civilian death and destruction" will probably be prohibited by IHL. Examples of this kind of attack include interference with an air traffic control system that led to the crash of a passenger aero plane or the manipulation of a medical database that resulted in civilians or injured troops receiving transfusions of the wrong blood type. A military commander should forego such attacks due to the high civilian fatality rate, probability of unnecessary harm, and lack of a certain military advantage. Similarly, IHL will ban any cyber-attack that would seriously damage the environment or cause the release of natural forces in violation of Articles 54[66], 55[67]and 56[68] of Additional Protocol I. Again, for these attacks, the use of a cyber-weapon would not change the analysis.[69]

Cyber force, unlike CNE operations, can be qualified as a use of "armed" force in the sense of Article 2 para. 4. On the other hand, only large scale cyber-attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self- defense under Article 51 of the UN Charter.[70]

---

[66] IHL Treaties, Article 54, available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-54 (last accessed; JAN 5, 2023)

[67]Article 55: Protection of the natural environment, available at: https://ihl-databases.icrc.org (last accessed: Jan 6,2023)

[68] Article 56: Protection of works and installations containing dangerous forces, Available at: https://ihl- databases.icrc.org/ihl/WebART/470-750071 (last accessed: Jan 6, 2023)

[69] Jeffrey T. Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare" *Michigan Law Review,* vol.107,no.7(2010) Available at: https://repository.law.umich.edu/mlr/vol106/iss7/6 (last accessed: Jan 7,2023)

[70] Marco Roscini., "Worldwide warfare: Jus ad bellum and the use of cyber force", in: von Bogdandy, A., Wolfrum, R. and Philipp, C.E. (ed.) Max Planck Yearbook of United Nations Law Leiden (Martinus Nijhoff) pp. 85-130.

3.4 Legal status of cyber space

It is neither necessary nor necessary for the creation of new international norms for state behavior in cyberspace to replace those that already exist. In both peacetime and armed conflict, established international principles that govern state behavior also apply online. However, because of the particular characteristics of networked technology, more research is needed to determine how these norms apply and what other knowledge would be required to support them. Existing international rules and principles will continue to apply to cyberspace followed by calls for responsible behavior by States or non-state actors. Undoubtedly, international law shapes State behaviors and interests in cyberspace and perhaps rationalizes them but it rarely pre-empts legislation.[71]

Cyber warfare is a practice that is now expanding so quickly and does not have a clear international legal framework to regulate it that there is no established case law on the subject. Although there is some limited State practice related to cyber war there is no treaty that specifically addresses it, and there is hardly any evidence of the opinio juris necessary to convert it into normative customary international law. What published authority there is for sources of international law on the subject, as defined in Article 38(1) of the Statute of the International Court of Justice, is at present restricted to the subsidiary source of academic commentary. It is therefore rather difficult to write authoritatively about international law and CW: one has a distinct feeling of the ink not yet being dry on the page. Nevertheless, it is submitted that as CW exists as a matter of

[71] Michael N. Schmitt, "Introduction to the Research Handbook on International Law and Cyberspace." In *Research Handbook on International Law and Cyberspace*, (Edward Elgar Publishing, 2021) 1-7, available at https://doi.org/10.4337/9781789904253.00008 (last accessed: Jan 7,2023)

fact, it cannot do so in a legal vacuum: discussion of the phenomenon must take place within the parameters of the Lex- lata of IHL.[72]

In both peacetime and armed conflict, established international principles that govern state behavior also apply online. However, because of the particular characteristics of networked technology, more research is needed to determine how these norms apply and what other knowledge would be required to support them. Existing international rules and principles will continue to apply to cyberspace followed by calls for responsible behavior by States or non-state actors. Undoubtedly, international law shapes State behaviors and interests in cyberspace and perhaps rationalizes them but it rarely pre-empts legislation.[73]

Cyber warfare is a practice that is now expanding so quickly and does not have a clear international legal framework to regulate it that there is no established case law on the subject. Although there is some limited State practice related to CW, there is no treaty that specifically addresses it, and there is hardly any evidence of the Opinio Juris necessary to convert it into normative customary international law. What published authority there is for sources of international law on the subject, as defined in Article 38(1) of the Statute of the International Court of Justice, is at present restricted to the subsidiary source of academic commentary. It is therefore rather difficult to write authoritatively about international law and CW: one has a distinct feeling of the ink not yet being dry on

[72] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities" *Journal of Conflict and Security Law*, Volume 17, No 2 (2012):279–297, Available at: https://doi.org/10.1093/jcsl/krs021 (last accessed: Jan 8,2023)

[73] Michael N. Schmitt, "Introduction to the Research Handbook on International Law and Cyberspace." In *Research Handbook on International Law and Cyberspace*, (Edward Elgar Publishing, 2021) 1-7, available at https://doi.org/10.4337/9781789904253.00008 (last accessed: Jan 7,2023)

the page. Nevertheless, it is submitted that as CW exists as a matter of fact, it cannot do so in a legal vacuum: discussion of the phenomenon must take place within the parameters of the Lex- lata of IHL.[74]

3.5 Rules Governing Military Operations other than Attacks

IHL forbids attacks that use weapons and tactics, including cyber weapons and tactics, that can't be targeted at a particular military objective, may be expected to evade the user's control, or, even when targeted at a military objective, may be expected to cause incidental civilian damage that is excessive compared to the concrete and direct military advantage anticipated. Article 49 of additional protocol says that Attacks means acts of violence against the adversary, whether in offence or in defense.[75]

It is well established that the notion of violence in this definition can refer to either the means of warfare or their effects, meaning that an operation causing violent effects can be an attack even if the means used to cause those effects are not violent as such.[76]The notion of "military operation" appears in a number of articles of the 1949 Geneva Conventions and their 1977 Additional Protocols. Of most interest here are the rules that regulate the conduct of military operations, including those carried out by cyber means. They include the basic rule that "parties to the conflict shall direct their operations only against military objectives" (AP I, Article 48), the principle that "the civilian population and individual

[74] David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities" *Journal of Conflict and Security Law*, Volume 17, No 2 (2012):279–297, Available at: https://doi.org/10.1093/jcsl/krs021 (last accessed: Jan 8,2023)

[75] Article 49 - Definition of attacks and scope of application, available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49 (last accessed: Jan 8, 2023)

[76] Laurent Gisel, Tilman Rodenhäuser, Knut Dörmann, Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts." *International Review of the Red Cross* 102, no. 913 (2020): 287–334, Available at: doi:10.1017/S1816383120000387 (last accessed: Jan 9, 2023)

civilians shall enjoy general protection against dangers arising from military Operations" (AP I, Article 51(1)), and the obligation that "constant care shall be taken to spare the civilian population, civilians and civilian objects" in the conduct of military operations (AP I, Article 57(1)). It is usually a significant advance above current legislation since it not only codifies the proportionality principle for the first time but also provides military commanders with generally accepted guidelines on their duty to protect civilians and the civilian population.[77]

The ICRC Commentary on Article 48 of AP I notes that the notion refers to military operations during which violence is used, and not to ideological, political or religious campaigns, it clarifies that it is a broader notion than attacks. The Commentary defines "military operations" for the purpose of these articles as any movements, man oeuvres and other activities whatsoever carried out by the armed forces with a view to combat or related to hostilities an understanding that is widely accepted. Those Cyber operations that do not amount to "military operation" as assumed in AP I might be regulated by some IHL rules stemming from the principle of distinction. For example, it has been noted that directing psychological operations or other types of propaganda at civilians would not violate Article 48 of AP I because these operations would not fall within the meaning of military operations as understood in Article 48. These acts must not be amount to an act of terror or IHL violations.

With regard specifically to the novelty of a weapon, Article 36 of Additional

[77]Antonio Cassese, "The Geneva Protocols of 1977 on the Humanitarian Law of Armed Conflict and Customary International Law", *UCLA Pacific Basin Law Journal*, 3, no.1-2(1984) available at: DOI
10.5070/P831-2021915 (last accessed: Jan 10, 2023)

Protocol I of 1977 stipulates that: In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine Whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[78]

3.6 Principle of Proportionality

The AP I targeting laws describe the proportionality principle, which prohibits States from causing excessive collateral or incidental injury or damage. Specifically, Article 51(5)(b) prohibits States from attacking when such an "attack 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." "In case of doubt whether a person is a civilian" and not a combatant or "whether an object which is normally dedicated to civilian purposes makes an effective contribution to military action," a presumption of immunity is required. The principle of proportionality prohibits indiscriminate attacks, that is, attacks that cause incidental loss of life or injury to civilians, damage or destruction to objects, or a combination thereof, which Would be excessive in relation to the military advantage expected from the operation.[79]

All tactics and techniques of warfare that inflict unnecessary pain on soldiers, that is, who inflict suffering with no discernible military benefit, are forbidden. Weapon

[78]International Humanitarian Law Databases, Available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-36, (last accessed: Jan 10,2023)

[79] Giacomo Biggio, "Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects", *Canadian Journal of Law and Technology*, 15, no.1(2017):1-14, available at: https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1161&context=cjlt (last accessed: Jan 10,2023)

systems that cannot be pointed at a particular military objective are likewise forbidden by international humanitarian law. These weapons are illegal by definition since they can be used to strike without discrimination civilians, military targets, combatants, and civilian objects. The international humanitarian law regulations, such as those governing the employment of weapon systems intended to protect people, civilian property, and other protected persons and locations during hostilities, are founded on the principle of distinction.[80]

Due to the nature of computers and cyber networks, their interconnection, and reliance on civil infrastructure, a proportionality analysis will nearly always be required. While proportionality aims to prevent "reckless" attacks, it does not impose any restrictions on commanders' options. In addition, a commander would choose a cyberattack over a kinetic strike if the commander reasonably anticipated, say, three civilian casualties, even though the cyberattack might cause collateral damage that destroys terabytes of data, including medical records and other important civilian data. Similar to this, defining "damage" in cyberspace will

[80] Michael N. Schmitt, "Autonomous weapon systems and international humanitarian law: a reply to the critics" *Harvard National Security Journal*, 4 (2013):1-37. Available at http://centaur.reading.ac.uk/89864/ (last accessed: Jan 11,2023)

be crucial to establishing effective defenses. A cyber-attack, for instance may have a variety of repercussions, ranging from those that result in a brief, reversible loss of use to those that result in physical harm and devastation. A necessary prerequisite to determining whether the injury or damage is excessive in relation to the anticipated direct and concrete military advantage is determining which of these effects qualifies as "damage" for IHL's purposes. This principle necessitates taking into account both direct and knock-on, or indirect, effects of attacks. The Tallinn Manual's experts acknowledged the special characteristics of the proportionality analysis in cyberwar. In the commentary to rule 113 (Proportionality), the experts noted that "a cyber-attack can cause collateral damage during transit and because of the cyber-attack itself."[81]

3.7 Principle of Necessity

The application of International Humanitarian Law (IHL) is an attempt to achieve an equitable balance between humanitarian requirements and the necessities of war.[82]like distinction and proportionality, the principle of necessity narrows permissible targeting. AP I strictly limits "attacks" to "military objectives." Article 52(2) prohibits attacks that do not "offer a definite military advantage." "Attack 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

[81] CDR Peter Pascucci, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution", *Minnesota Journal of International Law,* 26(2017):419, available at: https://scholarship.law.umn.edu/mjil/257/ (last accessed: Jan 11, 2023)

[82] Dan Saxon, ed. "International humanitarian law and the changing technology of war" (Martinus Nijhoff Publishers, 2013) available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Dan+Saxon%2C+International+Humanitarian+Law+and+the+Changing+Technology+of+War&btnG= (last accessed: Jan 12, 2023)

circumstances ruling at the time, offers a definite military advantage."[83]In essence, States are not allowed to attack individuals or things unless it is absolutely essential in order to prevent further suffering.

Because it doesn't address targeting problems specific to cyberspace or, at the very least, leaves these cyber challenges open to expansive interpretation, the current targeting law system under AP I is insufficient. Certainly, general IHL principles apply and cyber warfare does not completely operate in vacuum. However, IHL currently fails to address certain aggressive behavior unique to cyber warfare as illustrated above that the international community should prohibit. While targeting principles of distinction, proportionality, and necessity apply generally to all methods of warfare, the international community should strive to define parameters specific to the cyber domain as it has under AP I for land warfare. Otherwise, States will increasingly develop and employ devastating cyber tactics and techniques with little-to-no regard for IHL targeting laws. States are not unaccustomed to reforming IHL in response to new means of warfare.[84]

3.8 The Principle of Precaution

This principle has two aspects which include precautions in attack and precaution against the effect of attacks. Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 48,

[83] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and (last accessed: Jan 11,2023)

[84] Christian H. Robertson II, Different Problems Require Different Solutions: How Air Warfare Norms Should Inform IHL Targeting Law Reform & Cyber Warfare, *University of Michigan Journal of Law Reform*, 52, no.4 (2019):984. Available at: https://repository.law.umich.edu/mjlr/vol52/iss4/9 (last accessed: Jan 12, 2023)

49. Under this principle, IHL mandates that all reasonable efforts be made to verify that targets are military objectives, (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (a) (I)) as well that all feasible precautions in the selection of means and methods of warfare with the goal of avoiding or, at the very least, minimizing incidental civilian causalities and damage to civilian casualties and damage to civilian objects (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (a) (ii)).)). It

Also mandates that if it becomes clear that an attack would inflict considerable "collateral damage", the parties to the dispute must cancel or suspend the attack (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (b)). Many States has defined the word "feasible": "as being limited to those precautions which are practicable or practically possible, taking into account all circumstances ruling at the time.

In addition, when deciding between various military objectives with a similar military advantage, the attacker must take 'constant care' and 'reasonable precautions' to spare the civilian population and civilian objects (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (1)). In the cyber context, the 'constant care' means the entire person involve must be continuously sensitive to the effect of their activities at all times, not merely during preparation (Schmitt, 2017, p. 474).[85]The precautions against the effect of attacks require parties to the conflict "to the maximum extent feasible to remove the civilian population, individual civilians and civilian objects under their control" (Protocols Additional to the Geneva Conventions of 12 August 1949,

[85] Zuhra, Amalia, and Laila Almira. "THE LIMITATION OF CYBER WARFARE UNDER HUMANITARIAN LAW." *Teras law review*, 3, No.1 (2021): 1-10, Available at: https://doi.org/10.25105/teras-lrev.v3i1.10741 (last accessed: Jan 13, 2023)

Art. 58). However, in the context of cyber Tallinn Manual states, certain actions that need to be taken include: "segregating military from civilian cyber infrastructure; segregating computer systems on which critical civilian infrastructure depends from the Internet; backing up important civilian data elsewhere; making advance arrangements to ensure the timely repair of important computer systems against foreseeable kinds of cyber-attack; digitally recording important cultural or spiritual objects to facilitate reconstruction in the event of their destruction during armed conflict; and using antivirus measures to protect civilian systems that might suffer damage or destruction during an attack on military cyber infrastructure" (Schmitt, Op. Cit., 488). Unlike other principles that mention about the condition of dual-use, this principle strictly prohibited the dual-use and stated that it should keep distinct.

3.9 Compliance of Principles Of IHL With The New Means And Methods Of Cyber Warfare

Today, warfare is changing. Cyber operations have become a reality of armed conflict, and States are increasingly developing military cyber capabilities. Such developments come with risks, but they may also provide opportunities. New actors and new activities are seriously shaking the foundations of IHL by contesting its core values, in particular the distinction between combatants and civilians.[86]

The use of cyber operations during hostilities could have terrible humanitarian repercussions. It is critical for the ICRC to find measures to reduce the humanitarian cost

[86] Quénivet, Noëlle. "The War on Terror and the Principle of Distinction in International Humanitarian Law." *ACDI* 3 (2010): 155. available at: https://scholar.google.com/scholar?hl=en (last accessed: Jan 13, 2023).

of cyber operations and, in particular, to reiterate the applicability of IHL to this cutting-edge technology when it is applied to armed conflict. This is exactly what the Tallinn Manual's experts advise.

The Geneva Conventions were created in 1949, but the means and methods of war have changed since then. Nevertheless, IHL still applies to all actions taken by parties during an armed conflict and must be observed. However, it cannot be ruled out that when cyber technologies advance or their humanitarian impact is more recognized, it may be necessary to develop the law further to ensure that it offers the necessary protection to the civilian population. States will have to make that decision.

Although the Tallinn Manual is a non-binding document created by a group of experts, we certainly hope that it can contribute usefully to further discussion among States on these difficult issues and that States and non-State armed groups will ensure that any use of cyber operations in armed conflict will be in accordance with their international obligations. The interpretation and application of international law, particularly IHL, to State and non-State activities taking place in cyberspace are currently hotly contested topics. To meet these challenges, the ICRC will keep extending its IHL knowledge.

Assessing the legality of new weapons is in the interest of all States, as it will help them ensure that their armed forces act in accordance with their international obligations. Article 36 of the 1977 Protocol I additional to the Geneva Conventions requires each State party To make sure that any new weapons it deploys or considers deploying comply with

the Rules of IHL, another point usefully recalled by the Tallinn Manual.[87]

States parties to the Geneva Conventions called for "rigorous and multidisciplinary review" of new weapons, means, and methods of warfare at the 28th International Conference of the Red Cross and Red Crescent in 2003 in order to prevent the protection provided by the law from being surpassed by technological advancement. An ideal illustration of such rapid technological advancement is the use of cyber operations in armed conflict.

3.10 Shortcomings in The Existing Strategies Of Pakistan

Pakistan's standing in this particular area is still poor since the government hasn't given it much thought because its policymakers don't see it as a serious threat.[88] Pakistan is threatened by several outside forces using the cyberspace conundrum. Pakistan has been attempting to strengthen cyber security capabilities in the previous few years, particularly for the banking, telecom, military, and governmental sectors. The tragedy that occurred on Pakistan's 70th Independence Day provides evidence that these measures are not being pursued seriously. Following a coordinated cyberattack in which the hackers displayed "an Indian flag and a Happy Independence Day for India message on those websites," many of the nation's important ministries' websites were compromised. After that, Pakistan Telecommunication Authority (PTA) shut down the hacked websites, embarrassing the relevant authorities. Although protecting sensitive information is the

[87] "Cyberwarfare and international humanitarian law: the ICRC's position", last modified: 6, 2013, available at: https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (last accessed: Jan 14, 2023)

[88] Jawad awan, Shehzad memon, "Threats of Cyber Security and Challenges for Pakistan," (paper presented at 11th International Conference on Cyber Warfare and Security, USA, March, 2016), available at: https://www.researchgate.net/publication/318850748_Threats_of_Cyber_Security_and_Challenges_for_Pakistan (last accessed: Jan 14, 2023)

government's top priority, Pakistan's cyber services are still in their infancy. The primary issue in Pakistan and the major objective of cyber attackers is the theft of personal information.

In 2015, 25% of Pakistan's Cyber threats were Advanced Persistent Threats (APTs), in which an unauthorized user gains access to a network.33 Malware attacks, zero-day attacks, and insider threats continue to target Pakistan. These attacks made up 23%, 13.5%, and 13.5% of all attacks in 2015, respectively.

The Federal Investigation organization (FIA), the organization in question in Pakistan, lacked the skills necessary to handle such assaults. It was claimed that the department in charge of thwarting such attacks was unable to retrieve information about attacks made possible by TOR proxies, a program that allows users to obtain online anonymity. In 2016, Pakistan passed the Prevention of Electronic Crimes Act, which outlined penalties for cybercriminals.

With regard to certain infractions, the statute suggested both penalties and jail time. In addition, the development of Computer Emergency Response Teams was also mentioned in the provision for dealing with threats to essential infrastructure or information data. But these laws usually target internal issues, but overseas cyberattacks are much more harmful and a threat to Pakistan's national integrity.[89]

If we examine the technical and legal capacities of impoverished nations in the area of cyberspace, we discover that they are more advanced than Pakistan. Six million

[89] Sarmad Ali khan, "Cyber Warfare As A Non-Kinetic Threat: Implications For Pakistan," *NEW WORLD ARCHITECTURE OF ECONOMY AND SECURITY (*2019):477-492, available at: https://www.researchgate.net/publication/350387403_CYBER_WARFARE_AS_A_NON-KINETIC_THREAT_IMPLICATIONS_FOR_PAKISTAN (last accessed: Jan 15, 2023)

dollars were lost by Tanzania as a result of various online crimes.[90] This forced the Tanzanian government to build its cyber security infrastructure and skills, which resulted in the creation of the Computer Emergency Response Team (CERT) and Cyber Crime Unit (CCU).

On the other hand, Pakistan does not possess any such capabilities that can stop or neutralize a complex threat. Even old malware like Stuxnet could end up weakening Pakistan's cyber defenses. The then-Pakistani government established the Cyber Crime Wing in 2003, but it has not developed to address threats from the outside. Instead, it focuses on internal problems like cyber-harassment and cyber-theft. The NR3C in 2007, although it hasn't done anything to fulfil its objectives. Many domestic scholars and analysts contend that the nation urgently needs to build its cyberwarfare capabilities by hiring computer specialists skilled in dealing with a wide range of hardware and software threats.

The structural difficulty is just one of the many difficulties Pakistan faces in cyberwarfare. The politicization of cyberwarfare comprises these structural dislocations: attribution, cooperation, regulation, and communication. Cyberwarfare is frequently seen as being offensive in nature, which is why it has a bad reputation. Cybersecurity, however, is a component of cyberwarfare, which tries to defend a nation from network-centric assaults. This misunderstanding encourages more adaptable behavior while implementing a cyber-security or cyber-warfare strategy.

[90] Edephonce Ngemera Nfuka, The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania*?*, *INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE M. Mshangi et al., Vol. 3, No. 2,* available at: https://dergipark.org.tr/en/download/article-file/147965

Any sort of conflict or war has the ability to affect every person, whether they are a soldier, a combatant's relative, a civilian, a company, or a nation state. Because of this, it is beneficial and crucial to conduct study on cyberwarfare in order to address the challenges that this new kind of warfare has brought.[91] Cyberwarfare transcends both temporal and spatial bounds. Because of the spread of technology and easy access to information, anyone sitting anywhere in the world may launch cyberattacks on a budget. According to Bachmann, alongside terrorism and WMDs, NATO has identified cyber-warfare as one of the major hybrid threats to international peace and security in the modern era. 2015 (Bachmann).[92]

As India has an advantage over Pakistan in the field of information technology, it appears that Pakistan lags behind in cyberspace technologies. Pakistan was placed 131st out of 141 nations in the World Innovation Index 2015 (the lowest ranking in South Asia), while India was 81st, Sri Lanka was 85th, and Bangladesh was 129th (World Intellectual Property Organization, 2015). It should be emphasized, nevertheless, that Pakistan has recently implemented numerous network solutions into daily life, from banking services to e-governance in the form of web-based services and mobile applications. Due to these changes, Pakistan has fallen from 52nd place in the World Innovation Index 2019 to 105th place, whereas India, Sri Lanka, Bangladesh, and Bangladesh were all placed higher

[91] Michael Robinson, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." *Computers & security* 49 (2015): 70-94, available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Michael+Robinson%2C+Kevin+Jones%2C+Helge+Janice%2C+Cyber+warfare%3A+Issues+and+challenges%2C+March+2015%2C+https%3A%2F% (last accessed: Jan 15,2023)

[92] Sascha-Dominik Bachmann, "Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats-mapping the new frontier of global risk and security management." *Amicus Curiae* 88 (2011): 24, available at: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Bachmann%2C+Sascha-Dominik.+%22Hybrid+threats%2C+cyber+warfare (last accessed: Jan 15, 2023)

(World Intellectual Property Organization, 2015). As a result, it can be inferred from the table below that while Pakistan has made progress in this area, India and Sri Lanka still outpace Pakistan in terms of cyberspace innovation.[93]

Several organizations are working independently to improve redundancy in this area, but there is a lack of coordination among the national efforts. Even the security organizations operate in their own realms and require further cooperation for a thorough response. Although cybercrimes are pervasive in modern society, the majority of them go unnoticed. Additionally, it is increasingly normal practice to hack data using creative methods and even to steal money from bank accounts. In keeping with worldwide trends, cybercrime has increased swiftly and has impacted many facets of society. Although there have been general awareness efforts launched by numerous departments and people are becoming more aware in this respect, there is still room for improvement.

[93] Tahir Mahmood Azad, and Muhammad Waqas Haider. "Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan." *South Asian Studies* 36, no. 2 (2022):383-398, available at: http://journals.pu.edu.pk/journals/index.php/IJSAS/article/viewFile/5998/2751 (last accessed: Jan 16,2023)

To ascertain if the laws of war are even applicable in the case of a cyberattack. The 1949 Geneva Conventions, the 1977 Additional Protocols, the multiple 1899 and 1907 Hague Conventions, and customary international law make up the laws of war. They consist of the two main categories of rules and are only relevant during times of armed conflict: Firstly, laws that restrict the parties' ability to wage war, and secondly, laws that safeguard people and property during armed conflict. The laws of war do not specifically mention cyber-warfare. The absence of a specific reference does not imply that it is exempt from the use of the laws of war or that unrestricted cyberattacks are permissible. The Geneva Conventions and The Hague Conventions were created in 1949 and 1899 and 1907, respectively, before there was any mention of cyberwarfare, computers, or the internet. A weapon's uniqueness does not imply any legal implications. State parties concur that modern weapons are protected even though many of them are not mentioned in the laws of war. All forms of armed conflict are subject to the laws of armed conflict, which have an inherent humanitarian nature.[94]

In fact, state parties expected that there would be gaps in the legislation but that it should still be applicable. The laws of war contain a number of stipulations that lend credence to this idea. These clauses are the so-called Martens Clause, Article 36 of Additional Protocol I of 1977, and the St. Petersburg Declaration of 1868. The St. Petersburg Declaration of 1868 states that: The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future Improvements which science may effect in the armament of troops, in order to

[94] Jenny Gesley. "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime." *Archiv des Völkerrechts* 48, no. 4 (2010): 486-501, Available at: DOI:10.1628/000389210794439416 (last accessed: Jan 17, 2023)

maintain the principles which, they have established and to conciliate the necessities of war with the laws of humanity.

The so-called Martens Clause, which was added to the 1949 Geneva Convention and Article 1 of the two supplementary 1977 Protocols, was first mentioned in the preamble to the 1899 Hague Convention (II) with regard to the rules and customs of war on land and is as follows:

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.[95]

3.11 Conclusion

Any use of force by States cyber or kinetic is governed by the UN Charter, in particular the prohibition against the use of force. International disputes must be settled by peaceful means, in cyber space just like in all other domains. Asserting that IHL applies does not encourage the militarization of cyberspace or legitimize cyber-warfare. Instead, it affirms existing protection for civilian populations in the unfortunate event of an armed conflict and, in fact, limits the type of means and methods of warfare that may be developed in case States decide to militarize cyberspace.

From a legal point of view, there should be no doubt that existing IHL principles and rules apply to new weapons, means and methods of warfare, including those relying

[95] Rupert Ticehurst, " The Advisory Opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons, "*War Studies Journal*, Autumn 2(1), 1996, pp. 107-118, available at: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm

on information and telecommunications technology. When States adopt IHL treaties, they do so to regulate future conflicts. States have included rules that anticipate the development of new means and methods of warfare in IHL treaties, presuming that IHL will apply to them. For instance, if IHL did not apply to future means and methods of warfare, it would not be necessary to review their lawfulness under existing IHL, as required by Article 36 of the 1977 First Additional Protocol. Moreover, in the Advisory Opinion on the legality of the threat or use of nuclear weapons the International Court of Justice the Court recalled in paragraph 86 that the established principles and rules of humanitarian law applicable in armed conflict apply 'to all forms of warfare and to all kinds of weapons, including those of the future.

It is pertinent to mention here that shortcomings in the cyber-security world of Pakistan make it more vulnerable to cyber threats. The insufficient cyber-protection legislation in Pakistan does not address several important cyber-security issues. Pakistan must acknowledge the serious threat to its vital infrastructure and take serious measures to protect the nations linked infrastructure.

CHAPTER 4

CONCLUSION AND RECOMMENDATION

4.1 Conclusion

Research on cyber warfare is expanding and now includes ethical issues as well as the creation of new weapons. There is, however, little agreement over its definition and limitations. Despite this, some national forces have established doctrines for fighting in cyber space and regard it as a realm for warfare. We are entering a novel and untested kind of conflict with hazy international law, thus the lack of understanding and state-level tensions over cyber conflict are worrisome. To address the growing threat of cyberwarfare, a succinct definition of the term is required. States and institutions have different ideas about what constitutes cyberwarfare and cyberspace, although these distinctions are subtler than substantial. The Geneva Conventions, Additional Protocols, and M. N. Schmitt's work all demonstrate that the doctrine of jus in bello can be used to protect against cyberattacks if a consequence-based method is used rather than an actor-based method. Although it doesn't address competency concerns, identify the source of attacks, or assess the appropriate reactions to unidentified adversaries, it does provide the bare minimum protection for protected people and things. While jus ad bellum can extend international rules to cyberattacks, several legal loopholes still exist when it comes to some attacks against civilians and civilian property that do not result in harm or suffering.

A new international cyber treaty may be in the works, according to recent developments, as the existing international laws on cyberwarfare confront significant difficulties. Cyber warfare is legal under current humanitarian law, however there are some issues that need to be resolved. The determination of whether an operation qualifies as an "attack" is essential for the application of regulations derived from the concepts of distinction, proportionality, and prudence, which safeguard civilians and civilian objects. Cyberspace and technology are continuously evolving, thus there must be continuous monitoring and evaluation. Armed forces have the option of attaining their goals without directly harming civilians or physically destroying civilian infrastructure by deploying cyber technologies as a kind of warfare. Pakistan is a possible target for cyberattacks that steal information and disrupt national assets since it is a nuclear power and a manufacturer of cutting-edge missile technology. It is crucial to defend military equipment, communications, computers, and sites because all branches of the Pakistani military continue to be active targets for cyberwarfare. Additionally, the military should continue to be able to defend its data and assets from highly advanced threat actors and respond to sophisticated cyberattacks. Pakistan has been vulnerable to propaganda as a result of ongoing internal conflicts, including as religious, sectarian, and inter-provincial conflicts, which, if ignored, might have long-term repercussions for its internal stability, politics, and cohesion.

Pakistan ranked 94th in the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) 2018, down from 66th in 2018. The drop was attributed to Pakistan's failure to show progress in the five pillars of the GCI: legal, technical, organizational, capacity building, and cooperation. Other countries have started

demonstrating their commitments towards these pillars. Additionally, compare tech Reports ranks Pakistan as the 7th worst country in terms of cybersecurity. According to The Tribune, 25% of Pakistani mobile devices are infected with malware. This is a worrying statistic because unregulated internet and a lack of cybersecurity awareness expose the general populace to numerous computer viruses.

In order to prevent cyberattacks, industries like communications, finance, oil and gas, and defense must operate independently because Pakistan lacks powerful technological organizations like national Computer Emergency Response Teams (CERT) and sectoral CERTs. This lack of cooperation is especially troubling because these sectors constitute the backbone of the country's infrastructure and successful cyberattacks in one sector can have an impact on the military. For the Pakistani military to successfully detect and counter sophisticated cyberattacks, it lacks an integrated tri-services or Inter-Services Cyber Command (ISC2).

4.2 Recommendation

- Cybercrime and cyberwarfare are global problems that call for global solutions. To tackle cybercrime, a unified cyber law is required.
- There is a need for specialized venues for exchanging knowledge and experiences that include literary, technical, and scientific activities as well as research, teaching, and training.
- Law enforcement authorities, government departments, bar associations, the judiciary, institutions, universities, businesses, and other private organizations should be given access to these actions.

- The NCSC (National Cyber Steering Committee) is in charge of developing a thorough cyber security strategy and policy that takes into account both civil and military sectors, as well as worldwide trends and conventions. The policy should be thorough, guaranteeing Pakistan can build its capacities and successfully use the tools created.
- When employing novel strategies in cyberwarfare, governments must abide by the standards of international humanitarian law. Existing concepts and guidelines can be utilized to define cyber conflicts within the parameters of international humanitarian law until new ones are developed.
- Cyber rules and regulations should be created by a legal agency, and current laws should be improved.
- It is advised that the Ministry of Defence create a "Inter-Services Cyber Command" (ISC2) to defend Pakistan's military services against advanced cyber threats. The ISC2, which is made up of service members from Pakistan's Army, Air Force, Navy, and Military Intelligence Services, will create policies, tactics, and technological solutions to safeguard the military equipment that is deployed across the whole range of the country's armed forces.
- For the interest of both enterprises and customers, Pakistani lawmakers must create cyber policies and regulations that guarantee the security and protection of the IT sector.
- To safeguard civilian cyberspace and boost resilience, the National Cybersecurity Agency (NCSA) should execute a cybersecurity strategy and policy. The organization needs to handle issues and standardize its cyber procedures.

- It is essential to comprehend cyber warfare tactics and spread awareness of them because crime has altered in nature. All cybercrimes, including cyberwarfare, can be deterred using the deterrence principle, and the impact is strongly correlated with the likelihood of identification and the severity of the penalty.
- To improve the security of its digital systems and gain access to the most recent technologies from developed nations, Pakistan should sign up for international or bilateral cyber security treaties.
- In order to secure its cyber system, the government can conduct research and development using skilled hackers and hijackers.
- Making computers required in college and high school can aid the next generation in defending against cyberattacks.
- In order to enforce cyber laws and punish offenders severely, the government should create legislative committees. This will aid Pakistan in protecting and securing its digital infrastructure.
- Developing and implementing a cybersecurity system on par with other modern nations ensure effective coordination and planning between civilian and military authorities. This will assist Pakistan in addressing the cybersecurity threat.
- Pakistan needs a national cybersecurity strategy with regulations encompassing data privacy, terrorism, criminality, and cyberwarfare to tackle contemporary cybercrime trends like phishing and the usage of artificial intelligence, regulations should be developed.
- The government should set up research facilities as well as centres of excellence in terrorism, war, and cybercrime.

- To produce human resources and create regulations for diverse cyber domains, the Higher Education Commission should launch cybersecurity courses and establish a cyber-workforce.
- The Pakistani government should concentrate on cyber security and study the approaches taken by developed and first-world nations to counteract cyber threats and secure digital systems against unauthorized access.
- Raising internet user awareness and enforcing stronger regulations can help reduce cybercrime.
- Electronic transaction order (ETO) scope is limited and needs to be redefined as cybercrimes are not covered by ETO, and penalties are less harsh than those under U.S. law. Legislation.

BIBLIOGRAPHY

Ackoski, Jugoslav, and Metodija Dojcinovski. "Cyber terrorism and cyber-crime–threats for cyber security." In Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012. MIT University–Skopje, 2012.

Alexander Amanda , "A Short History of International Humanitarian Law." European Journal of International Law 26, no.1 (2015)

Awan, Jawad Hussain, Shahzad Memon, and Fateh Muhammad Burfat. "Role of Cyber Law and Mitigation Strategies in Perspective of Pakistan to Cope Cyber Threats." International Journal of Cyber Warfare and Terrorism (IJCWT) 9, no. 2 (2019): 29-38.

Awan, Jawad Hussain, Shahzad Memon, Rahat Ali Khan, Abdul Qudoos Noonari, Zahoor Hussain, and Muhammad Usman. "Security strategies to overcome cyber measures, factors and barriers." Eng. Sci. Technol. Int. Res. J 1, no. 1 (2017): 51-58.

Baloch, Rafay. "Cyber Warfare Trends, Tactics and Strategies: Lessons for Pakistan." Journal of Development Policy, Research & Practice (JoDPRP) 3, no. 1 (2019): 23-43.

Baradaran, Nazanin, and Homayoun Habibi. "The Applicability of International Humanitarian law in Cyber warfare." Public Law Studies Quarterly 49, no. 1 (2019): 139-158.

Bernik, Igor. "Cybercrime and cyber warfare." (2014).

Billo, Charles, and Welton Chang. "Cyber warfare." An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS (2004).

Buchan, Russell. "Cyber warfare and the status of anonymous under international humanitarian law." Chinese Journal of International Law 15, no. 4 (2016): 741-772.

B. Gazula Mohan , "Cyber Warfare Conflict Analysis and Case Studies", Working Paper CISL# 2017-10 May 2017,

MALIK MUHAMMAD BAQIR, "Pakistan and India Cyber Security Strategy", Defence Journal 17, no.11 (2014):59

Biggio Giacomo, "Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects", Canadian Journal of Law and Technology, 15, no.1(2017):1-14,

Brecht Daniel , "Cyber Warfare and Cyber Weapons, a Real and Growing Threat", InfoSec Resources, (January 15, 2015):75-105

Chang Zen, , "Cyberwarfare and International Hitarian Law." Creighton Int'l & Comp. LJ 9 (2017): 29. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4262971

Conflict and Customary International Law", UCLA Pacific Basin Law Journal, 3, no.1-2(1984)

Culle Anthony. "The characterization of remote warfare under international humanitarian law." (In Research Handbook on Remote Warfare):pp. 110-132. Edward Elgar Publishing, 2017

Cooper, Frank E. "Federal Agency Investigations: Requirements for the Production of Documents." Michigan Law Review 60, no. 2 (1961): 187-206.

Cyberwarfare and international humanitarian law: the ICRC's position", last modified: 6, 2013

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security." Case studies in information warfare and security: For researchers, teachers and students 72 (2013).

Denagamage, PL, Thalpathawadana,TRMYSB. "International Humanitarian Law and Cyber Warfare: Sufficiency of International Humanitarian Law in Combating Cyber Warfare as a New Phenomenon", South Eastern University Arts Research Session 2015

Diamond Eiten , "Applying International Humanitarian Law to Cyber Warfare", Law and National Security, Selected Issues, Institute for National Security Studies (2014),

Dr.F. Krepinevich Andrew, Jr "Cyber Warfare a "Nuclear Option?" Centre for strategic and Budgetary Assessments, 2012.

F. Krepinevich Andrew. "Cyber Warfare: A "Nuclear Option"? (Centre for Strategic and Budgetary Assessments, August 24, 2012)

Gesley Jenny. "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime." Archiv des Völkerrechts 48, no. 4 (2010): 486-501

Gisel Laurent, Rodenhäuser Tilman, Dörmann Knut, Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts." International Review of the Red Cross 102, no. 913 (2020): 287-334

Hjortdal Magnus , "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence" Journal of Strategic Security 4, no.2 (2014):12

H. Aldrich George , "Prospects for United States Ratification of Additional Protocol I to the 1949 Geneva Conventions." American Journal of International Law 85, no. 1 (1991): 1-20.

Herzog, Stephen. "Revisiting the Estonian cyber attacks: Digital threats and multinational responses." Journal of Strategic Security 4, no. 2 (2011): 49-60.

HOLLIS DUNCAN. "A brief primer on international law and cyberspace." Carnegie Endowment for International Peace, 15 (2021)

Hollis, David. "Cyberwar case study: Georgia 2008." (2011): 1-10.

J. Harknett Richard and Smeets Max , "Cyber campaigns and strategic outcomes", Journal of Strategic Studies, Volume 45, Issue 4(2022): 534-567

Khan, Ghalib, Sobia Bashir, Faisal Shahzad, and Saeed Ullah Jan. "Federal investigation agency against the crime of book piracy in Pakistan." Library Philosophy and Practice (2021): 1-13.

KHAN, Sarmad Ali. "CYBER WARFARE AS A NON-KINETIC THREAT: IMPLICATIONS FOR PAKISTAN."

Kozlowski, Andrzej. "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan." COBISS. MK-ID 95468554 (2014): 236.

L. Caton Jeffrey , "The Land, Space, and Cyberspace Nexus: Evolution of the oldest Military Operations in the Newest Military Domains

M. Archer Emerald , "Crossing the Rubicon: Understanding Cyber Terrorism in the European Context" The European Legacy 19,no. 5(2014)

Mahmood Azad Tahir, and Haider Muhammad Waqas. "Cyber Warfare as an Instrument of Hybrid Warfare: A Case Study of Pakistan." South Asian Studies 36, no. 2 (2022):383-398

Maitra Amit, "Offensive cyber-weapons: Technical, legal, and strategic aspects", Environment Systems and Decisions 35, no.1(2014):169-182

Mirza, Muhammad Nadeem, and Muhammad Shahzad Akram. "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare." Strategic Studies 42, no. 1 (2022): 62-80.

McCallion Jane , "What is cyber warfare?"

Nur Sevis Kamile , seker Ensar , "Cyber warfare: terms, issues, laws and controversies", July 2016, Conference: 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security, DOI:10.1109/CyberSecPODS.2016.7502348)

N. Schmitt Michael, "Introduction to the Research Handbook on International Law and Cyberspace." In Research Handbook on International Law and Cyberspace, (Edward Elgar Publishing, 2021) 1-7,

N. Schmitt Michael, "Autonomous weapon systems and international humanitarian law: a reply to the critics" Harvard National Security Journal, 4 (2013):1-37

Naseer Rizwan, Amin Musarat. "Cyber-Threats to Strategic Networks: Challenges for Pakistan's Security", Research Journal of South Asian Studies Vol. 33, No. 1 (January - June 2018):35 – 48

Ottis, Rain. "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective." In Proceedings of the 7th European Conference on Information Warfare, p. 163. Reading, MA: Academic Publishing Limited, 2008.

Paganini Pierluigi , "NATO and definition Rules For Cyber Warfare," Cyber Defence Magazine, March 21,2013

Paganini Pierluigi , "Cyber Warfare: From Attribution to Deterrence". InfoSec resources (October 3, 2016)

Pascucci Peter CDR, "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution" Minnesota Journal of International Law ,26 (2017):419

Protocols additional to the Geneva Conventions of 12 August 1949

Paul, Cornish,Livingstone David , Clemente Dave , and Yorke Claire , "On cyber warfare", (London: Chatham House), 2010.

Philip Faga Hemen , "THE IMPLICATIONS OF TRANSNATIONAL CYBER THREATS IN INTERNATIONAL HUMANITARIAN LAW: ANALYSING THE DISTINCTION BETWEEN CYBERCRIME, CYBER ATTACK, AND

CYBER WARFARE IN THE 21ST CENTURY" Baltic Journal of Law & Politics 10, no.1 (2017): 1-34

Pallin, Carolina Vendil, and Fredrik Westerlund. "Russia's war in Georgia: lessons and consequences." In Crisis in the Caucasus: Russia, Georgia and the West, pp. 150-174. Routledge, 2013.

Rein, David B., Diane Orenstein, Roberta T. Constantine, Hong Chen, Patricia Jones, J. Nell Brownstein, and Rosanne Farris. "Peer Reviewed: A Cost Evaluation of the Georgia Stroke and Heart Attack Prevention Program." Preventing chronic disease 3, no. 1 (2006).

Robinson Michael , Jones Keven , Janicke Helge , "Cyber warfare: Issues and challenges", Ma, Computers & Security 49:70-94, DOI:10.1016/j.cose.2014.11.007 rch 2015, Computers & Security 49:70-94, DOI:10.1016/j.cose.2014.11.007 Jeffrey L. Caton, "The Land, Space, and Cyberspace Nexus: Evolution of the oldest Military Operations in the Newest Military Domains"

Roguski, Przemysław. "Russian cyber attacks against Georgia, public attributions and sovereignty in cyberspace." (2020).

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." *Survival* 53, no. 1 (2011): 23-40.

Darıcılı, Ali Burak. "ANALYSIS OF IRAN'S CYBER SECURITY STRATEGY WITH REGARD TO THE ATTACK AND THE DEFENSE CAPACITY." *Turkish Studies-Social Sciences* (2019).

Iasiello, Emilio. "Cyber attack: A dull tool to shape foreign policy." In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pp. 1-18. IEEE, 2013.

Shackelford, Scott. "Estonia two-and-a-half years later: a progress report on combating cyber attacks." *Journal of Internet Law, Forthcoming* (2009).

SHIN BeomChul , " An Inquiry on the Interpretation of Article 2(4) of the UN Charter and Its Implications for the Jus Ad Bellum" (Final Draft for the S.J.D. Dissertation May 2010)

Subah Maliha Nishat , "Cyber Warfare: Challenges In The Application Of International Humanitarian Law To Virtual Conflict"(Research monograph, Department of Law University of Dhaka august 30,2020)

Syed Ghayyur Ahmed, , "Cyberwarfare and the Applicability of the Principle of Distinction" Social Sciene Research Center (December 15, 2018)

[1]"Treaties, States Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977"

Taddeo Mariarosaria.,, "An analysis for a just cyber warfare." *In 2012 4th international conference on cyber conflict (CYCON 2012), pp. 1-10. IEEE, 2012.*

TALBOT JENSEN ERIC, "THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS", GEORGETOWN JOURNAL OF INTERNATIONAL LAW, Vol. 48(2017):735,

THE ELECTRONIC TRANSACTIONS ORDINANCE, 2002", Pakistan code

Zahra, Iradhati, Irawati Handayani, and Diajeng Wulan Christianti. "Cyber-Attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law." *Yustisia Jurnal Hukum 10, no. 1 (2021): 48-66.*