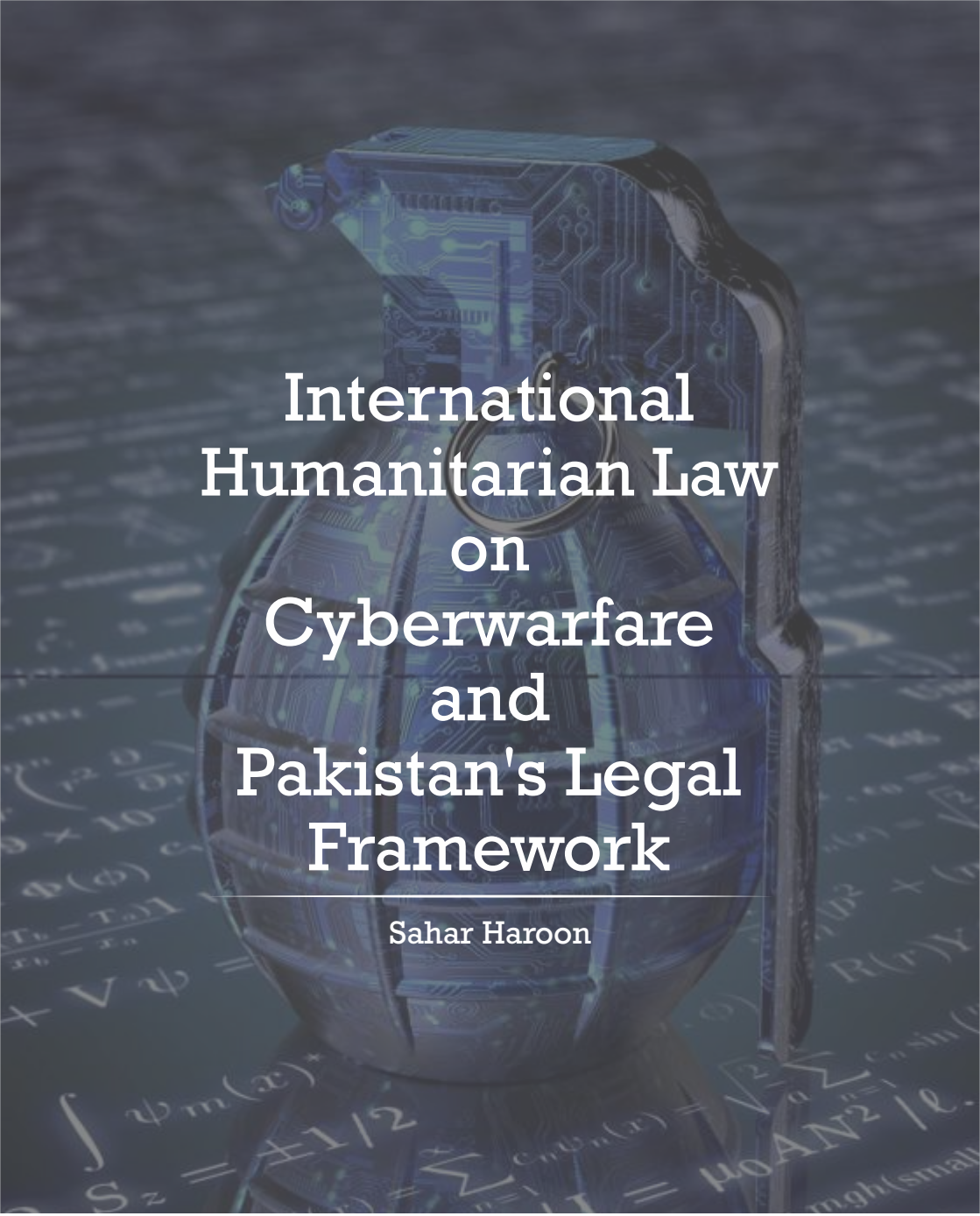


International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework

Sahar Haroon

RSIL
RESEARCH SOCIETY OF INTERNATIONAL LAW PAKISTAN

International Humanitarian Law on Cyberwarfare and Pakistan's Legal Framework

Sahar Haroon
Research Associate
Conflict Law Centre, RSIL

THE RESEARCH SOCIETY OF INTERNATIONAL LAW

The Research Society of International Law is a research and policy institution whose mission is to conduct research into the intersection between international law and the Pakistani legal context. RSIL was founded in 1993 by Mr. Ahmer Bilal Soofi, Advocate Supreme Court of Pakistan, and aims to inform policy formulation on a national level through its efforts. The Society is a non-partisan and apolitical organization, dedicated to examining the critical issues of law - international as well as domestic - with the intention of informing discourse on issues of national importance and effecting positive change in the domestic legal space.

To this end, RSIL engages in academic research, policy analysis and an approach of engagement with policy-makers and stakeholders in the domestic and international politico-legal contexts in order to better articulate meaningful and insightful national positions on these matters.

RSIL is staffed by a team of dedicated researchers and practitioners with a broad spectrum of specializations within international law, whose expertise covers the major policy areas and significant issues arising out of the intersection between the international and domestic legal spaces. The team contributes to the domestic legal policy discourse by conducting research and analysis into the challenges faced, both domestic as well as international, which arise out of the operation of the law.

THE CONFLICT LAW CENTRE

The Conflict Law Centre was established at the Research Society of International Law, in September 2015. It is a specialized division of RSIL dedicated to the study of International Humanitarian Law (IHL) in the Pakistani context. The Centre formalizes much of RSIL's existing work in the field of IHL by dedicating a team of lawyers to undertake cutting-edge research and build capacity through various initiatives.

A primary objective of the Centre is to legally analyse law enforcement operations conducted under Article 245 of the Constitution of the Islamic Republic of Pakistan under the legal rubric of 'actions in aid of civil power'. This Constitutional space provided to Government forces raises interesting questions for the domestic application of IHL and Human Rights Law (HRL) principles to the conduct of such operations and generates a need to identify an outline of Domestic Humanitarian Law.

The current world security situation and ongoing conflicts raise unique challenges for the Government, key stakeholders, and ordinary citizens and will continue to do so for years to come. In view of this condition it was deemed necessary to provide continuity in research through the establishment of a dedicated research centre focusing on the law of conflict as understood in domestic law and under IHL. The Centre's research hopes to assist not only the legal community but also the judiciary and other stakeholders which are faced with a myriad of legal questions arising out of these operations.

SUPERVISOR
Ahmer Bilal Soofi, President RSIL and Advocate Supreme Court of Pakistan

AUTHOR
Sahar Haroon, B.A-LL.B (BUIC)
Research Associate

ACKNOWLEDGEMENTS

This article has been developed from my LL.B. dissertation titled, 'Application and Compatibility of International Humanitarian Law: The Hard Case of Cyber Warfare'. For their guidance, I would like to sincerely thank all my instructors and professors at Bahria University, most specifically Professor Ahmad Ali Khan and my dissertation supervisor Ms. Saadia Zahoor.

I am also grateful to the ICRC, Islamabad Delegation, for their continued cooperation during my dissertation. This work would not have been possible without their unwavering support.

I would also like to express my gratitude to the entire RSIL team for their constant encouragement and assistance, particularly, Mr. Ahmer Bilal Soofi who has been a continuous source of inspiration and relentless support.

EXECUTIVE SUMMARY

It is well-established that existing International Humanitarian Law (IHL) is applicable to cyberwarfare, however there are certain difficulties that need to be addressed. The initial issue is the classification of malicious cyber activity as 'attack' for the purposes of IHL, and then 'attribution' for such acts in cyberspace is also problematic. Inherently linked to the identification of the perpetrator is the challenge of categorizing the nature of the armed conflict. Moreover, once an act is recognized as an 'attack', it remains to be ascertained how the fundamental principles of IHL would be practically replicated in cyberspace. These challenges may be addressed either through classic treaty interpretation or by analogically applying existing corpus of law to cyberwarfare. To tackle the unique issues posited thereby, sometimes a new treaty regime is suggested, however the same would not receive ratifications as rapidly as the threat of cyberwarfare grows. Therefore, the only logical way to uphold and protect the intransgressible principles of humanity and dictates of public conscience is through universal consensus and evolving State practice. Though, cyberwarfare has not yet had dramatic humanitarian consequences, but our growing dependency on cyber infrastructure to sustain our daily lives increases that risk. Therefore, 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.

The State of Pakistan has been victim to cyber espionage and hacking on multiple occasions, yet lacks an effective system to defend against such acts and even less so against cyber-attacks. Therefore, it must actively seek to address the cyber threats it faces and establish a cyber defense mechanism by firstly identifying cybersecurity loopholes. Pakistan is bound by existing IHL with regards to cyberwarfare and must adhere to those rules in the establishment of such a mechanism. However, where such rules are insufficient domestic cyber laws are relevant to determine State practice and may be built upon.

ACRONYMS

AALCO	Asian-African Legal Consultative Organization
AP	Additional Protocol
APT	Advanced Persistent Threat
CIHL	Customary International Humanitarian Law
CNN	Cable News Network
DDoS	Distributed Denial of Service
DNC	Democratic National Committee
ETO	Electronic Transactions Ordinance 2002
FBI	Federal Bureau of Investigation
FO	Foreign Office
GC	Geneva Convention
IAC	International Armed Conflict
ICJ	International Court of Justice
ICRC	International Committee of Red Cross
ICTs	Information and Communications Technology
ICTY	International Criminal Tribunal for (the former) Yugoslavia
IGE	International Group of Experts
IHL	International Humanitarian Law
ISPs	Internet Service Providers
JAR	Joint Analysis Report
NATO	North Atlantic Treaty Organization
NATO CCD COE	NATO Cooperative Cyber Defense Centre of Excellence
NIAC	Non-International Armed Conflict
PEC Act	Prevention of Electronic Crimes Act 2016
PTA	Pakistan Telecommunication Authority
UN	United Nations
UNGA	United Nations General Assembly
UNIDIR	United Nations Institute for Disarmament Research
UNSC	United Nations Security Council
US	United States
WMDs	Weapons of Mass Destruction

TABLE OF CONTENTS

SECTION 1

IDENTIFYING THE PROBLEM

Cyber technology has witnessed unbridled growth in recent years becoming the primary tool to manage global infrastructure for economic, social, political and subsequently military activity. Though aiding rapid development, cyberspace has simultaneously given rise to new means and methods of warfare. It puts the security of all States at risk, raising internal and external concerns. Such threats can lead to cyberwarfare which, as generally understood, materializes when hostilities in situations of armed conflict[1] between States[2] or between organized armed groups[3] are conducted in cyberspace.[4] The ends of cyberwarfare are the same as those attributed to kinetic[5] use of force, i.e. for weakening the military might of another State, or to press one's own advantage. Moreover, like kinetic warfare, cyberwarfare is governed under the law of nations or 'Public International Law'.

Public International Law constitutes both *jus ad bellum*[6] and jus in *bello*.[7] 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.[8] On the other hand, *jus in bello*, commonly referred to as International Humanitarian Law (IHL), is that branch of law which comes into effect once an armed conflict has been initiated. It focuses on minimizing the humanitarian cost of attacks, thereby protecting those individuals and objects that do not offer any military advantage to any of the parties to the conflict.[9] Although both these branches of international law raise fundamental questions in respect to cyberwarfare, 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.

---

1. The existence of an armed conflict is the essential prerequisite for the triggering the application of IHL. This aspect is further elaborated in Section 3
2. "An international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States." Rule 22 of the Michael N. Schmitt (gen. ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press 2013) [hereinafter "the Tallinn Manual"]
3. "A non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organization" Rule 23 of the Tallinn Manual
4. "The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state." Major Arie J. Schaap, 'Cyber Warfare Operations: Development and Use Under International Law' [2009] 64 AFLR
5. Meaning e.g., dropping bombs, shooting missiles or bullets
6. Latin for "law to war"
7. Latin for "law in waging war"
8. Peter Malanczuk, Akehurst's Modern Introduction to International Law (7th edn Routledge, 1997) [306 – 345]
9. Nilz Melzer, International Humanitarian Law: A Comprehensive Introduction (ICRC Geneva 2016) [17]

Next in this section, the scope of study is outlined and then a brief background to cyberwarfare is provided. This section ends with an understanding of cyberwarfare while differentiating it from 'cybercrimes' and 'cyberterrorism'. Section 2 focuses on how IHL is applicable to this unconventional form of warfare. Section 3 highlights the legal challenges posed by cyberwarfare. Section 4 continues the examination of the issue, in light of the fundamental principles of IHL and how these principles cannot be applied ad *verbatim*[10] in the cyberspace. Section 5 constitutes the concluding remarks, summarizing the preceding arguments and recommendations.

1.1. Scope of Study

The issue central to the present work is to determine what acts in cyberspace would amount to an 'attack', thus triggering an 'armed conflict' and application of IHL. Furthermore, it is sought to understand whether the fundamental principles of distinction, proportionality and precautions in attack can be fully observed in cyberspace.

Another major concern in cyberwarfare is 'attribution'. It is vital to ascertain where the attack originated from and who initiated it, in order to determine the nature of the armed conflict. This determination is comparatively easy in case of nuclear weapons for instance, which fall in the government's domain and cannot be used anonymously nor can their point of origin be disguised. On the other hand, the internet is much more complicated. Thus, the question arises whether IHL, in its current form, becomes redundant for the governance of warfare in cyberspace.

As the corpus of IHL is made up of customary practices and treaties, another issue surfaces, as to whether existing IHL treaties are applicable analogically to modern means of warfare, or are new instruments required to fill the lacunae? This would depend on whether IHL instruments in their current form are sufficient to confine cyberwarfare or not.

Lastly, a main objective of this article is to provide an understanding of the Pakistani legal framework vis-à-vis cyberwarfare. Therefore, domestic legislation, i.e. the Prevention of Electronic Crimes Act 2016 (the PEC Act), which deals with cybercrimes is analysed in order to determine whether it can qualify as State practice under international law and consequently provide certain guidelines with regard to developing a national military strategy for understanding and dealing with the threat of cyberwarfare.

10. Latin for "corresponding word to word; using the same words"

1.2. Background

The first noted incident of malicious use of cyber technology between States is from 2007 when riots enabled through social media by provoking ethnic Russians were led in the streets of Estonia.[11] The Russian government was also allegedly[12] involved in this incitement. This social media campaign took the shape of organized cyber-attacks that originated from over 150 countries hitting Estonia's private and government systems and shutting them for ten days, along with making fire and ambulance services unavailable for over an hour.[13]

Estonia as a member of NATO[14] could claim 'collective defense' under Art. 5[15] of the NATO Treaty, but that option could not be availed because the aggressor could not be identified. Though, this issue did not fall under IHL[16] owing to the absence of an armed conflict, it nevertheless captured the world's attention with regards to threats posed by cyber technology.[17]

It was reported[18] that by 2007 between 120 to 140[19] States were engaged in developing cyber-attack technology. This number has been expected to rise greatly as well as to trigger a race among nations in the coming decades, as States seek to ascertain the potential advantages and challenges of such

11. Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016
12. Paul A. Walker, 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' [2010] Journal of National Security and Policy, Forthcoming 1 <http://ssrn.com/abstract=1586504> accessed 17 November 2015; See Also Scott J. Shackelford, 'Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks' [2009] Journal of Internet Law, Forthcoming 1 <http://ssrn.com/abstract=1499849> accessed 17 November 2015
13. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 375 <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015
14. North Atlantic Treaty Organization
15. "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area…"
16. Rather it could be categorized under jus ad bellum. i.e., whether there was use of force against Estonia and whether it triggered her right of self-defense.
17. Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016
18. McAfee Virtual Criminology Report, 'Cybercrime: The Next Wave' (2007) 13 <http://www.mcafee.com/us/research/criminology_report/default.html> accessed 15 March 2016
19. Susan W. Brenner and Leo L. Clarke, 'Civilians in Cyberwarfare: Conscripts' [2010] 43 Vanderbilt Journal of Transitional Law 2 <http://ssrn.com/abstract=1650743> accessed 30 December 2016

assaults.[20] The hostile events[21] of 2008, between Russia and Georgia focused global attention on the emerging, inevitable[22] and real threat of cyberwarfare.[23]

The Assistant Director of the United States' (US) Federal Bureau of Investigation (FBI) cyber division observed that cyber-attacks posed as big a threat as weapons of mass destruction (WMDs).[24] NATO's Cyber Defense Chief similarly asserted that *"cyberterrorism [and] cyber-attacks pose as great a threat to national security as a missile attack."*[25] Moreover, as noted by a study on cybercrime laws, *"in the networked world, no island is an island",*[26] therefore cyberspace must be protected.[27]

In order to contain the threat posed by cyber operations, an initial discourse on whether such activity is governed by existing legal frameworks or not is of prime importance. In this regard, it may be noted that even though 'cyber operations' qualify as new technologies, such qualification does not suggest that there are no restrictions on their use in an armed conflict. Cyber technology is covered within the ambit of Art. 36 of Additional Protocol I, 1977 (AP I).[28] Art. 36 is applicable to all 'new weapons' as envisaged by the

20. McAfee Virtual Criminology Report, 'Cybercrime: The Next Wave' (2007) 13 <http://www.mcafee.com/us/research/criminology_report/default.html> accessed 15 March 2016
21. "When Georgia attacked South Ossetia and tried to take this territory back, issues of compliance with IHL during cyber operations were raised. During this period, Russian peacekeepers were already stationed in South Ossetia and eventually an IAC broke out between Russia and Georgia. Simultaneously with the launch of military operations, a list of targets and malware was uploaded on a Russian website. This website gave easy and quick access to anyone who was interested in attacking any of the Georgian official websites – listed there – by just downloading the malware and attacking that particular Internet Protocol (IP). These attacks led to six hours of DDoS, and targeted government websites like the Ministry of Defense, banks and Internet Service Providers (ISPs)." See generally Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016; See also Commentary to Rule 2 of the Tallinn Manual [28] [68]
22. -- , 'US Homeland Chief: Cyber 9/11 could happen "Imminently" ' Reuters (24 January 2013) <http://www.reuters.com/article/us-usa-cyber-threat-idUSBRE90N1A320130124> accessed 14 November 2016
23. See Introduction to the Tallinn Manual [16] – [17]
24. Special, 'Cyber Attacks Ranked 3rd Danger Behind Nuclear War' ARY Oneworld (8 January 2009) <http://www.thearynews.com/english/newsdetail.asp?nid=19868> accessed 13 March 2016
25. Kevin Coleman, 'Cyber Weapons and E-Bombs' (March 2008) DefenseTech Organization <http://www.defensetech.org/archives/cat_cyberwarfare.html> accessed 15 March 2016
26. McConnell International Report, "Cyber Crime … and Punishment: Archaic Laws Threaten Global Information," (December, 2000) <http://www.witsa.org/papers/McConnell-cybercrime.pdf> accessed 19 November 2015
27. William J. Lynn III, Remarks at the USAF–TUFTS Institute for Foreign Policy Analysis Conference, Deputy Secretary of Defense (21 January 2010) <http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1410> accessed 20 November 2015
28. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978)

provision, regardless of whether such technology existed at the time of its drafting; however, the military potential of cyberspace is yet to be completely understood.[29]

In Pakistan, there is a fundamental lack of the urgency to develop cyber capabilities and strategies,[30] and a general unawareness of its peculiarities.[31] In the absence of these, Pakistan remains vulnerable to cyber targeting of all kinds: hacking, espionage, malware uploads etc. or outright cyber-attacks.[32] The Foreign Office (FO) of Pakistan experienced three major cyber operations against its information infrastructure between January 2015 and May 2016.[33] These incidents highlighted a serious security vacuum in the country and the inability of State functionaries to protect critical data[34] and/or infrastructure.[35]

While previously domestic legislation[36] existed to curtail cybercrimes, its ineffectiveness and/or limited scope led to the adoption of the PEC Act. The PEC Act, though a step in the right direction,[37] is insufficient to deal with the complex nature of cyberspace and the multitude of challenges posited thereby. This is primarily because the wording of the PEC Act is too generic,[38] thus making implementation quite problematic along with giving broad

29. See Section 2.1. below
30. For instance US President Obama issued an 'executive order' in April 2015 empowering the highest office bearer to impose economic sanctions against countries that targeted US critical infrastructure, see The White House, Office of the Press Secretary, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities' (Executive Order) (1 April 2015) <https://assets.documentcloud.org/documents/1699240/executive-order-obama-establishes-sanctions.pdf> accessed 17 November 2016; 'Critical Infrastructure' has been comprehensively defined in Presidential Policy Directive 21, see The White House, Office of the Press Secretary, 'Presidential Policy Directive – Critical Infrastructure Security and Resilience' (Presidential Policy Directive/PPD-21) (12 February 2013) <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> accessed 17 November 2016
31. Kunwar Khuldane Shahid, 'An Analysis of Pakistan's Cyber Security Dilemma' [2016] MIT Technology Review Pakistan <http://www.technologyreview.pk/cyber-security-work-in-progress/> accessed 19 November 2016
32. FireEye, 'APT: A Window into Russia's Cyber Espionage Operations?' (Special Report) (27 October 2014) [17] <http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf> accessed 16 November 2016
33. Staff Reporter, 'FO to Seek ISI Help for Protecting itself from Hackers' Dawn News (Islamabad, 6 May 2016) <http://www.dawn.com/news/1256603> accessed 18 November 2016
34. Prevention of Electronic Crimes Act 2016 s 2 (x) and (xi) [hereinafter referred to as 'the PEC Act']
35. Khawar Ghumman, 'Cyber Attacks against Govt Expose Fatal Cracks in Pakistan's Digital Fence' Dawn News (Islamabad, 19 May 2015) <http://www.dawn.com/news/1182856> accessed 18 November 2016
36. Electronic Transaction Ordinance, 2002, having limited scope in respect of growing use of cyberspace vis-à-vis electronic commerce; and the since repealed Prevention of Electronic Crimes Ordinance, 2007
37. Dr Nadia Khadam, 'Seriousness towards Cyber Crime Laws in Pakistan' The News (Islamabad, 19 August 2016) <https://www.thenews.com.pk/print/143651-Seriousness-towards-cyber-crime-laws-in-Pakistan> accessed 21 November 2016
38. Shahama Tul Amber, 'Critics Highlight Issues in Cyber Crimes Bill Passed by NA' Daily Times (Islamabad, 12 August 2016) <http://dailytimes.com.pk/pakistan/12-Aug-16/critics-highlight-issues-in-cyber-crime-bill-passed-by-na> accessed 21 November 2016

powers to the enforcement agencies.[39] Furthermore, it fails to make a distinction between 'cybercrime', 'cyberterrorism' and 'cyberwarfare',[40] thereby adding to the confusion. Nevertheless, it must be borne in mind, that although the PEC Act does not directly deal with cyberwarfare, it can be understood as providing a basic framework[41] which would amount to State practice[42] under customary international humanitarian law (CIHL).[43]

1.3. Cyber Operations: Definitions and Classification

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; owing primarily to the common domain through which these are conducted, i.e., cyberspace.[44] 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.

1.3.1. Cybercrimes

'Cybercrime' is a crime committed in the cyber domain,[45] i.e. over the internet. While "*commission of cybercrime was not imaginable three decades ago*",[46] in today's world, crimes such as theft, fraud, harassment, and extortion are easily comprehensible and committed in such ways.[47] Such activity is so common nowadays that every three seconds someone's identity is stolen over the internet, while 594 million people worldwide were victims of online crime[48] in

39. Haroon Baloch, 'Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016' (2016) APC Issue Paper 1 – 10 <http://www.netfreedom.pk/wp-content/uploads/2016/06/CSO-criticism-on-PECB-2016_IssuePaper.pdf> accessed 21 November 2016
40. Raza Khan, 'Cyber Crime Bill Passed by NA: 13 Reasons Pakistanis should be Worried' Dawn (Islamabad, 11 August 2016) <http://www.dawn.com/news/1276662> accessed 21 November 2016; see also Sections 1.2.2. and 1.2.3. hereinbelow
41. See Sections 3 and 4 hereinbelow
42. See, for example, Rule 1 of ICRC CIHL Study, "The Principle of Distinction between Combatants and Civilians" <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_cou_pk_rule1> accessed 21 November 2016, wherein the Army Act, 1952 is taken as reflective of State practice on the matter.
43. Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law Volume I: Rules (CUP 2005) xxxviii - xlv
44. "The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks." See the Tallinn Manual
45. "A crime involving the use of a computer, such as, sabotaging or stealing electronically stored data" in Bryan A. Garner, Black's Law Dictionary (9th edn, West Publications 2009) 443
46. Mst. Marium Haji v Mrs. Yasmin R. Minhas, PLD 2003 Kar 148 [155] [Para 11]
47. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [382] – [386] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
48. Norton by Symantec, 'What is Cybercrime?' <http://us.norton.com/cybercrime-definition> accessed 26 March 2016

2015.[49] In this sense, cybercrimes can be categorized as the commission of age-old crimes in a novel way.[50]

However, there are also those emerging crimes that are only committed through cyber means and have increased with the evolution of such infrastructure. An example of such crimes is a distributed denial of service (DDoS) attack which *"makes a computer resource [such as a website] unavailable to its intended users."*[51] DDoS attacks were seen in force in February 2000;[52] when major web portals like CNN,[53] Yahoo!, and eBay were targeted by a 15-year old Canadian hacker, and resulted in their complete shutdown.[54] More recently, popular websites such as Twitter and Netflix were brought down through such attacks.[55] Some of these crimes are covered by the PEC Act, for example 'spamming' that is defined as occurring when harmful, fraudulent, misleading, illegal or unsolicited information is transmitted to any person without his prior consent.[56]

Therefore, whether new crimes or traditional ones committed in a modern way, the distinguishing feature of cybercrime is that it threatens the internal order of a State, independent of where it originates in the world.[57] The difficulty in the enforcement of most definitions of cybercrime has been that they do not address those activities which though threaten internal order, were not previously conceived and thus require new legislation.[58] In the Pakistani context, it may be observed that the PEC Act addresses this problem,

---

49. Norton Anti-Virus, developed and distributed by Symantec Corporation
50. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [383] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
51. Ibid [385]
52. Brian Ries, 'Hackers' Most Destructive Attacks' The Daily Beast (12 December 2010) <http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html> accessed 4 April 2016
53. Doug Gross, ''Mafiaboy' Breaks Silence, Paints 'Portrait of a Hacker'' CNN (New York 15 August 2011) <http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/> accessed 4 April 2016
54. -- 'A Q & A with MafiaBoy' Infosecurity Magazine (3 September 2013) <http://www.infosecurity-magazine.com/news/a-qa-with-mafiaboy/> accessed 4 April 2016
55. Jeff Parsons and Gemma Mullin, 'Twitter, Spotify and Netflix among dozens of popular websites brought down by 'hackers' in major DDoS attack' Mirror (United Kingdom 21 October 2016) <http://www.mirror.co.uk/news/world-news/breaking-twitter-spotify-airbnb-others-9096519?service=responsive> accessed 20 November 2016
56. The PEC Act s 23
57. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [386] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
58. Tom Espiner, 'UK Outlaws Denial-of-Service Attacks' CNET News (10 November 2006) <http://news.com.com/2100-7348_3-6134472.html> accessed 13 March 2016

giving a detailed list[59] of cybercrimes as well as providing for means of enforcement.[60] However, as mentioned hereinbefore, it has been criticised for being broadly and vaguely worded, leaving room for abuse of power.[61]

1.3.2. Cyberterrorism

UN Security Council Resolution 1566 calls upon all States to prevent the following acts and further provides that these shall not be justified on political, philosophical, ideological, racial, ethnic or religious considerations:

> "…Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act..."[62]

The purpose of terrorism 'to provoke a state of terror in the general public' is also reflected in the definition of cyberterrorism under the PEC Act. It is defined as any person interfering with[63] or without authority copying or transmitting[64] critical infrastructure data[65] with the intent to create a sense of fear, panic in the Government or the public or to advance sectarianism.[66] However, the PEC Act by classifying cyberterrorism as a cybercrime fails to appreciate the distinction between them.[67] Nevertheless, it may be deemed to be a positive development as this definition also criminalizes interference with data for the advancement of objectives of terrorist networks.[68] This is crucial as cyberterrorists till date have used cyberspace to garner support, recruit or spread propaganda.

Like cybercrime, cyberterrorism also consists of using computer technology[69]

---

59. The PEC Act chapter II s 3 – 28
60. The PEC Act chapter III s 29 – 41
61. Shahama Tul Amber, 'Critics Highlight Issues in Cyber Crimes Bill Passed by NA' Daily Times (Islamabad 12 August 2016) <http://dailytimes.com.pk/pakistan/12-Aug-16/critics-highlight-issues-in- cyber-crime-bill-passed-by-na> accessed 21 November 2016
62. UNSC Resolution 1566(2004) (8 October 2004) UN Doc S/RES/1566(2004)
63. The PEC Act s 8
64. The PEC Act s 7
65. The PEC Act s 2 (xi)
66. The PEC Act s 10
67. The PEC Act chapter II dealing with 'Offences and Punishments'
68. The PEC Act s 10(c)
69. Clay Wilson, CRS Report for Congress, 'Computer Attack and Terrorism: Vulnerabilities and Policy Issues for Congress' (1 April 2005) <http://www.iwar.org.uk/cyberterror/resources/crs/45184.pdf> accessed 12 January 2016

for committing acts in unconventional ways, in this case for spreading terror among the citizens. Another similarity between the two is that both serve to undermine internal order. However, these are two distinct acts in their objective as well as result and are thus treated differently.[70]

Where cybercrimes are based on acquiring personal, wrongful gain by causing physical or psychological injury to another individual;[71] cyberterrorism is geared more towards political goals as part of its agenda.[72] Cyberterrorists, 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[73] by targeting civilians.[74] This may be differentiated from cyberwarfare which theoretically does not allow[75] civilians to be made the object of attack.

1.3.3. Cyberwarfare

The phrase 'information war' as defined[76] by the Shanghai Cooperation Organization,[77] may only be applied to those 'cyber-conflicts' and 'cyber

70. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [386] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
71. Ibid [387]
72. S. Ventkatesh, Cyber Terrorism (Authors Press, Delhi 2003) 24
73. Pippa Norris, Montague Kern and Marion Just (eds.), Framing Terrorism: The News Media, the Government, and the Public (Routledge 2003) 255
74. Reuven Young, 'Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation' [12 January 2006] 29(1) Boston College International and Comparative Law Review 86 <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1054&context=iclr> accessed 18 December 2015 "…Acts done to advance an ideological, political, or religious cause and to induce terror in any population or to compel a government or international organization to act in a certain way are terrorism if they cause one of the following outcomes: death or serious injury; serious risk to public health or safety; destruction or serious damage to property of great value or importance; major economic loss or major environmental damage if it threatens injury, death, endangers life or the public health and safety; serious interference with infrastructural facilities likely to endanger life; and releasing disease-bearing organisms likely to devastate the national economy."
75. Preamble to the Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight (adopted 11 December 1868, entered into force 11 December 1868) International Military Commission, St. Petersburg [hereinafter referred as "St. Petersburg Declaration, 1868"]; Arts. 48, 50, 51 of AP I; Art. 13 of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) [hereinafter "AP II"]
76. Defined as, "confrontation between two or more States in the information space aimed at damaging information systems, processes and resources, and undermining political, economic and social systems, mass brainwashing to destabilize society and State, as well as forcing the State to take decisions in the interest of an opposing party."
77. Annexure to the Agreement between the Government of the Member States of the Shanghai Cooperation in the Field of International Information Security (16 June 2009) Shanghai Cooperation Organization (SCO) [based on an unofficial translation]; Pakistan has been an Observer at SCO since 2005 and acquired full member status in June 2016

hostilities' where they would qualify as an armed conflict within the meaning of IHL. The International Committee of the Red Cross (ICRC) understands 'cyberwarfare' 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 International Humanitarian Law."[78] Moreover, a cyber-attack is a concern for 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."[79] Furthermore, where kinetic or physical attacks are launched against belligerent cyber facilities it would not amount to a cyber-attack,[80] but physical damage or destruction may be caused from a cyber operation.[81]

Cyberwarfare, just like kinetic warfare, can be of different natures. However, where parties to the armed conflict, whether during an international (IAC),[82] non-international (NIAC)[83] or transboundary hostilities,[84] remain easily identifiable in the physical world, cyberspace changes all that. In modern times, any number of individuals regardless of physical location or affiliation

78. ICRC, 'What Limits Does the Law of War Impose on Cyber Attacks?' (June 2013) <https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> accessed 15 November 2015
79. Rule 30 of the Tallinn Manual
80. Marco Roscini, 'World Wide Warfare: Jus ad bellum and the Use of Cyber Force' (2010) 14 Max Planck Ybk of UN Law 96
81. Nils Melzer, 'Cyber-warfare and International Law' [2011] United Nations Institute for Disarmament Research Resources [4] – [6] <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 18 November 2015
82. Art. 2 Common to Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 35 [hereinafter "GC I"]; Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 81 [hereinafter "GC II"]; Geneva Convention (III) relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 [hereinafter "GC III"]; and Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 [hereinafter "GC IV"]; See also Art. 1 of Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) International Peace Conference, The Hague; See also AP I art 43
83. GC I, II, III, IV common art 3; See also AP II art 1(1); The Prosecutor v Dusko Tadic (Judgment) ICTY-1997-IT-94-I-T [7 May 1997] [Para 561] – [568]
84. 32nd International Conference of the Red Cross and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (December 2015) Doc. 32IC/15/11 [18] – [19] <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016; See also 31st International Conference of the Red Cross and Red Crescent Report, 'International Humanitarian Law and Challenges of Contemporary Armed Conflicts' (December 2011) Doc. 31IC/11/5.1.2 [11] – [12] <https://app.icrc.org/e-briefing/new-tech-modern-battlefield/media/documents/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf> accessed 10 December 2015

may easily engage in activity that would qualify as cyberwarfare.[85] 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.[86]

The PEC Act, incorrectly, blurs the distinction between cyberwarfare and cybercrime by criminalizing unauthorized access,[87] copying, transmission[88] or interference[89] with critical infrastructure. Under this Act, critical infrastructure means.

Critical elements of infrastructucre namely assets, facilities, systems, networks or processes the loss or compromise of which could result in: …

(b) significant impact on national security, national defense, or the functioning of the state …[90]

It may be pointed out that interference or unauthorized access with such infrastructure impacting national security does not result in merely cybercrime, rather can be deemed to constitute 'use of force'[91] under the Charter of the United Nations (UN Charter)[92] raising cybersecurity[93] issues.

Cyberwarfare is one of the contemporary technologies which raises problems of compliance with IHL. Hereinafter, the application and compatibility of IHL to cyberwarfare is deliberated upon, with simultaneous analysis of the subject at hand in the context of Pakistan.

85. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [409] – [440] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
86. See Section 3. 3.; See also Rules 6, 7, and 8 of the Tallinn Manual
87. The PEC Act s 6
88. The PEC Act s 7
89. The PEC Act s 8
90. The PEC Act s 2 (1) (x)
91. UN Charter art 2(4)
92. Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) United Nations Conference on International Organization, San Francisco
93. "Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries." Andrew Walls, Earl Perkins and Juergen Weiss, 'Definition: Cybersecurity' (2013) Gartner ID G00252816 <https://www.gartner.com/doc/2510116/definition-cybersecurity> accessed 7 January 2017

SECTION 2

APPLICABILITY OF IHL TO CYBERWARFARE

As observed from the examples of Estonia[94] and Georgia',[95] cyberwarfare 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 applies in cyberspace just as it does in kinetic operations.[96] Similarly, the only justification to engage in such activity would be founded on either Art. 42 or Art. 51 of the Charter.[97] Furthermore, once hostilities are engaged into, IHL becomes applicable.[98] This latter category comprises of numerous Conventions[99] and their Protocols,[100] as well as CIHL[101] derived from State practice and opinio juris.[102]

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.[103] Nevertheless, the Red Cross and Red

94. See Section 1.1.
95. Ibid
96. See Commentary to Rule 6 of the Tallinn Manual [Para 3]
97. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal [393] – [395] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015
98. See Advance Questions for Lt. Gen. Keith Alexander, USA Nominee for Commander, US Cyber Command Before the S. Armed Service Command (2010) <http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf> accessed 15 March 2016; See also Duncan B. Hollis, 'Why States Need an International Law for Information Operation' [2007] 11 LCLR 1048
99. For example, Hague Law; Geneva Law; Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137; Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention (adopted May 14 1954) 249 UNTS 240
100. For example, Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict (adopted 25 May 2000, entered into force 12 February 2002) 2173 UNTS 222; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict (adopted 26 March 1999, entered into force 9 March 2004) 2253 UNTS 212
101. Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law (ICRC and CUP 2005) <https://www.icrc.org/customary-ihl/eng/docs/home> accessed 14 October 2015 [hereinafter "ICRC CIHL Study"]
102. "This is the psychological factor, the belief by a state that behaved in a certain way that it was under a legal obligation to act that way. It is known in legal terminology as opinio juris sive necessitatis and was first formulated by the French writer Francois Geny as an attempt to differentiate legal custom from mere social usage." Malcolm N. Shaw, International Law (6th edn., CUP 2008) 75
103. See Sections 3 and 4

Crescent Movement (the Movement)[104] opines[105] that even though new technologies[106] pose difficulties for IHL they are governed thereunder.

2.1. Rationale for the Applicability of Existing IHL

As an initial point of deliberation, it may be examined whether IHL in its present form is applicable to cyber operations[107] in an armed conflict or not. Those who question its applicability firstly argue that there is no provision in IHL that directly deals with cyber operations. Additionally, that international instruments constituting IHL were concluded at a time when cyber operations were not even comprehended, hence were not within the intention of the member States. Lastly, that it deals with those means and methods of warfare which are not cyber but kinetic in nature.[108]

The first two criticisms are disqualified with reference to Martens Clause[109] and the Advisory Opinion[110] of the International Court of Justice (ICJ) in the Nuclear Weapons case.[111] The Martens Clause which was first enshrined in the preamble to the Hague Convention, 1899,[112] is later found incorporated within the Geneva Conventions of 1949,[113] as well as the Additional Protocols

104. It is important to note that the 4-yearly International Conference of the Movement is not restricted to members of its delegations around the world, but States party to the Geneva Conventions of 1949 also attend this Conference and are active members of the deliberations and dialogue, see Standing Commission of the Red Cross and Red Crescent Movement, 'About the International Conference' <http://standcom.ch/about-the-international-conference/> accessed 4 December 2016
105. 31st International Conference of the Red Cross and Red Crescent Report, 'International Humanitarian Law and Challenges of Contemporary Armed Conflicts' (December 2011) Doc. 31IC/11/5.1.2 [36] - [37] <https://app.icrc.org/e-briefing/new-tech-modern-battlefield/media/documents/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf> accessed 10 December 2015
106. These technologies include:
    1. the cyberspace that potentially opens a new domain for military operations;
    2. remote-controlled weapons systems – such as drones which are used by the parties to armed conflicts in greater extent; and
    3. automated weapons systems – such as combat robots.
107. Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' [2002] 84(846) IRRC 368
108. Emily Haslam, 'Information Warfare: Technological Changes and International Law'[2000] 5 JCSL 157; Richard Aldrich, 'The International Legal Implications of Information Warfare' [1996] AJ 99; and Mark Shulman, 'Discrimination in the Laws of Information Warfare' [1999] 37 CJTL 939
109. Named so after its' author: Fyodor Fyodorovich Martens (F. F. de Martens), an eminent Russian jurist and diplomat, international arbitrator, and historian of European colonial ventures in Asia and Africa
110. Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226 (hereinafter the 'Nuclear Weapons case')
111. Theodor Meron, 'The Martens Clause, Principles of Humanity, and Dictates of Public Conscience' [2000] 94(1) AJIL [78] – [89]
112. Hague Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations concerning the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900) International Peace Conference, The Hague [hereinafter "Hague Convention (II)"]
113. GC I art 63; GC II art 62; GC III art 142; GC IV art 158

of 1977,[114] and the Convention Prohibiting Certain Conventional Weapons, 1980.[115] It lays down that:

> 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 public conscience.[116]

According to the ICRC commentary to AP I, the Martens Clause is dynamic in nature by "proclaiming the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology."[117] Similarly, Shahabudeen J. in the ICJ Advisory Opinion observed[118] that this clause should be interpreted as reflective of new concepts.

The opinion that a technology is not specifically addressed in the existing body of law does not conclude that it would remain – or in any way could operate – without restrictions. In relation to cyberspace, since most of IHL is designed to be an adaptive body of law – it is, thus, designed to include new weapons.[119] 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

114. AP I art 1(2); AP II preamble para 4
115. Preamble Para 5 to Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137
116. Preamble to Hague Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 29 July 1899, entered into force 4 September 1900) International Peace Conference, The Hague [hereinafter "Hague Convention (II)"]
117. Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (eds.), ICRC Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (ICRC Geneva 1987) [hereinafter "ICRC AP Commentary"] [Para 39]
118. "In effect, the Martens Clause provided authority for treating the principles of humanity and the dictates of public conscience as principles of international law, leaving the precise content of the standard implied by these principles of international law to be ascertained in the light of changing conditions, inclusive of changes in the means and methods of warfare and the outlook and tolerance levels of international community. The principles would remain constant, but their practical effect would vary from time to time: they could justify a method of warfare in one age and prohibit it in another." Nuclear Weapons case [Para 406] (Shahabuddeen J. dissenting)
119. Interview with Lloyd Gillett, Regional Delegate to the Armed and Security Forces, ICRC (Islamabad 19 November 2015)

> 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",[120] 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.[121] 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.[122] This logic may also be derived from the ban on biological[123] and chemical weapons;[124] which though not physical means of attacks, fall within the ambit of IHL.[125]

2.2. Tallinn Manual on the International Law Applicable to Cyberwarfare

The Tallinn Manual126, a NATO CCD COE[127] project, led by Professor Michael N. Schmitt[128] is an attempt to define the rules of war applicable to cyberwarfare, as they existed in June 2012.[129] It is pertinent to note here, that the International Group of Experts (IGE)[130] endeavoured to compile these

120. See Section 3.1. hereinbelow
121. AP I art 49
122. Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' [2002] 84(846) IRRC 373 [374]
123. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (adoption 16 December 1971, entered into force 26 March 1975) 1015 UNTS
124. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997) UN Doc. CD/CW/WP.400/Rev. 1
125. Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' [2002] 84(846) IRRC 374
126. In 2009, an independent IGE was invited by NATO to produce the Tallinn Manual, which was then published by the Cambridge University Press in 2013
127. The NATO Cooperative Cyber Defense Centre of Excellence, an international military organization based in Tallinn, Estonia.
128. Michael N. Schmitt is Charles H. Stockton Professor and Director of the Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law at Exeter University; and Senior Fellow at the NATO CCD COE
129. The date of the meeting at which the IGE adopted the final draft
130. The IGE consisted of 16 renowned international law practitioners who had or were then serving as senior legal advisers for their governments. A panel of 4 technical advisers assisted and observed the experts from NATO, the US Cyber Command and the ICRC. The work thus compiled was subsequently peer reviewed by 13 internat0ional law specialists; For example, Professor Michael Schmitt [US Naval War College]; Air Commodore (Retired) William H Boothby [Formerly Deputy Director of Legal Services, Royal Air Force (United Kingdom)]; Bruno Demeyere [Catholic University of Leuven]; Professor Wolff Heintschel von Heinegg [Europa-Universität Viadrina] among others

rules reflective of de *lege lata*[131] at that time, as opposed to de *lege ferenda*.[132]

The Tallinn Manual, consisting of ninety-five rules, is a non-binding text in that it does not comprise an official document. However, it still carries importance as it is a pioneer document in this field, wherein all the sixteen members of the IGE unanimously[133] agreed that the existing body of IHL is rather robust and can be applied to cyberwarfare in a way that is very logical and meaningful.[134] It also carries persuasive value, as it consolidates State practice as it existed with regards to cyberwarfare in June 2012. Just as the CIHL database[135] compiled by the ICRC (ICRC CIHL Study) though not a binding text, is accepted by States, the same could be concluded for the Tallinn Manual.[136]

Each of the ninety-five rules of the Tallinn Manual, addressing both IAC and NIAC, are accompanied by a comprehensive commentary,[137] detailing the position and acceptance of each rule by the IGE, and the debate preceding their acceptance. Thus, clarifying their position in minute detail, as to which view was accepted by the majority and the minority position, if any, and what ultimately led to unanimous agreement.[138]

There has been some criticism on the way the Tallinn Manual was compiled as it lacks global representation, however it does have validity as it is the first tangible source on cyberwarfare.[139] The following sections deal with the

131. "The principle that a Court should decide based on actual law and not how it thinks the law ought to be." Bryan A. Garner, Black's Law Dictionary (9th edn, West Publications 2009) 491
132. "A proposed principle that might be applied to a given situation instead or in absence of a legal principle that is in force." Bryan A. Garner, Black's Law Dictionary (9th edn, West Publications 2009) 491
133. See Rule 20 of the Tallinn Manual, "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."; See also Commentary to Rule 20 of the Tallinn Manual [Para 1]; Rules 22 and 23 of the Tallinn Manual
134. Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016
135. Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law (ICRC and CUP 2005) <https://www.icrc.org/customary-ihl/eng/docs/home> accessed 14 October 2015
136. Michael N. Schmitt and Sean Watts, 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare' [2015] 50(2) Texas International Law Journal 189 <http://www.tilj.org/content/journal/50/14%20SCHMITT%20&%20WATTS%20PUB%20PROOF.pdf> accessed 10 April 2016
137. See for example Commentary to Rule 30 of the Tallinn Manual [91] – [95]
138. See Introduction: The Commentary to the Tallinn Manual [19]; See also Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016
139. AALCO Secretariat, 'International Law in Cyberspace (Deliberated)' (2016) [9]-[11] <http://www.aalco.int/Cyberspace%202016.pdf> accessed 23 January 2017; see also AALCO Res (20 May 2016) AALCO/RES/55/S17 New Delhi

compatibility of IHL with cyberwarfare and the legal challenges consequently posed. For that discussion, the Tallinn Manual, in light of existing IHL, is extensively referred to as it provides a modern and comprehensive analysis of the issue at hand. Furthermore, as mentioned above, it is reflective of what law is on these points. Therefore, it serves as a reliable source for understanding the accepted principles of IHL in the context of cyberwarfare.

2.3. Pakistan Cyber Laws and the IHL Paradigm

Studying and analysing cyberwarfare in the context of Pakistan poses a greater conundrum as compared to other countries. While some explicit legislation[140] and State practice[141] 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, (ETO) which is still in force, primarily deals with cyber activity. The ETO remains limited in scope as it concerns issues related to economic commerce.[142] The emergence of novel cybercrimes emphasised the need for a more comprehensive framework leading to the adoption of the PEC Act. However, it is mostly silent on cyberwarfare, and provides only a rudimentary framework even for the issues it does address, leaving a lot to be resolved.

---

140. See, for example, U.S. Department of Defense, Office of General Counsel, 'Law of War Manual', 2015 <http://www.dod.mil/dodgc/images/law_war_manual15.pdf> accessed 14 November 2016; See also Eric A. Fischer, 'Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions', Congressional Research Service, 2013 <https://fas.org/sp/crs/natsec/R42114.pdf> accessed 14 November 2016; See also Piret Pernik, Jesse Wojtkowiak and Alexander Verschoor-Kirss, National Cyber Security Organization: United States (NATO CCD COE, Tallinn, Report 2016) <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf> accessed 14 November 2016; See also Mikk Raud, China and Cyber: Attitudes, Strategies, Organization (NATO CCD COE, Tallinn, Report 2016) <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf> accessed 14 November 2016
141. "Information Operations now form the essential part of all military planning and training. A 2011 survey commissioned by the UN Institute for Disarmament Research (UNIDIR) found that 33 States including China, Russia and the US, have included cyber warfare in their military planning and organization. At least 12 countries including India have either established or are in the process of establishing military cyber warfare organizations." Dr Tughral Yamin, Cyberspace CBMs Between Pakistan and India (NUST Publishing, Islamabad 2014) [4]; James A. Lewis and Katrina Timlin, 'Cybersecurity and Cyber Warfare: Preliminary Assessment of National Doctrine and Organization' (2011) (UNIDIR Report) <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf> accessed 29 November 2016; See also Abhishek Bhalla, 'India gets Set for Unified Cyber Cell' Daily News & Analysis, New Delhi (3 December 2016) <http://www.dnaindia.com/india/report-india-gets-set-for-unified-cyber-cell-2279175?utm_content=buffer20bdb&utm_medium=social&utm_source=t witter.com&utm_campaign=buffer> accessed 5 December 2016
142. Dr Nadia Khadam, 'Seriousness towards Cyber Crime Laws in Pakistan' The News (Islamabad 19 August 2016) <https://www.thenews.com.pk/print/143651-Seriousness-towards-cyber-crime-laws-in-Pakistan> accessed 21 November 2016

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[143] to the Additional Protocols of 1977, it must adhere to existing IHL as this responsibility arises from Art. 1 of the Hague Convention, 1907[144] and Common Art. 1 of Geneva Conventions, 1949 to which Pakistan is party.[145] Moreover, these provisions, like most of IHL are derived from customs, and have attained the status of customary IHL themselves[146] – most prominent amongst which is the Martens Clause[147] – therefore their importance and applicability to the State of Pakistan cannot be denied.

Furthermore, the ICRC CIHL Study makes it evident that 'domestic legislation' falls among constituent elements of verbal acts[148] 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.

---

143. Pakistan is however a signatory to the Additional Protocols of 1977 since 12 December 1977, see ICRC, Treaties, States Parties and Commentaries: Geneva Conventions of 1949 and Additional Protocols, and their Commentaries' (ICRC) <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp> accessed 12 October 2015; The United Nations General Assembly (UNGA) adopted a Resolution in December 2016 calling for the universal adoption of the Additional Protocols. It is interesting to note that this UNGA Resolution was adopted upon the Report of the Sixth Committee (A/71/512) during the 71st Session of UNGA 2016, at which time a Pakistani (Dr. Bilal Ahmad) served as the Vice-Chairperson on the Bureau of the Sixth Committee, see UNGA Res 71/144 (20 December 2016) UN Doc A/RES/71/144, see also General Assembly of the United Nations, Legal – Sixth Committee, 'Seventy-First Session: Bureau' (UN) <http://www.un.org/en/ga/sixth/71/bureau.shtml> accessed 30 December 2016
144. Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) International Peace Conference, The Hague [Hereinafter 'Hague Convention IV']
145. GC I, II, III, and IV ratified by Pakistan on 12 June 1951, see ICRC, Treaties, States Parties and Commentaries: Geneva Conventions of 1949 and Additional Protocols, and their Commentaries' (ICRC) <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp> accessed 12 October 2015
146. Nuclear Weapons case [Para 74] – [87]; See also Michael N. Schmitt and Sean Watts, 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare' [2015] 50(2) Texas International Law Journal 189 <http://www.tilj.org/content/journal/50/14%20SCHMITT%20&%20WATTS%20PUB%20PROOF.pdf> accessed 10 April 2016
147. See Section 2.1.
148. "… Both physical and verbal acts of States constitute practice that contributes to the creation of customary international law. Physical acts include, for example, battlefield behavior, the use of certain weapons and the treatment provided to different categories of persons. Verbal acts include military manuals, national legislation, national case-law, instructions to armed and security forces, military communiques during war, diplomatic protests, opinions of official legal advisers, comments by governments on draft treaties, executive decisions and regulations, pleadings before international tribunals, statements in international organizations and at international conferences and government positions taken with respect to resolutions of international organizations." Jean-Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law Volume I: Rules (CUP 2005) [xxxviii] – [xlv]

SECTION 3

LEGAL CHALLENGES TO THE APPLICATION OF IHL IN THE CYBERSPACE

As alluded hereinbefore, cyber-attacks raise several fundamental legal challenges to the application of IHL. First among these is the qualification of a violent act as an 'attack' and then identification and attribution of that attack to the aggressor. This is inherently linked to the complexity of determining the nature of an armed conflict which would thus trigger the application of IHL. Each of these challenges are analysed in this section in light of the applicable law.

3.1. Cyber Operations as 'Attacks'

Though, cyberwarfare poses certain challenges for compatibility with IHL, the first and foremost issue is to categorize how cyber operations would amount to an 'attack'. Previously, the two approaches to the triggering of an armed conflict have been 'permissive'[149] and 'restrictive'.[150] The former focuses on actual physical destruction and damage caused as the result of a cyber operation, thus impliedly allowing such operations which do not result in physical destruction. The latter focuses on the military advantage that is gained consequently, therefore, restricting cyber operations as a matter of law.

The Tallinn Manual gives another approach to understand 'attacks', that of 'functionality'. Rule 30[151] incorporating this approach provides a definition of

149. HL is consequence-based; in that it prohibits those attacks which denote physical force, and result in damage, loss or injury to their targets. Therefore, when applied in the cyber context, would it imply that cyber-attacks not resulting in death or injury to civilians, or destruction or damage of objects, are not prohibited? This implication leads to the conundrum posed by the term 'attacks' when applied to cyber operations. See Michael N. Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' [2002] 84(846) IRRC [365]; See also ICRC AP Commentary [Para 1880]
150. Knut Dörmann, 'Applicability of the Additional Protocol to Computer Network Attack' in Karin Bystrom (ed.), Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law (Stockholm, 17–19 November 2011) 139 Swedish National Defense College 2005 <www.icrc.org/eng/resources/documents/misc/68lg92.htm> accessed 18 November 2015; Art. 48 of AP I calls for distinction between military and civilian objects and only for 'operations' to be directed against military objectives. This begs the question whether all kinds of operations against civilian objects are prohibited; which would be an over-simplification of the matter see Michael N. Schmitt, 'Attack as a Term of Art in International Law: The Cyber Operations Context' [2012] NATO CCD COE Publications 289 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2184833> accessed 15 November 2015; See also Michael N. Schmitt, 'PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors' (April 2015) Lecture at Harvard Law School <http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors> accessed 20 January 2016
151. See Rule 30 of the Tallinn Manual [91]

cyber-attacks; "a cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." Under this approach, cyber operations which damage the functionality of a system rendering it inoperative constitute an 'attack'[152] under IHL. However, global consensus has not been achieved on whether such damage to functionality must always be permanent or whether temporary damage will also suffice to constitute an attack. The functionality approach is supported by the Movement however it calls for a somewhat liberal understanding of this notion as the disabling of objects by means of cyber operations should constitute an attack because such a position is compatible with Art. 52 of AP I that refers to 'neutralization' of objects.[153]

To date, the only incident which could be classified as cyber-attack under the functionality approach, is the cyber sabotage campaign against Iran in September 2010. The US in collusion with Israel launched 'Operation Olympic Games'[154] whereby a computer worm 'Stuxnet' was aimed at causing malfunctions at Iran's Natanz uranium enrichment facility. Resultantly, a thousand centrifuges were decommissioned and replaced.[155]

The above classification of a cyber-attack and the approach of functionality

152. As the Tallinn Manual is reflective of de lege lata thus Rule 30 itself is unanimous; however, the commentary shows some disagreement among the IGE upon what 'functionality' signifies. In the majority view, where functionality is damaged in such a way to require replacement of the systems' component parts it would qualify as an attack. While in the view of the minority, complete destruction of the computer system that leads to loss of functionality would only qualify. Among the majority, opinion was again split on where functionality was restored by re-installing of operating system would that still be an attack or not. It was decided that it would not qualify as an attack. See Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' [2014] 96(893) IRRC 189 [198] – [201]; See also Commentary to Rule 30 of the Tallinn Manual [92] – [95]
153. "An overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities, which is to ensure the protection of the civilian population and civilian objects against the effects of hostilities. Indeed, under such a restrictive understanding, a cyber operation that is directed at making a civilian network (electricity, banking, communications or other network) dysfunctional, or risks causing this incidentally, might not be covered by the IHL prohibition of directing attacks against civilian objects, the prohibitions of indiscriminate or disproportionate attacks and the principle of precautions in attack, despite the potentially severe consequences of such operations for the civilian population." See 32nd International Conference of the Red Cross and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (Report) (December 2015) Doc. 32IC/15/11 [41] <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32 IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016
154. David E. Sanger, 'Obama Order Sped up Wave of Cyber Attacks against Iran' The New York Times (1 June 2012) <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0> accessed 17 November 2015
155. Marco Sassoli, Antoine A. Bouvier, and Anne Quintin, 'Iran, Victim of Cyber Warfare' (ICRC How Does Law Protect in War? July 2015) [Para 3] <https://www.icrc.org/casebook/doc/case-study/iran-victim-of-cyberwarfare.htm> accessed 28 November 2016, 'President Mahmoud Ahmadinejad recently admitted that a software attack affected Iran's centrifuges. "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts…"'

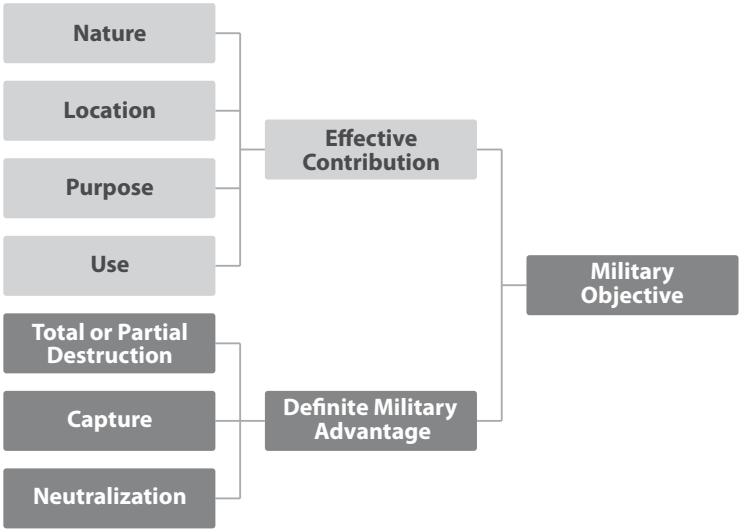
require further refinement and deliberation which would be seen through future State practice.[156] This is because standing as it does presently, all acts of violence in cyberspace which do not result in long-term damage to a systems' component parts fall outside the domain of 'cyber-attacks'.

3.1.1. 'Data' as an 'Object'

Another category of malicious activity that does not qualify as attack under the functionality approach is which results in loss of data stored on a computer system. This is because 'data' is not considered as an object, thereby incapable of protection even if it is civilian in nature.

Protection afforded to civilian objects is found in Rule 37 of the Tallinn Manual, while Rule 38 lays down the criteria for ascertaining objects as 'military'. Thus,

Figure: *Classification of Objects as 'Military Objectives'*



156. Jean-Marie Henckaerts, Cordula Droege, Laurent Gisel, Knut Dorman et al (contributors), Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (2nd edn, ICRC 2016) [256] <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518#94_B> accessed 13 December 2016

in that way defining civilian objects as being all those that do not qualify as military objects. These Rules are reflective of Art. 52(2) of AP I as well as Rules 7, 8, and 9 of CIHL.[157]

Art. 52(2) of AP I provides a framework for the classification of objects as military objectives. The criteria for ascertaining an object as military in nature, is when:

1. it effectively contributes through its nature, location, purpose or use to the military might of the adversary; and
2. its destruction, capture or neutralization affords definite military advantage to the aggressor.

Under Art. 52(1) only those objects are legitimate targets of attack that qualify as military objectives. While those that do not qualify as such, are to be deemed civilian in nature and thus protected from attacks and reprisals. Although this is seemingly convenient criteria to gauge in respect of cyber infrastructure or computers, problems arise with regards to 'data'.

The question whether data could be treated as an object or not attracted differing opinions among the IGE.[158] In view of the ordinary meaning[159] of the word 'object' as well as that given to it by the ICRC commentary to the Additional Protocols, an object is something tangible and visible.[160] Therefore, the majority of IGE opined that data does not qualify as an object.[161] Furthermore, it is not protected from attack because as it is not an 'object' thus its nature too cannot be ascertained under the criteria of Rule 38.[162]

The majority approach leads to the problematic conclusion that even if vital data is corrupted or lost due to cyber operations, such acts would not qualify as attacks while functionality is intact. Furthermore, because data is not an object it is not afforded any protection under existing IHL. However, in the Movement's opinion, such a conclusion would be incompatible with the

157. ICRC CIHL Study
158. See Commentary to Rule 38 of the Tallinn Manual [107] – [113]
159. "A thing that can be seen and touched, but is not alive" A. S. Hornby, Oxford Advanced Learner's Dictionary (6th edn, OUP 2005) 872
160. ICRC AP Commentary [Para 2021]
161. See Commentary to Rule 38 of the Tallinn Manual [Para 5]
162. Ibid

norms and object of IHL since corruption of or tampering with data has the potential to have greater detrimental impact[163] on civilian life than the loss of functionality of an information system.

The approach argued by the minority[164] is a more appropriate position, but was not accepted as there was no State practice to establish the same.[165] This approach rests on the idea that data is the most vital component of cyber technology. Therefore, if it is rendered useless or corrupted, regardless of whether the computer network itself is functioning, that should be regarded as an attack and data be afforded protection if determined to be civilian in nature.[166]

The position in Pakistan could be taken as more in accordance with the minority view above. Though the PEC Act does not define data per se, it does afford protection to certain kinds[167] of data and criminalizes unauthorized access,[168] transmission[169] and interference[170] with such data. Out of these, the third, i.e. 'interference with data' is the most important to gauge State practice regarding its protection. The relevant provisions are quoted herein below:

> "Section 5 – Interference[171] with information system[172] or data: Whoever with dishonest intention interferes with or damages[173] or

163. "Deleting or tampering with such data [i.e., social security data, tax records, bank accounts, companies' client files or election lists or records] could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects. The conclusion that this type of operation would not be prohibited by IHL in today's ever more cyber-reliant world – either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an object that would bring into operation the prohibition of attacks on civilian." See 32nd International Conference of the Red and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (December 2015) Doc. 32IC/15/11 [43] <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016
164. Michael N. Schmitt, 'The Notion of Objects during Cyber Operations: A Riposte in Defense of Interpretive and Applicative Precision' [2015] 48(1) Israel Law Review 81 <http://journals.cambridge.org/abstract_S0021223714000314> accessed 20 November 2015
165. See Commentary to Rule 38 of the Tallinn Manual [Para 5]
166. Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' [2014] 96(893) IRRC [200] – [201]
167. Content data, critical infrastructure data and traffic data, see The PEC Act s 2(1)(viii), 2(1)(xi), 2(1)(xxx) respectively
168. The PEC Act s 6
169. The PEC Act s 7
170. The PEC Act s 5, 8
171. The PEC Act s 2(1)(xxii) "interference with information system or data" means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data"
172. The PEC Act s 2(1)(xx)
173. The PEC Act s 2(1)(xii) "damage to an information system means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system"

> causes to be interfered with or damages any part or whole of an information system or data shall be punished ..."
>
> "Section 8 – Interference with critical infrastructure information system[174] or data: Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished..."

The PEC Act also criminalizes 'electronic forgery' which is caused by interference with information system or data by alteration, deletion or suppression of data thereby resulting in inauthentic data.[175] Similarly, Section 37 of the ETO criminalizes alteration, modification, deletion or removal of any information[176] through or on any information system.[177]

Thus, from the above provisions it is observed that in Pakistan 'data' is regarded as a crucial component of an information system and detrimental interference with it leads to criminal liability. Therefore, the same inference may be drawn in instances of cyber-attacks and data protected from such attacks. Moreover, where an act of violence is directed to such data and results in interference, alteration, deletion, or modification, it would amount to an 'attack' for the purposes of Rule 30 of the Tallinn Manual and thereby trigger an armed conflict as far as the State of Pakistan is concerned.

However, it may be observed that in the opinion of a prominent scholar Marco Sassoli,[178] "if deletion of data is included in the notion of attacks, then that is over-inclusive, but if you limit attacks to killing or injuring then that is too narrow because destruction is also a consequence of attack."[179] This view is also reflected in the updated Commentary to GC I, whereby the contributors opined that theft, deletion or destruction of data alone would not qualify as an attack because the requisite intensity of violence[180] is not likely to be

174. The PEC Act s 2(1)(xi)
175. The PEC Act s 13
176. Electronic Transactions Ordinance 2002 s 2(o) [hereinafter referred to as 'ETO']
177. ETO s 2(p)
178. Marco Sassoli, Professor of International Law, University of Geneva Switzerland; Associate Professor at the Universities of Quebec and Laval, Canada; Chairman of the Board of Geneva Call
179. Interview with Marco Sassoli, 'New Technologies and Warfare' (25 March 2014) ICRC Humanitarium, Geneva, Switzerland <https://www.youtube.com/watch?v=im9U9KR68QI> accessed 5 April 2016
180. NIAC is distinguished from internal disturbances based on the two-pronged test, i.e. the 'intensity of violence' and the 'organization of the parties to the conflict', see The Prosecutor v Dusko Tadic (Judgment) ICTY-1997-IT-94-I-T [7 May 1997] [Para 562]

reached.[181] It is therefore stressed that States should find a middle ground by applying the standard of Art. 52(2) of AP I and subsequently protect essential civilian data.

3.2. Identification and Attribution

Once it is determined that an act does amount to a cyber-attack, then questions arise as to the nature of the conflict. Ascertaining the nature of the armed conflict is inherently linked to the identification of the perpetrator, which in the cyber context remains excessively obscure.[182] The cyber-attacks on the US Bureau of Industry and Security in October 2006 are a case in point which were traced back to Chinese ISPs, raising fundamental and complex questions. Since the attackers could not be identified,[183] this instance highlights the role 'anonymity' plays in such attacks. Cyberspace makes it completely possible for attackers to hide their identity and to conceal[184] the true place of origin of the attack. In such a scenario, the US had to consider whether it could legitimately hold China responsible.[185] Moreover, aggressors may also leave 'false flags'[186] which further puts global security at risk.[187]

According to a January 2017 Background Report[188] to the US Joint Analysis Report (JAR)[189] of December 2016, "the nature of cyberspace makes

181. Jean-Marie Henckaerts, Cordula Droege, Laurent Gisel, Knut Dorman et al (contributors), Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (2nd edn, ICRC 2016) [437] <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?ac tion=openDocument&documentId=59F6 CDFA490736C1C1257F7D004BA0EC#147> accessed 13 December 2016
182. S. Ventkatesh, Cyber Terrorism (AuthorsPress, Delhi 2003) [1] – [7], [22] – [26]
183. Marco Roscini, Cyber Operations and the Use of Force in International Law (1st edn, Oxford University Press, London 2014) 33
184. Scott J. Shackelford and Richard B. Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' [2001] GJIL 982, "The 1998 'Solar Sunrise' attack that broke into the US Department of Defense system was for instance carried out by an Israeli teenager and Californian students through a computer based in the United Arab Emirates."
185. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology [379] <http://www.jstor.org/stable/40042831> accessed 16 November 2015
186. See generally Commentary Rule 8 of the Tallinn Manual, "The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State."
187. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 374 [397] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015; See also Commentary Rule 6 of the Tallinn Manual, "A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation."
188. National Intelligence Council, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytical Process and Cyber Incident Attribution' (Report) (6 January 2017) [2] <https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf> accessed 8 January 2017
189. Federal Bureau of Investigation and US Department of National Security, 'Grizzly Steppe – Russian Malicious Cyber Activity' (JAR Report) (29 December 2016) <https://www.us-cert.gov/sites/default/files/publications/ JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf> accessed 7 January 2017

attribution of cyber operations difficult but not impossible. Every kind of cyber operation—malicious or not—leaves a trail." However, the report itself gives little to no indication of this 'trail' and does not offer any proof thereby adding to the scepticism surrounding the veracity of US allegations of Russian hacking in to Democratic National Committee's (DNC) networks.[190]

3.3. Complexity in Attribution and Determining the Nature of Armed Conflict

There are manifold reasons embedded within the architecture of the internet that create complexity and perhaps even improbability of attribution.[191] Summarized, they may be categorized in to four layers[192] that provide numerous opportunities for anonymity.

Figure 2: *Internet Layers*

Data link	Hardware to Access the Internet
Transport	Breaking up and Reassembling Data
Network	Rerouting Data to its Destination
Applications	Direct User Interaction with the Software

As illustrated above, the first is the 'Data Link Layer' comprised of hardware used for internet access, e.g. Wi-Fi or broadband.[193] It may be noted that pre-paid or wireless internet does not record user identity thus contributing to anonymity.[194] However, more recently, domestic measures call for biometric

190. Ronald Deibert, 'The DHS/FBI Report on Russian Hacking was a Predictable Failure' (4 January 2017) Just Security <https://www.justsecurity.org/35989/dhsfbi-report-russian-hacking-predictable-failure/> accessed 7 January 2017; See also David E. Sanger, 'Putin Ordered "Influence Campaign" Aimed at US Election, Report Says' The New York Times (6 January 2017) <http://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html> accessed 7 January 2017
191. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 374 [397] – [400] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015
192. "The shared rules for formatting and transmitting data, known as the Transmission Control Protocol/Internet Protocol (TCP/IP), made the system work, and remain the foundation for today's Internet" Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 374 [398] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015
193. Tim Wu, 'Application-Centered Internet Analysis' [1999] 85 VLR [1189] – [1194]; See also Microsoft Support, 'The OSI Model's Seven Layers Defined and Functions Explained' (February 2002) <http://support.microsoft.com/kb/103884> accessed 10 March 2016
194. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal 374 [399] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015

verification of broadband internet to record user data.[195]

After the Data Link layer are the 'Transport' and 'Network' layers that are responsible for breaking up and reassembling data and then routing it to its destination. At these layers, as the first order of business, a victim would depend on the records of the ISPs to identify the perpetrator;[196] but these are routinely emptied due to overload.[197] In the context of Pakistan, it is pertinent to note that the PEC Act requires ISPs to retain specified[198] traffic data[199] for a minimum of one year.[200] However, even if record is available with the ISP, it could lead to a public place, like a library or internet café,[201] which provides users free access or to a corporation with a vast number of users hence virtually being useless data.[202]

Lastly is the 'Applications Layer'. At this layer the user is in direct interface with the software and most prone to cyber hostility. As clarified by a Pakistan Telecommunication Authority (PTA) spokesperson, "most cyber-attacks against government departments or other organizations were made possible 'due to vulnerabilities in their web application layer and endpoint infrastructure'."[203] Moreover, at this point a victim could easily be led to 'false flags' or 'stepping stones' which the perpetrator had employed for the very purpose of hiding his identity.[204]

---

195. See, e.g., Zaib un Nisa (Assistant Director PR), 'Biometric Verification System for Issuance of Wireless Local Loop Connections Launched for Safer Pakistan' (8 December 2015) Pakistan Telecommunication Authority<http://www.pta.gov.pk/index.php?option=com_content&task=view&id=2165&Itemid=739> accessed 15 April 2016
196. David Chaikin, 'Network Investigations of Cyber Attacks: The Limits of Digital Evidence' [2006] 46 CLSC 239 [244]
197. Ibid [245]
198. The PEC Act s 31, data which is required for a criminal investigation and there is risk of its being modified or lost, an authorized officer of the investigation agency may by written notice require the preservation of such data
199. The PEC Act s 2(1)(xxx)
200 The PEC Act s 32; see also ETO s 5, 6
201. "No law existed by which cyber cafes were required to keep record of persons using the computer of cafes" Qurban Ali v The State, 2007 PCrLJ 675 (Sindh)
202. Duncan B. Hollis, 'An e-SOS for Cyberspace' [2011] 52(2) Harvard International Law Journal [399] <https://citizenlab.org/cybernorms2012/esos.pdf> accessed 15 November 2015
203. Khawar Ghumman, 'Cyber Attacks against Govt. Expose Fatal Cracks in Pakistan's Digital Fence' Dawn News (Islamabad, 19 May 2015) <http://www.dawn.com/news/1182856> accessed 18 November 2016
204. Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It (HarperCollins Publishers 2010) [214] – [215]; David Chaikin, 'Network Investigations of Cyber Attacks: The Limits of Digital Evidence' [2006] 46 CLSC [245] – [246]

Even if it may be assumed that the point of origin of attack could be identified in a given case, the question would still remain whether the same could be attributed to the State of origin or not.[205] This is vital[206] because an armed conflict is categorized either as an IAC,[207] or a NIAC.[208] Where NIAC is recognized in the physical world, the same when analogically transported to cyberspace becomes very complex and difficult to establish.[209] A third instance is that of transboundary warfare between States and terrorist networks. This is a hard case for IHL[210] under traditional warfare itself,[211] thus rules pertaining to the same could hardly be applied analogically to

205. Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology 379 [413] – [415, [424] – [425] <http://www.jstor.org/stable/40042831> accessed 16 November 2015; See also Rule 7 of the Tallinn Manual, "The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation."
206. "An assessment of attribution usually is not a simple statement of who conducted an operation, but rather a series of judgments that describe whether it was an isolated incident, who was the likely perpetrator, that perpetrator's possible motivations, and whether a foreign government had a role in ordering or leading the operation" National Intelligence Council, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytical Process and Cyber Incident Attribution' (Report) (6 January 2017) [2] <https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf> accessed 8 January 2017
207. Susan W. Brenner, 'Toward a Criminal Law for Cyberspace: Distributed Security' [2004] 10(1) Boston University Journal of Science and Technology Law [45] – [46] <http://www.bu.edu/law/journals-archive/scitech/volume101/brenner.pdf> accessed 18 November 2015
208. GC, I, II, III, and IV common art 3; AP II art 1(1)
209. "It remains to be seen how State practice on classifying cyber operations as non-international armed conflicts will develop. Some commentators accept that in the light of 'ever more destructive and disruptive cyber operations and societies becoming deeply dependent on the cyber infrastructure, State practice accompanied by opinio juris can be expected to result in a lowering of the current threshold", in Jean-Marie Henckaerts, Cordula Droege, Laurent Gisel, Knut Dorman et al (contributors), Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (2nd edn, ICRC 2016) [437] <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?ac tion=openDocument&documentId=59F6CDFA490736C1C1257F7D004BA0EC#147> accessed 13 December 2016; See also Michael N. Schmitt, 'Classification of Cyber Conflict' [2012] 17(2) Journal of Conflict and Security Law 245 [260] <https://ssrn.com/abstract=2184831> accessed 23 December 2016; See also Susan W. Brenner, 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare' [2007] 97(2) The Journal of Criminal Law and Criminology 379 [403 – 404] <http://www.jstor.org/stable/40042831> accessed 16 November 2015; See also Susan W. Brenner, 'Toward a Criminal Law for Cyberspace: Distributed Security' [2004] 10(1) Boston University Journal of Science and Technology Law 105 – 106 <http://www.bu.edu/law/journals-archive/scitech/volume101/brenner.pdf> accessed 18 November 2015
210. In the opinion of the Movement, this hostile conduct is incorrectly termed 'war against terrorism'; in fact, it does not fall within the ambit of an 'armed conflict' thus IHL is not triggered in these circumstances. Rather it is a case of terrorism and counter-terrorism, which remains within the domain of domestic laws and human rights norms. See 32nd International Conference of the Red and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (December 2015) Doc. 32IC/15/11 <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016
211. Hans-Peter Gasser, 'Internationalized Non-International Armed Conflicts: Case Studies of Afghanistan, Kampuchea, and Lebanon' [1983] 33(145) The American University of Law Review [146] – [152]; James G. Stewart, 'Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict' [2003] 85(850) IRRC 313

cyberwarfare. Therefore, it becomes practically impossible to ascertain the nature of the armed conflict in cyberspace; with the perpetrator remaining hard to identify.[212]

For a cyber threat to be governed under the prohibitions[213] and restrictions[214] of jus in bello, it is essential that application of IHL be triggered through an armed conflict, which results from military operations, i.e., attacks. However, as the discussion in this section has shown, both the existence of attacks and the nature of an armed conflict are not easily inferable in the cyber domain. Therefore, compatibility of and adherence to IHL are mostly theoretical deliberations as long as these issues remain unresolved.

212. Jack M. Beard, 'Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law' [2014] 47(67) VJTL 73 [78] <http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1195&context=lawfacpub> accessed 15 November 2016
213. For example, AP I art 20, 37, 48
214. AP I art 28, 52, 57

SECTION 4

COMPATIBILITY OF CYBERWARFARE WITH IHL

Under the auspices of the UN General Assembly, the 2015 Group of Governmental Experts[215] confirmed that, "the established legal principles, including … the principles of humanity, necessity, proportionality and distinction"[216] were applicable to the use of Information and Communications Technologies (ICTs). Thus, affirming that IHL is applicable to cyberwarfare. However, these fundamental principles of IHL are neither easily nor absolutely replicable in cyberspace due to its differing characteristics from the physical world. Each of these principles is explained hereinafter in light of the Tallinn Manual, which based on existing IHL and CIHL provide a set of rules applicable in cyberwarfare.

4.1. Cyber Means and Methods of Warfare

The existing corpus of IHL does not expressly refer to cyber operations; however as noted before,[217] the ICJ observed that "the established principles and rules of humanitarian law… apply to all forms of warfare, and to all kinds of weapons, those of the past, those of the present and those of the future".[218] Accordingly, the IGE while determining rules for the legality of new cyber means and methods of warfare, adopted the same approach affirmed by the Court for legality of nuclear weapons.[219]

Section 5 of the Tallinn Manual constituting Rules 41 to 48, deals with cyber means and methods of warfare. Rule 41[220] defines the terms 'means' and 'methods'. Simply understood, 'means' are weapons while 'methods' are the techniques or strategies adopted for conducting cyber operations.

Under Rule 48 of the Tallinn Manual, all States are under customary[221] duty to ensure that any cyber means of warfare used or acquired by them are capable of compliance with IHL.[222] Furthermore, the IGE unanimously agreed that Art.

---

215. Group of Government Experts Report, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN General Assembly Doc. A/70/174 <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174> accessed 13 March 2016
216. Ibid [Para 28(d)]
217. See Section 2. 1.
218. Nuclear Weapons case [Para 86]
219. See Section 5 of the Tallinn Manual [118]
220. "For the purposes of this Manual:
    (a) 'Means of cyber warfare' are cyber weapons and their associated cyber systems; and
    (b) 'Methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted."
221. By virtue of Hague Convention IV art 1, and GC I, II, III, IV common art 1
222. See Commentary to Rule 48 of the Tallinn Manual [Para 2]

36 of AP I applies to all new means and methods of warfare, whether within the intention of the Parties at the time of ratification of AP or not.[223] Therefore, legal review of new weapons, means and methods while at the stage of "study, development, acquisition or adoption" remains an obligation on all States party to API.[224]

Pakistan is not a State party to AP I, therefore under the Tallinn Manual approach it is not obligated to review new cyber means and methods of warfare, nevertheless, it is bound by customary law to ensure compliance of IHL during acquisition or use of such methods. Expressed succinctly, Pakistan is under an obligation to have in place internal processes for review of new methods of cyberwarfare.

4.2. ESSENTIAL PRINCIPLES OF IHL

4.2.1. Principle of Distinction

This is the cardinal[225] principle of IHL, as the entire law of war is meant to reduce human suffering and protect non-combatants.[226] Enshrined within Art. 48 of API,[227] this principle calls for distinction between civilians and military personnel as well as civilian objects and military objectives. It requires that military operations only be targeted at military and military objectives. Practically this principle entails, for instance, that indiscriminate attacks[228] may not be launched.

The principle of distinction applies to cyberwarfare under Rule 31 of the Tallinn Manual in any nature of an armed conflict,[229] while indiscriminate attacks are prohibited under Rule 49. Though seemingly simple in traditional or kinetic warfare that occurs in a real, stable environment, this rule becomes quite complex to adhere to in the cyberspace. The primary reason is that the internet thrives on its interconnectedness. Therefore, military objectives are often run on inherently civilian infrastructure.[230] Furthermore, most objects in

223. See Section 5 of the Tallinn Manual [118]; See also Commentary to Rule 41 of the Tallinn Manual [Para 2]; Rule 48 of the Tallinn Manual
224. Rule 48 of the Tallinn Manual
225. Derived from the St. Petersburg Declaration preamble; See also Nuclear Weapons case [Para 78] [79]
226. Nils Melzer, International Humanitarian Law: A Comprehensive Introduction (ICRC Geneva, 2016) 134
227. See also Rule 1 of ICRC CIHL Study
228. AP I art 51(4)
229. See Commentary to Rule 31 of the Tallinn Manual [Para 2]
230. Khawar Ghumman, 'Cyber Attacks against Govt. Expose Fatal Cracks in Pakistan's Digital Fence' Dawn News (Islamabad, 19 May 2015) <http://www.dawn.com/news/1182856> accessed 18 November 2016

cyberspace are bound to be dual[231] in nature, making distinction relatively challenging.

4.2.2. Principles of Military Necessity and Proportionality – Direct and Indirect Effects

Military necessity[232] dictates that the military commander shall direct cyber-attacks solely against military objects and objectives,[233] however, where such distinction is not possible then the principle of proportionality[234] is invoked. Rule 51 of the Tallinn Manual is reflective of this principle which is embodied in Art. 51(5)(b) and Art. 57(2)(iii) of AP I, as well as in Rule 14 of CIHL.

Under proportionality an attack is prohibited where collateral damage to civilian life and/or objects would be in excess to the concrete and direct military advantage to be gained from it. While judging proportionality, a commander is further required to assess not only the direct[235] effects an anticipated cyber-attack would have on civilian life or objects, but also any foreseeable indirect[236] effects. For example, interfering with air traffic control would likely affect civilian aircrafts as well; therefore, it must be factored into proportionality. However, where for instance, malware directed at a secure military objective is unexpectedly transferred from its intended target by a portable device and thus leaked into civilian cyber infrastructure, it would not qualify as neither a foreseeable nor indirect effect.[237]

---

231. "In practice, almost any civilian object can be used for military purposes and can therefore be a military objective for the duration of such use. Objects simultaneously used for civilian and military purposes are particularly problematic. Typical examples of objects that might become "dual-use" objects are logistical infrastructure (roads, bridges, railways, ports and airports), power plants, and electricity and communication networks." Nils Melzer, International Humanitarian Law: A Comprehensive Introduction (ICRC Geneva, 2016) 92
232. See St. Petersburg Declaration preamble; See also Marco Sassoli, Antoine A. Bouvier and Anne Quintin, 'Military Necessity' [ICRC How Does Law protect in War?] (June 2012) <https://www.icrc.org/casebook/doc/glossary/military-necessity-glossary.htm> accessed 10 November 2015
233. For determination of objects as 'military' see Figure 1 above, Section 3.1.1.
234. "Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited." Rule 14, ICRC CIHL Study
235. "Immediate, first order consequences, unaltered by intervening events or mechanism" in Chairman, Joint Chiefs of Staff, 'Joint Targeting' (13 April 2007) Joint Publication 3-60 at I-10 <http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf> accessed 11 January 2016
236. Ibid "The delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms"
237. See Commentary to Rule 31 of the Tallinn Manual [Para 6]; See also Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack' [2013] 89 International Law Studies 207 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2154938> accessed 20 November 2015

Furthermore, cyber-attacks against dual-nature objects are not prohibited because such objects are considered military objects under Rule 39 of the Tallinn Manual, unless excessive damage is anticipated to be caused to civilian life or objects.[238] Moreover, such an assertion does not mean that the commander is precluded from taking precautions in attack.[239]

4.2.3. Principle of Precautions in Attack

The principle of precautions in attack is divided into two categories under IHL. First is the responsibility to assess the 'feasibility of attacks' which fall under active precautions, while the other is the obligation of passive precautions 'against dangers resulting from attacks'.

A. Feasibility of Cyber-Attacks

The 'feasibility' criterion is not expressly defined in IHL, however, as a committee constituted by the International Criminal Tribunal for Yugoslavia (ICTY) observed:

The obligation to do everything 'feasible' is high but not absolute. A military commander must set up an effective intelligence gathering system to collect and evaluate information concerning potential targets... must also direct his forces to use available technical means to properly identify targets during operation.[240]

Rules 52 to 58 of the Tallinn Manual are reflective of IHL[241] in this respect. These Rules require constant care[242] to spare civilians from the effects of attacks and to verify targets[243] as well as issue warnings.[244] Among other things[245] it also requires that in case the proportionality criteria is not met, the attack be cancelled or suspended.[246]

B. Precautions against Dangers Resulting from Cyber-Attacks

Under Rule 59[247] parties to a conflict are under an obligation to take all

238. See Commentary to Rule 51 of the Tallinn Manual [Para 4]; See also Commentary to Rule 39 of the Tallinn Manual [Para 2]
239. See Commentary to Rule 39 of the Tallinn Manual [Para 4]
240. ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia (June 8, 2000) reprinted in 39 I LM 1257 (2000) [Para 129]
241. AP I art 57
242. Rule 52 of the Tallinn Manual
243. Rule 53 of the Tallinn Manual; Rule 16 of ICRC CIHL Study
244. Rule 58 of the Tallinn Manual
245. See Rules 54 and 56 of the Tallinn Manual
246. Rule 57 of the Tallinn Manual
247. Based on AP I art 58(c) and Rule 22 of ICRC CIHL Study

feasible measures and to protect civilians under their control[248] from the dangers resulting from a cyber-attack. It is also pertinent to note that though the passive protection obligations laid down in clauses (a)[249]and (b)[250] of Art. 58 of AP I are not expressly incorporated in the Tallinn Manual, they are implicit[251] in Rule 59 as it is a 'catch-all' provision encompassing the entirety of passive protections.[252]

According to the majority of IGE, 'dangers' would mean loss of civilian life, death or injury to civilians and damage to civilian objects. However, the minority asserted that such dangers should include major disruption of day to day life too, but not merely irritation or inconvenience.[253] Like the previous principles, this principle also posits challenges because globally military systems rely on civilian infrastructure.[254]

It is a particularly alarming situation for Pakistan, as "telecom companies control critical infrastructure in any nation, the impact of an attack against their networks could have far-reaching repercussions."[255] Moreover, for better cyber functionality the accepted practice within organizations is to run their cyber infrastructure on 'shared networks'.[256] This measure also weakens their security because even though particular ISPs may ensure security of their

248. For the purposes of kinetic warfare, 'control' is understood as within the territory of the defending State. This approach adopted by the majority of the IGE for the purposes of cyber warfare including unoccupied territory as well as enemy occupied territory. However, a minority of IGE opined that this obligation could not be conceived territorially, as in the cyberspace it is possible to not be in control of a computer system which is located within a particular State's territory. See ICRC AP Commentary [Para 2239]; See also Commentary to Rule 59 of the Tallinn Manual [Para 8]
249. To remove the civilian population, objects or individuals, from the vicinity of military objectives
250. To not locate military objectives in urban areas
251. See Commentary to Rule 59 of the Tallinn Manual [Para 10]
252. See Commentary to Rule 59 of the Tallinn Manual [Para 4]
253. See Commentary to Rule 59 of the Tallinn Manual [Para 9]
254. See for example News Desk, 'NSA Spied on Pakistani Civil-Military Leadership' Dawn News (Islamabad 21 August 2016) <http://tribune.com.pk/story/1166854/nsa-spied-pakistani-civil-military-leadership/> accessed 19 December 2016 "The United States' National Security Agency (NSA) hacked Pakistan's National Telecommunications Corporation (NTC) to spy on Pakistani civilian and military leadership, online publication The Intercept reported …"
255. Khawar Ghumman, 'Cyber Attacks against Govt. Expose Fatal Cracks in Pakistan's Digital Fence' Dawn News (Islamabad, 19 May 2015) <http://www.dawn.com/news/1182856> accessed 18 November 2016
256. "The same cyber functionality that enables great efficiency along the chain — from raw materials procurement to production to inventory and distribution — also introduces vulnerability at every link. A hack that brings down a vital piece of equipment, sometimes for only a few hours, can start a chain reaction. Disruptions in procurement impede production, which can deplete inventories and result in the inability to fulfil orders. As each link in the chain is impaired, financial losses mount." Deloitte, 'Focus On: The Board's-Eye View of Cyber Crisis Management' <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-cm-focus-on-cyber-crisis-management.pdf> accessed 9 January 2017

channel, it is still possible for an infected department to infect other systems on its networks because of shared infrastructure.[257] Such practices make it difficult to distinguish between and to protect essential infrastructure from excessive incidental loss.

257. Deloitte, 'Focus On: The Board's-Eye View of Cyber Crisis Management' <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ers-cm-focus-on-cyber-crisis-management.pdf> accessed 9 January 2017

SECTION 5

CONCLUSION AND RECOMMENDATIONS

Means such as those considered or adopted during the conflicts in Iraq,[258] Libya[259] and Syria[260] have brought cyber operations to the forefront of global attention261. Furthermore, the cyber operations mounted during the Russia–Ukraine[262] and Palestine–Israel[263] conflicts of 2014 have demonstrated the continued necessity for clarification as to how international law is to be interpreted and applied with respect to activities in cyberspace.[264]

It is expected that such means which are fast becoming the norm[265] will

258. In 2003, before the US-Iraq war, the US considered blocking Saddam Hussein's bank accounts so that he would not be able to fund the upcoming war. However, due to the risks such an implementation posed to European cyber infrastructure, these means were not adopted. See Eric Jensen Talbot, 'Cyber Attacks: Proportionality and Precautions in Attack' [2013] 89 International Law Studies [208] <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2154938> accessed 20 November 2015; See also John Markoff and Thom Shanker, 'Halted '03 Iraq Plan Illustrates US Fear of Cyber-war Risk' The New York Times (1 August 2009) <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=0> accessed 22 November 2015
259. Right before the kinetic attacks were launched against Libyan air-defense, the US considered cyber-attacks for the same purpose. Though these means were then not adopted due to the fear of setting a precedent that could be followed by other States in similar situations, especially China and Russia. See Eric Schmitt and Thom Shanker, 'US Debated Cyber-warfare in Attack Plan on Libya' The New York Times (17 October 2017) <http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html> accessed 22 November 2015; See also Jack L. Goldsmith, 'Quick Thoughts on the US Governments' Refusal to Use Cyber-attacks in Libya' (18 October 2011) Brookings Institute <http://www.brookings.edu/blogs/up-front/posts/2011/10/18-cyberattack-libya-goldsmith> accessed 22 November 2015
260. The Global Research and Analysis Team at Kaspersky Lab discovered new malware attacks in Syria, with malicious entities using a plethora of methods from their toolbox to hide and operate malware. In addition to proficient social engineering tricks, victims were often tempted to open and explore malicious files because of the dire need for privacy and security tools in the region. In the hopes of maintaining anonymity and installing the latest "protection", victims fall prey to these malicious creations. Report, Kaspersky Lab Global Research and Analysis Team, 'Syrian Malware, the Ever-Evolving Threat' (August 2014) Kaspersky Lab <https://securelist.com/files/2014/08/KL_report_syrian_malware.pdf> accessed 7 February 2016; See also Eva Galperin, Morgan Marquis-Boire and John Scott-Railton, 'Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaign' (Electronic Frontier Foundation 2013) <www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf> accessed 17 November 2015
261. Shane Harris, 'The Cyber War Plan,' [2009] National Journal Online <www.nationaljournal.com/member/magazine/the-cyberwar-plan-20091114> accessed 18 November 2015
262. The Ukraine crisis between 2013 and 2015 demonstrates that cyber-attacks have been used in a broader strategy of information warfare. They encompass digital propaganda, DDoS campaigns, website defacements, information leaks and cutting-edge cyber espionage malware. See Kenneth Geers (ed.), Cyber War in Perspective: Russian Aggression against Ukraine (NATO CCD COE Publications, Tallinn 2015)
263. Rebecca Kaplan, 'The Next front in the Israel-Gaza Conflict?' CBS News (28 July 2014) <http://www.cbsnews.com/news/cyber-warfare-the-next-front-in-the-israel-gaza-conflict/> accessed 11 January 2016
264. Michael N Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defense of Interpretive and Applicative Precision' [2015] 48(1) Israel Law Review 84 <http://journals.cambridge.org/abstract_S0021223714000314> accessed 20 November 2015
265. Lt. Gen. Richard P. Mills (Speech at AFCEA TechNet Land Forces East Chapter Lunch 21 August 2012) <www.slideshare.net/afcea/afcea-technet-land-forces-east-aberdeen-chapter-lunch-ltgenrichard-p-mills-usmc> accessed 20 November 2015

ultimately serve as the primary offence tool because they are relatively cheaper to maintain and do not require as much manpower as kinetic warfare does.[266] This makes it all the more urgent to bind them within the constraints of IHL[267] as protecting humanity is the entire raison d'être[268] of the law of war.[269]

It is well-accepted that new means and methods of warfare fall within the ambit of IHL,[270] and must not be incapable of being used in accordance with the fundamental principles of the law of war. However, owing to the difficulties[271] that arise in interpretation of IHL to regulate cyberwarfare, some scholars believe that perhaps a new Convention would provide answers.[272] It is put forth that as with numerous conventions and treaties, they take many years to draft and even more to come in to force,[273] while technology itself grows at rapid speed and poses a serious threat such that even nuclear facilities[274] and other installations containing danger forces, such as dams, are rendered unsecure. Therefore, such a solution could be detrimental to the protection of vulnerable segments of the society essentially undermining the purposes of IHL. Thus, amendments or further clarifications, as required, in the existing international instruments are a more viable option.

Moreover, recent years have shown international organizations, publicists and academics playing a more active role in understanding and developing

266. Susan W. Brenner and Leo L. Clarke, 'Civilians in Cyberwarfare: Conscripts' [2010] 43 Vanderbilt Journal of Transitional Law 3 <http://ssrn.com/abstract=1650743> accessed 30 December 2016
267. ICRC, 'Weapons: ICRC Statement to the United Nations, 2015' (October 2015) <https://www.icrc.org/en/document/weapons-icrc-statement-united-nations-2015> accessed 12 November 2015
268. Reason for being/existing
269. Robert Cryer, Hakan Friman, Darryl Robinson and Elizabeth Wilmshurst, An Introduction to International Criminal Law and Procedure (2nd edn, Cambridge University Press 2010) 268
270. See Section 2
271. Jeffery T.G. Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' [2008] 106(7) Michigan Law Review 1427 <http://www.jstor.org/stable/40041623> accessed 10 November 2015
272. See for example Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' [2006] 47(1) Harvard International Law Journal 215 <http://www.harvardilj.org/wp-content/uploads/2010/10/HILJ_47-1_Brown.pdf> accessed 10 November 2015
273. For example Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (adopted 13 January 1993, entered into force 29 April 1997) UNGA A/RES/47/39; See also Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (adoption 16 December 1971, entered into force 26 March 1975) 1015 UNTS
274. NTI, 'Cybersecurity: Addressing the Growing and Potentially Catastrophic Cyber Threat to Nuclear Systems and Facilities around the World' <http://www.nti.org/about/cyber/> accessed 7 January 2017

IHL in comparison to States. However,[275] incidents such as the Sony hack,[276] the APT28 Report[277] on Russian phishing[278] activities, the US-China agreement[279] against corporate espionage[280] and the alleged Russian hacking of the DNC servers[281] have not just directed attention towards this growing problem but have also forced States to actively deliberate on how to deal with and ward off such situations.[282] Though these are not incidents of cyber-attacks within the meaning of IHL but their handling does contribute towards evolving State practice.[283] It is vital that these deliberations must be done while keeping the fundamental principles of IHL at their core, in order to build on them and strengthen them.[284]

---

275. "The reluctance of States and their legal representatives to communicate and commit to clear views on IHL matters vitiates legal discourse, degrading the functioning and development of a critical aspect of the international legal system…" in Michael N. Schmitt and Sean Watts, 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare' [2015] 50(2) Texas International Law Journal [189] <http://www.tilj.org/content/journal/50/14%20SCHMITT%20&%20WATTS%20PUB%20PROOF.pdf> accessed 10 April 2016
276. Julia Boorstin, 'The Sony Hack: One Year Later' CNBC (24 November 2014) <http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html> accessed 10 December 2016
277. FireEye, 'APT: A Window into Russia's Cyber Espionage Operations?' (Special Report) (27 October 2014) <http://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf> accessed 16 November 2016
278. "This refers to illegal attempts to acquire sensitive information such as usernames, passwords, and credit card details often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication, such as someone you know or regularly correspond with."
279. The White House, Office of the Press Secretary, 'Fact Sheet: President Xi Jinping's State Visit to the United States' (Press Release) (25 September 2015) <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> accessed 7 January 2017
280. Gary Brown and Christopher D. Yung, 'Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace' The Diplomat (19 January 2017) <http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/?allpages=yes&print=yes> accessed 21 January 2017
281. National Intelligence Council, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytical Process and Cyber Incident Attribution' (Report) (6 January 2017) [2] <https://assets.documentcloud.org/documents/3254237/Russia-Hack-Report.pdf> accessed 8 January 2017; See also David E. Sanger, 'Putin Ordered "Influence Campaign" Aimed at US Election, Report Says' The New York Times (6 January 2017) <http://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html> accessed 7 January 2017
282. Mark Pomerleau, 'Hope for Global Cyber Norms Struggles Following Russian Hacking Allegations' (C4ISRNET 5 January 2017) <http://www.c4isrnet.com/articles/hope-for-global-cyber-norms-struggles-following-russian-hacking-allegations> accessed 10 January 2017
283. See generally Jean-Marie Henckaerts, Cordula Droege, Laurent Gisel, Knut Dorman et al (contributors), Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (2nd edn, ICRC 2016) [256] <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?ac tion=openDocument&documentId= BE2D518CF5DE54EAC1257F7D0036B518#94_B> accessed 13 December 2016; See also Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack,' [2014] 96(893) IRRC 189; See also William J. Bayles, 'The Ethics of Computer Network Attack' [2001] Parameters 44 <http://www.iwar.org.uk/iwar/resources/ethics-of-cna/bayles.htm> accessed 28 February 2016
284. 32nd International Conference of the Red and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (December 2015) Doc. 32IC/15/11 <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016

Furthermore, the initial point to improved cyber security would be to separate military and civilian infrastructure as far as possible;[285] and to afford protection to essential infrastructure.[286] Another crucial step would be for military commanders to seek active advice from IHL experts for policy formulations. Many States over the years have established such Cyber Commands[287] with news of Indian deliberations on the same.[288]

It is proposed that the State of Pakistan instead of a reactive paradigm to cybersecurity should be more proactive and preventive in its approach.[289] No State should wait till it is subjected to attacks for discovering the flaws in its security, rather it should actively identify these lacunae and seek to address them. This would be best achieved through a unified cyber command, whereby the military commanders of armed forces and more importantly cyber security experts and legal advisors through their shared resources, unique expertise and experience[290] could tackle the challenges of cyberwarfare and minimize the threat posited by others in possession of offensive cyber capabilities.

---

285. See 32nd International Conference of the Red and Red Crescent Report, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (December 2015) Doc. 32IC/15/11 <http://rcrcconference.org/wp-content/uploads/sites/3/2015/10/32IC-Report-on-IHL-and-challenges-of-armed-conflicts.pdf> accessed 17 April 2016
286. Ibid [43]
287. US Cyber Command (USCYBERCOM) <http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/> accessed 17 November 2016; Strategic Support Force, China; Cyber Defense Cell, France
288. James A. Lewis and Katrina Timlin, 'Cybersecurity and Cyber Warfare: Preliminary Assessment of National Doctrine and Organization' (2011) (UNIDIR Report) [13] <http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf> accessed 29 November 2016; See also Centre of Excellence for Cyber Security Research and Development in India (CESRDI), 'India Speeding up Formation of Tri-Service Cyber Command for Armed Forces of India' (Global Techno Legal News and Views 7 June 2016) <http://perry4law.co.in/news/?p=182> accessed 20 December 2016; see also Arun Mohan Sukumar, 'Upgrading India's Cyber Security Architecture' The Hindu (9 March 2016) <http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece> accessed 3 January 2017; See also Abhishek Bhalla, 'India gets Set for Unified Cyber Cell' Daily News & Analysis, (New Delhi, 3 December 2016) <http://www.dnaindia.com/india/report-india-gets-set-for-unified-cyber-cell-2279175?utm_content=buffer20bdb&utm_medium=social&utm_source=t witter.com&utm_campaign=buffer> accessed 5 December 2016
289. Louis M. Giannelli, The Cyber Equalizer: The Quest for Control and Dominance in Cyber Spectrum (2012) [CH 11]
290. For example, in July 2016 Poland inaugurated such a centre whereby putting research, operational tasks, training and analytics under one roof in collaboration with all stakeholders including telecommunications and banking sectors. Daria Mamont, 'Poland Launched National Cybersecurity Centre' (6 July 2016) <http://wbj.pl/poland-launches-national-cybersecurity-center/> accessed 17 January 2017; See also Alexander Klimburg (ed.), National Cyber Security: Framework Manual (NATO CCD COE Tallinn, 2012)