International Criminal Law And Its Response To Digital Crime: A Roadmap for Pakistan

By

MARVI MUSTAFA

LLM HUMAN RIGHTS LAW

REG NO: 286-FSL/LLMHRL/F19

UNDER THE SUPERVISION OF

PROF. DR. SADIA TABASSUM

DEPARTMENT OF LAW

FACULTY OF SHARIAH AND LAW

INTERNATIONAL ISLAMIC UNVERSITY ISLAMABAD

NOVEMBER 2022

International criminal law

Computer crimes - Law and legislation

Digital media - " "

Cybercrime - Pakistan

Criminal justice, Administration of - Pakistan

APPROVAL SHEET

INTERNATIONAL CRIMINAL LAW AND ITS RESPONSE TO DIGITAL CRIME; A ROAD MAP FOR PAKISTAN

By

Marvi Mustafa

LLM (Human Rights Law)

Reg. No. 286-FSL/LLMHRL/F19

Accepted by the Department of Law, Faculty of Shariah & Law, International Islamic University, Islamabad in the partial fulfillment for the award of the degree of LL.M (Human Rights Law).

Supervisor: ______________________

Dr. Sadia Tabassum,
Assistant Professor,
Faculty of Shariah & Law
International Islamic University, Islamabad.

Internal Examiner: ______________________

Ms. Ghazala Ghalib Khan,
Assistant Professor,
Faculty of Shariah & Law
International Islamic University, Islamabad.

External Examiner: ______________________

Dr. Yasar Aman Khan
Advocate, Supreme Court.

Abstract

Cybercrimes, originated with the advancements in information technology, are developing at a faster pace with the developments in computer and its related technologies. Cybercrimes are complex and transnational in nature and whole world is facing the cybercrime threat so there is a dire need of updated and developed cybercrime laws to effectively deal with the cybercrimes. The transnational nature of cybercrimes requires international laws to be followed by all states. The international community is cooperating by making laws and institutions to control cybercrimes. Pakistan is also facing the cybercrime threat and steps are being taken at public and private both levels to deal with the cybercrimes. Research concludes that the steps taken in Pakistan have proved helpful to some extent but there is a need of effective and updated laws to cope with the emerging cybercrime threats. The cyberspace of Pakistan can be saved by providing awareness about cyber threats and laws among general public. The standard of IT education and laws can also play an important part in saving Pakistan from emerging threat of new kinds of cybercrimes.

Acknowledgment

I want to acknowledge and express my sincere gratitude to my supervisor (Dr. Saadia Tabbasum). who helped me through every stage of writing my thesis and who made my effort feasible.

Additionally, I would like to express my gratitude to my father, son, and my friend Nida for their unwavering encouragement and support during the course of my research and thesis writing. I've made it this far thanks to your prayers for me.

Finally, I want to express my gratitude to Allah for guiding me through all of my challenges. Every day, I experience Your guidance. Only You enabled me to finish my degree. I trust You and continue to put my future in your Hands.

Table of Contents Table of Contents

Introduction

CHAPTER 1 History and Nature of Cybercrimes

CHAPTER 2

International Legislative Framework on Cybercrimes

Chapter 3

Strategies Adopted by International and National Bodies to Reduce Cybercrimes

Chapter 4

Lesson for Developing Countries and Specifically for Pakistan

CONCLUSION

BIBLIOGRAPHY

THESIS STATEMENT

While internet in today's world is perceived more of a fundamental right than a need, there are growing concerns among the global community about providing a safe sphere for the users in the wake of emerging digital crimes. International criminal law has keenly taken up the subject and laws are framed to penalize such cybercrimes but with reference to Pakistan, efforts have been made in recognizing digital crimes are not satisfying with growing advancements, and there are loopholes in legislating over it.

Introduction

This research has explored the nature and evolution of cybercrimes and the different techniques applied to perform categories of cybercrimes. It has analyzed the cybercrimes legislations applicable around the world. In this regard cybercrime laws of the United States of America and the United Kingdom are analyzed. The role of national and international law enforcement bodies to deal with the issue of cybercrimes is also be analyzed. The cybercrime laws enforced in Pakistan are also analyzed in detail.

Legal Questions

1. If cybercrimes are increasing in the world, then what attempts have been done by the states to save themselves from cybercrime threats.

2. If Pakistan is also effected by cybercrimes, then what efforts have been done by Pakistan.

3. Whether the cybercrime laws in Pakistan are updated and able to deal with the emerging cybercrime threats, if not then what are the possible ways to make Pakistan a safer cyber place.

Cybercrimes and the World

The relationship of human beings and crimes dates back to the creation of mankind. The basic reasons for criminal activities may be desire for money, power or other social or personal benefit that remain unchanged at all times. Major changes in this regard are the tools and phenomenon adopted to accomplish the illegitimate objectives of criminals.[1] The style of committing crimes has developed with the passage of time but the basic motive behind the criminal activities has remained unchanged.

With the advancement of digital technology, cyberspace and the internet has become an integral part of our routine works and businesses.[2] Though this technological progress has brought tremendous positive revolution in our lives, in addition to this, it has paved the way for new sort of crimes committed through the abuse of computers.[3] Cybercrimes are basically associated with different computer-related activities performed for attaining illegal objectives.[4] It can also be described as the use of computers in order to harm others[5] for their personal benefits. In order

[1] Calum Jaffery and Tobias Feakin, "Underground Web: The Cybercrime Challenge" Australian Strategic Policy Institute 2015, 1, accessed 20 February, 2022. http://www.jstor.org/stable/resrep04074.

[2] Lior Tabansky, "Cybercrime: A National Security Issue". Military and Strategic Affairs 4: no.3 (December 2012), 117.

[3] Majid Yar and Kevin F. Steinmetz, *Cybercrime and Society*, 3rd ed. (London: Sage Publications, 2019), 4; Joshua B. Hill and Nancy E. Marion, Introduction to Cybercrime: Computer Crimes, Laws & Policing in the 21st Century (Santa Barbara CA: Praeger Publishers, 2016), 4.

[4] Budi Arief, Mohd AzeemBin Adzmi, and Hoams Gross, "Understanding Cybercrimes from Its Stakeholders perspectives: part 1-Attackers", IEEE Security & Privacy 13, no 1 (2015), 71, accessed 10 February, 2022.

[5] Ebi Robert, "Attempting a Definition of Cybercrime", (April 20, 2021), 1, accessed 15 February, 2022. http://ssrn.com/abstract=3830589.

to have a complete understanding of Pakistan's response to cybercrimes, it is vital to have some basic knowledge about the evolution of cybercrimes and how these crimes have been described by different scholars and international documents. The details are mentioned in coming chapter.

Computer and its related technologies are expanding and so are the cybercrimes. Various sophisticated techniques are applied to commit different kinds of cybercrimes that are developing with the passage of time. The techniques used to commit different kinds of cybercrimes conducted by the application of various techniques have been mentioned in the coming chapter to have a better understanding of the phenomenon of cybercrimes. Surveys and research have revealed that the issue of cybercrimes is increasing at a faster pace and many countries are working and cooperating with each other at international level to curb the problem.[6]

Literature Review

In order to formulate a clear understanding of the concept of cybercrimes and the need for legislation in Pakistan, many books and articles have been consulted. ***The Internet Myth: From the Internet Imaginary to Network Ideologies***[7] written by ***Paolo Bory.*** provides a detailed description regarding the history of evolution of internet and the theories linked to its evolution with reference to variety of sources. The author has used historical approach in the collection of data about evolution and development of internet in the world. He has also discussed even those attempts of building the internet

[6] S. M. Furnell, "Categorising Cybercrime and Cybercriminals: The Problem and Potential Approaches", *Journal of Information Warfare* 1: no 2 (2001), 35.

[7] Bory, Paolo. *The Internet Myth: From the Internet Imaginary to Network Ideologies*. London: University of Westminster Press, 2020.

that failed and have been forgotten with the main idea that failure always leads to success. The attempts of Italian computer experts that were unsuccessful is an instance of such examples presented in the book to remember these forgotten events. This book provides great help in understanding the efforts carried out by the experts of different countries during the evolution and development of internet.

Cybercrime: Key Issues and Debates[7] has been written by ***Alisdair A. Gillespie.*** This book explains key issues related to cybercrimes in an effective manner. The author has provided a detailed account of the cybercrime legislations in the United Kingdom and Europe. Different categories of cybercrimes including the newly emerging trends of the illegal use of cyber technology, like cyber terrorism, have also been discussed in the book with detail. The book is basically written with the purpose of providing knowledge regarding cybercrimes to the students hence provides a clear understanding on the topic to the new readers. This book will be of great help during the present research.

Introduction to Cybercrime: Computer Crimes, Laws & Policing In the 21st Century[8] written by ***Joshua B. Hill and Nancy E. Marion.*** This book explains evolution of internet with a detailed account of history of cybercrimes that developed with the developments of computer and its related technologies. Different categories of cybercrimes have been mentioned in the book along with a detailed description of the efforts of the law enforcement agencies to deal with these crimes. Two separate chapters have been allocated to the new emerging crimes of cyber terrorism and cyber war. The book presents a very effective description of the response of the US government and the international community to deal with cybercrimes. The book is

[8] Hill and Marion, *Introduction to Cybercrime.*

relevant to present research and will be of great help in understanding the concept of cybercrimes and its evolution.

Cyberspace Management in Pakistan[9] written by ***Dr. Tughral Yamin.*** In this article, the author has explained cyber security in an effective manner. Cybersecurity models of different countries including the US, Australia and India have been discussed in the research. The need of having an effective Cybersecurity plan has been explained with examples of cyber threats to Pakistan from other states including India. He has also pointed out towards lack of efforts on national level and has stressed that efforts at national level are required in Pakistan to respond to cyber security threats likely to cause massive destruction. This article is very helpful in formulation of a clear idea about need of cyberspace management in Pakistan and about steps to make an effective strategy.

Cybersecurity and US Legislative Efforts to address Cybercrime[10] has been written by ***Angelyn Flowers, Sherali Zeadally and Acklyn Murray.*** The authors have explored legislative attempts to deal with the emerging cybercrime trends in the US. the jurisdictional limitations faced in the application of cyber laws has been mentioned with some incidents of cybercrimes committed outside the boundaries of the US. The laws made by different other countries have also been analyzed in the article. The article is related to the present research and will help a lot in getting knowledge about the US cyber laws. This article has mentioned cyber laws of the United Kingdom in a precise manner that will be discussed in present research in

[9] Tughral Yamin, "Cyberspace Management in Pakistan", *Governance and Management Review* 3: no 1 (2018); 46-61.

[10] Angelyn Flowers, Sherali Zeadally and Acklyn Murray, "Cybersecurity and US Legislative Efforts to address Cybercrime", Homeland Emergency & Security Management 10: 1 (2013), 1-27.

detail.

Electronic Crimes Ordinance: An Overview of Its Preamble and Extent[11] written by ***Muhammad Amir Munir.*** This article is an analysis of Prevention of Electronic Crimes Ordinance, 2007. The author has made a comparative analysis of the preamble of the Ordinance with the preambles of the cybercrime laws of the UK, the US, India and Malaysia. Different ambiguities present in the ordinance have also been analyzed in detail. The article is of much importance to the present research but it does not deal with the latest legal developments so the present research aims to fill in this gap and discuss the latest developments in Pakistan.

Cybercrime, Internet and Cybercrime Legislation: A Study of Pakistan[12] written by ***Abdul Ghaffar Korai, Abdul Samad, Ahad Ghaffar, Javed Ahmed and Imtiaz Ahmed Memon.*** This article is an account of cybercrimes in Pakistan and legislation to stop these crimes. The global perspective of cybercrimes and different categories of cybercrimes have also been mentioned in the article. This article is related to present and has been helpful during research but the topics have been mentioned in a brief manner. Present aims to fill in this gap and describe the topics in a detailed manner especially development of different cybercrimes trends and the legislations in Pakistan in detail.

The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium written by ***Michael A. Sussmann.***[13] This article is an

[11] Muhammad Amir Munir, "Electronic Crimes Ordinance: An Overview of Its Preamble and Extent", Pakistan Journal of Criminology 2: no1 (Quarterly, January 2010), 189-202.

[12] Abdul Ghaffar Korai et al., "Cybercrime, Internet and Cybercrime Legislation: A study of Pakistan", *Psychology and Education* 57: 7 (2020); 118-27.

[13] Michael A. Snssmann, "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", *Duke Journal of Comparative & International Law* 9 (1999); 451-89.

analysis of the challenges faced by the US due to jurisdictional issued faced in computer-related crimes where crimes are committed in a country away from the crime scene and that particular country has no specific legislation declaring the act as crime. The author has also mentioned international cooperation to combat cybercrimes. This article is relevant to the present research and will be very helpful in collection of details about the efforts done by international organizations.

Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation[14] has been written by ***Asad Munir and Ghulam Shabbir.*** The authors have enlisted different categories of cybercrimes and cybercriminals in a brief manner. The cyber laws enacted in Pakistan have also been enlisted along with a discussion Cybercrime Bill, 2015. The article is based on a survey conducted by the authors to estimate the level of knowledge about cybercrimes and cyber laws among youth of Pakistan. The article will be helpful during present research but the authors have not provided detailed description of the cyber laws of Pakistan hence the researcher is aimed to fill this gap and provide detailed analysis of cybercrime legislations in Pakistan.

Developments of Information Technology, Telecom and E-Commerce in Business Environment of Pakistan: An Analysis of Banking and Manufacturing Sectors[15] written by ***Muhammad Shaukat.*** In this article, the author has provided a description about evolution of internet and computer in Pakistan. The use of information technology, E-Commerce and Telecom in banking and industrial sectors of Pakistan

[14] Asad Munir and Ghulam Shabir, "Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation", Global Political Review III: II (Quarterly, Fall 2018), 84-97.

[15] Muhammad Shaukat, "Developments of Information Technology, Telecom and Ecommerce in Business Environment of Pakistan: An Analysis of Banking and Manufacturing Sectors", Pakistan Journal of Social Sciences 29: no 2 (2009); 259-78.

has also been explored. The development of these sectors with the help of latest IT technologies has also been mentioned in detail. The article also provides an analysis of the Government's contributions towards development of information technology in these sectors. This article is relevant to the present research regarding history of computer and internet in Pakistan and will of help in understanding the evolution of computer and its related technology in Pakistan.

Legal Issues

This research aims to find out the cyber laws applicable in Pakistan and the cyber security efforts carried out in Pakistan to save the country and people from cyber threats that are increasing at a fast speed. In this regard, legislations of some other countries have been analyzed to understand their laws and the problems faced to tackle with the cybercrimes in their respective jurisdictions.

The study reveals that cybercrimes are increasing at a faster pace with the development of information technology. The analysis of cybercrimes that have created many problems for the mankind, including hacking, cyber-attacks, viruses and many other related issues, reveal that state laws and records have been breached into by the illegal use of information technology. In addition to this, fraud, spam, hacking and many other unlawful activities have also created serious issues for the law enforcement authorities. Pakistan lags far behind from the developed countries in the formulation of specific legislation to overcome cybercrimes.

Outcome of Research

The research proposes that there is a need of improved, and effective cybercrime laws in Pakistan to deal with the emerging cybercrimes specially to stop the use of cyber space and technology by the terrorists to destroy the peace and stability of the country. A comprehensive legislation can only be made with the consultation of computer experts and legislators hence it is needed that representatives of legal, media and technical fields must be consulted while framing the bill for legislation. Cybercrime laws of developed countries should also be taken into account keeping ion view the problems faced by those countries during formulation of their respective cybercrime policies.

Chapter Breakdown

Introduction provides the objectives of present research with thesis statement, legal questions and literature review of research.

Chapter 1 gives information about meaning and the origin of internet and cybercrimes. It also explains different techniques used to commit cybercrimes. In the end, different categories of cybercrimes have been mentioned.

Chapter 2 provides a detailed description of international and regional legislative attempts to deal with cybercrimes. Detailed analysis of legal framework of international bodies and organizations regarding cybercrimes has been mentioned. The cybercrime laws of the United States of America and the United Kingdom have been mentioned in detail.

Chapter 3 explains the role of international law enforcement bodies to prevent cybercrimes along with the strategies applied by these bodies to control cybercrimes. The challenges faced by the international community during this process are also discussed in detail.

Chapter 4 deals with the cybercrime laws of Pakistan. After a brief description of cybercrime laws of India and Bangladesh, the cybercrime laws of Pakistan are discussed in detail. The efforts of Pakistan to deal with cybercrimes and the problems faced during such process are discussed in detail.

CHAPTER 1

History and Nature of Cybercrimes

1.1 Introduction

The origin of cybercrimes has its roots with the invention of computer, used in the commission of cybercrimes and invention of internet has provided a new way to commit such crimes in more developed ways. Cybercrimes cannot be completely understood without having basic information about the evolution of the phenomenon along with the different techniques used to commit cybercrimes. Preset chapter provides information about the nature and history of cybercrimes. In addition to this, the techniques used to commit cybercrimes have been explained with an analysis of the different categories of cybercrimes.

1.2 History of Cybercrimes

The practical application of cybercrimes dates back to 1960's with the invention of internet[16] and its further advancements like Advance Research Projects Agency Network (ARPANET),[17] Transmission Control Protocol/Internet Protocol (TCP/IP protocols)[18] and the world wide web (www)[19] in the coming years.[20] ARPANET is

[16] Zia ul Islam, Muhammad Aqeel Khan, and Muhammad Zubair, "Cybercrime and Pakistan", *Global Political Review* IV: no II (Quarterly, 2019); 12, accessed 16 February, 2022. URL: http://dx.doi.org/10.31703/gpr.2019 (IV-II).02

[17] It is the Initial version of internet with the basic purpose of linking computers at Pentagonfunded research institutions over telephone lines. Janet Abbate, *Inventing the Internet* (Cambridge: Massachusetts Institute of Technology, 1999), 37.

[18] These are sets of communication rules used to communicate the network devices on the internet. Andrew G. Blank, *TCP/IP Jumpstart: Internet Protocol Basics* (San Francisco: Sybex, 2002), 1-no 2.

[19] It is a software system that allows sharing of information and other documents through the internet. "World-Wide-Web", *Britannica,* Accessed 18 March, 2022. https://www.britannica.com/topic/World-Wide-Web

[20] Paolo Bory, The Internet Myth: From the Internet Imaginary to Network Ideologies (London: University of Westminster Press, 2020), 8.

closely connected to the origin of cybercrimes as the security provided by this project was breached by a group of IT experts called Phreakers who managed to break into the telecommunication system and discovered ways to make free calls and conducted credit theft thus giving rise to a new term hacking.[21] The computer virus was also seen and experienced for the first time in ARPANET. The virus was called 'Creeper Virus' and appeared for a short while on the screen.[22] In 1973, the first organized cybercrime was detected when money from a company was stolen by the chief teller of the Savings Bank through manipulation of the account data in the computer system of the bank.[23]

Another notable incident of cybercrimes in the US is the hacking of almost sixty computer systems in 1983 by a group of six boys who called themselves as '414.' Frequent use of system by the boys helped in being tracked by the Federal Bureau of Investigation[24] (FBI). The use of computers increased with the passage of time as use of personal computers also started since 1990 providing wider area for the hackers to perform their illegal activities. People were unaware of system protection techniques so ratio of cybercrimes increased rapidly. In 1994, the longest prison sentence of 51 months was given to a cybercriminal named Kevin Poulson also called as Dark Dante, who was involved in fraud through computer and mail, wiretapping and money laundering.[27] Cybercrimes have now crossed borders and security of modern technology has been breached by the cybercriminals causing huge monetary

[21] Islam, Khan and Zubair, "Cybercrime", 13.

[22] Michael Gervais, "Cyber Attacks and the Laws of War", *Journal of Law & Cyber Warfare* 1: no.1 (Biannual, 2012), 15.

[23] Hill and Marion, *Introduction to Cybercrime*, 29.

[24] Primary investigation agency of the US. Government. Athan G. Theoharis, "A Brief History of the FBI's Role and Powers", in *The FBI: A Comprehensive Guide*, ed. Athan G. Theoharis et al., (Arizona: Oryx Press, 1999), 2.

and confidentiality loss. In 2009, a huge amount of money was extracted from First Federal Savings Bank, Kentucky. Investigations revealed that the account was operated from Ukraine, a country known as a base of the cybercriminals.[25]

1.3 The Nature and Definition of Cybercrimes

Cybercrime as a distinct criminal activity is associated with illegal and illicit use of cyberspace for unauthorized personal gain.[26] In other words, it is the combination of crime and cyberspace.[27] Some other terminologies like computer crime, e-crime and high-tech crime have also been used for cybercrime.[28] Modern states have amalgamated all the terminologies including all computer related offences to fall within the category of cybercrimes.[29]

Cybercrimes have been defined for the first time by Donn Parker.[30] According to Parker, the term can be described as any intentional act related to a computer resulting in loss or expected loss of the victim and gain or expected gain of the perpetrator.[31] This definition has been further expanded by Robert Taylor[32] when he classified the computer related crimes into four categories based on the style in which a computer is used in a particular crime. These categories include use of computer as a main tool; use as a target; computer is related indirectly to the crime and lastly

[25] Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes (*Boston: North Eastern University Press, 2012),6-no.7.

[26] Arief, Adzmi and Gross, "Understanding Cybercrime", 71.

[27] Ibid.

[28] Jonathan Clough, *Principles of Cybercrime,* 2nd ed. (Cambridge: Cambridge University Press, 2015), 9-10.

[29] Robert, "Attempting", 3-4.

[30] Well renowned researcher and expert on computer security and cybercrimes. James S. Tiller, *A Technical Guide to IPSec Virtual Private Networks* (Boca Raton: CRC Press, 2001), 10.

[31] Robert, "Attempting", 4.

[32] Professor in Department of Criminology and Criminal Justice at the University of Texas at Dallas. "RW Taylor", *UT Dallas,* accessed 25 March, 2022. https://profiles.utdallas.edu/rwtaylor

dominance of computer in commission of a crime. So Taylor has tried to explain and simplify Parker's definition that incorporated all kinds of computer related activities resulting in gain of one and loss of another within the ambit of cybercrimes.[33] Taylor has further explained and classified these activities making it easier for future penal legislation for cybercrimes.

Cybercrimes have been defined by Sarah Gordon [34]and Richard For [35]in an article written by them. According to them cybercrime is a crime committed by using a computer network or any hardware device[36]. They state that cybercrime can be classified into two categories on the basis of style of using computer and its related technologies. First category includes use of computer as a crime ware by the introduction of virus or any other infected program like for instance, data theft through hacking or identity theft. The second category includes the indirect use of computer in achieving the criminal objectives like harassment and blackmailing[37]. Another definition of cybercrimes has been provided by Kapersky [38]as an illegal act in which either a computer or a network device is used or targeted. Prashant Mali[39] has defined cybercrimes in a comprehensive way as a general terminology applicable to all kinds

[33] Robert, "Attempting", 4.

[34] A computer security researcher and adept in antivirus technologies. Roger A. Grimes, Malicious Mobile Code: Virus Protection for windows (Sebastopol: O Reilly Media. (2001), 15.

[35] Chief Scientist at Force Point and also worked as Head of Computer science and cybersecurity department at Florida Institute of Technology, "Dr. Richard Ford", Force point accessed 20 March, 2022. http://www.forcepoint.com/de/company/biographies/dr-richard-ford-0

[36] Sarah Gordon and Richard Ford, "On The Definition and Classification of Cybercrime", Journal in Computer Virology 2 (Quarterly, 2006), 14, accessed 10 March, 2022.

[37] Ibid

[38] Eugene Kaspersky is a world renowned Russian Cybersecurity Expert and Chief Executive Officer of Kaspersky Lan, an IT security company, accessed 21 March 2022.

[39] An advocate and thought leader having research experience of twenty years in the field of IT security and legal matter related to cyber laws. He has also written several books on cybercrimes and cyber laws, accessed 22 March, 2022. http://www.prashantmali.com/

of criminal activities conducted by the use of computers, internet, cyberspace or the world wide web.[40]

Apart from the above mentioned definitions by scholars, cybercrimes have been defined at international level for the first time in 1990 by the Eighth UN's Congress on the Prevention of Crime and the Treatment of Offenders. [41] [40] Cybercrimes mentioned as computer-related crimes have been categorized into five classes by the Manual on the Prevention and Control Of computer-Related Crime published in 1994 by UN.[42] It states that computer-related crimes include:

a) Fraud conducted through computer;

b) Forgery conducted through alteration of documents stored on computer;

c) Alteration of computer data or program;

d) Illegal approach to a computer network; and

e) Illegal replication of computer programs. [43]

The UN's Manual is of great significance as an international level document but the Council of Europe's Convention on Cybercrime entered into in 2001 is the leading multilateral binding document in this regard.[44] The Convention classified cybercrimes into four categories incorporating new offences within the ambit of cybercrimes. These categories are:

[40] Ibid

[41] Aleš Završnik, "Cybercrime Definitional Challenges and Criminological Particularities", Masaryk University Journal of Law and Technology 2: 2 (Biannual, 2008), 07.

[42] UN Centre for Social Development and Control of Computer-Related Crime. International Review of Criminal Policy. No. 43-44. New York: UN, 1994. "Record", *Digital library.un*, accessed

[43] Ibid

[44] Jonathan Clough. "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation", Monash University Law Review 40: 3 (Tri-annual, 2014), 699-700, accessed 30 March, 2022. https://ssrn.com/abstract=2615789

a) Crimes in which privacy of computer system and its data is attacked and put in danger;

b) Crimes conducted through the use of computer like fraud;

c) Crimes in which the offence is conducted through content placed on computer or internet like child pornography; and

d) Crimes which violate copyright and other related rights.[45]

New sophisticated cybercrimes, for instance money laundering, crimes conducted by the use of virtual currencies, theft of identity and use of illegal content and its storage, have evolved with the passage of time whereas the Convention does not include these newly developed cybercrimes.[46] There is a need that the term 'cybercrimes' should be defined in a broader perspective. Profesor Nir Kshetri[47] has stated that cybercrimes include motivation to the criminal in terms of cost and gain and for that purpose the criminal uses computer networks.[48] While defining cybercrimes, Professor Kshetri has also given certain examples of cybercrimes like online fraud, money laundering, and identity theft.[49] Susan Brenner[50] has provided another categorization of cybercrimes. Brenner has categorized cybercrimes into three classes as:

a) Use of computer as a tool to commit a crime like online fraud;

[45] "Council of Europe (Coe): Convention on Cybercrime", *International Legal Materials* 41: no 2 (Monthly, 2002), 284, accessed 24 March, 2022. doi:10.1017/S0020782900009918

[46] Sheshtak Viktor and Koscheeva Darya, "Cyber Crime during the COVID-19 Pandemic: Key Trends and Ways to Solve the Problem", *Moscow: Institute of Legislation and Comparative Law* (October 20, 2021), 2-3, accessed 18 March, 2022. https://ssrn.com/abstract-3957903.

[47] Associate Professor at the University of North Carolina and has also written books on cybercrimes. Nir Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (Heidelberg: Springer Publishing, 2010), xvii.

[48] Nir Kshetri, "The Simple Economics of Cybercrimes", *IEEE Security and Privacy* 4: no 1 (Bimonthly, January/February, 2006), 33-34.

[49] Kshetri, *The Global*, 3.

[50] She is a Professor of Law and Technology at the University of Dayton, Ohio. Susan W. Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships", *North Carolina Journal of Law & Technology* 4:no 1 (2002), 1. Brenner, *Cybercrime and the Law*, 14.

b) Use of computer as a target, for instance, hacking; and

c) Use of computer as a secondary tool in the commission of a crime, for instance, monitoring sales and profits of illegal drugs by storing data on computer.[51]

Another authentic and comprehensive definition of cybercrimes was presented by the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders.[52] It defines cybercrimes as crimes that can be committed using a computer system or network, within a computer system or network or against a computer system or network. [53]

Preceding discussion makes it clear that both the terminologies 'computer crimes' and 'cybercrimes' have been used interchangeably as all those illegal activities which are conducted through the aid of digital means and the main role is played by information technology in the whole process. [54] It can be concluded that cybercrimes are termed as crimes in which the information technology and computer used as a tool to commit the crime. The topic of cybercrimes cannot be completely understood with just definitions and history; it is also important to discuss the techniques that are used to commit different kinds of cybercrimes.

1.4 Different Techniques Used to Commit Cybercrimes

The need to understand different methods used to commit cybercrimes is necessary due to lack of knowledge regarding this particular category of crimes. Mostly general people and even the police officials do not have the exact information about all the

[51] Brenner, Cybercrime and the law, 14.

[52]The Resolution has been adopted by General Assembly on 17 December, 1999 while report was presented on 10-17 April, 2000. "Record", *Digital library.un,* accessed 28 March, 2022. https://digitallibrary.un.org/record/404748?ln=n

[53] Ibid

[54] Yar and Steinmetz, *Cybercrime and Society*, 9.

techniques used to commit cybercrimes and may mix them with ordinary crimes.[55] An in-depth analysis of the methods applied by cybercriminals to commit illegal acts can guide the law enforcement agencies, lawyers and legislature to understand the phenomenon applied by cybercriminals and in making and applying correct laws to stop cybercrimes.

1.4.1 Spoofing

Spoofing refers to making of a fake but almost similar website or email id of a company or a bank which directs the users to use their emails and passwords after which this information is hacked and loss is incurred to the users.[56] Another style in which spoofing can occur is the redirection of the users to another website which contain explicit material. Spoofing can also occur by hacking the website and then defacing it. Defacement of websites is the most common and popular style of spoofing and many famous companies including internet companies have been targeted by the offenders.[57] The advancements in technology and lack of regulations have made it very easier to make counterfeit/fake emails as Simple Mail Transfer

Protocol (SMTP)[58] provides no authentication procedure for emails.[59]

1.4.2 Phishing

Phishing can be explained as an ordinary kind of fraud committed through online resources.[60] It can also be referred as stealing personal information of the bank

[55] Michael Cross, *Scene of the Cybercrime*, 2nd ed. (Burlington: Syngress Publishing, 2008),

[56] Ido Dubrawsky, *how to Cheat at Securing Your Network* (Burlington: Syngress Publishing, 2007), 180.

[57] Yar, *Cybercrime*, 29-30.

[58] The technical standards or mechanism followed while transmission of emails making email delivery possible. Hossein Bidgoli, *Handbook of Information Security*, vol. 1 (New Jersey: John Wiley & Sons, 2006), 878.

[59] Mishra, *An Overview*, 17.

[60] Steven Myers, "Introduction to Phishing",in *Phishing and Countermeasures*, ed. Markus Jakobsson and Steven Myers (New Jersey: Wiley Publishing, 2007), 1.

customers and their official accounts through using online resources. The term 'phishing' was used for the first time in 1996 when accounts of American Online (AOL)[61] were stolen by false procurement of passwords. In this category of cybercrimes, the offenders pose themselves as legal companies and obtain personal information from the customers. After obtaining the required personal data, the offenders log into the bank accounts and steal the amount.[62] Bank frauds are committed by posing to be the representative of bank while phishing occurs by forming such sites that look legal and then information is collected when the victim logs into the site or fills the given form and enters his/her personal info. The offenders get access to the victim's accounts without letting him know that a fraud has been committed.[63]

1.5.3 Hacking

Hacking can be defined as accessing someone's computer without any permission or authority.[64] This unauthorized access to computer is considered a cybercrime because it falls within one of the categories of cybercrimes as expounded by computer experts like Taylor. There may be a possibility that computer is used as a tool to commit crime, computer is the main target in the crime, computer is used indirectly in the commission of a crime or computer is the dominant factor in a particular crime. Hacking as a criminal activity may cause alteration or destruction of the computer system or related

[61] It is one of the largest internet service provider companies in the US. "AOL", *Britannica*, accessed 27 March, 2022. https://www.britannica.com/topic/AOL

[62] Fawzia Cassim, "Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing?" *The Comparative and International Law Journal of Southern Africa* 47: 3 (Tri-annual, 2014), 403-404.

[63] Er. Navneet Kaur, "Introduction of Cybercrime and Its Types", *International Research Journal of Computer Science* 8:no 5 (Monthly, August 2018), 437, accessed 15 April, 2022. ISSN: 2393-

[64] Robert Moore, *Cybercrime: Investigating High-Technology Computer Crime,* 2nd ed. (Oxon: Routledge, 2015), 3.

data or it may cause huge damage to the computer systems through the internet.[65] In the US, hacking was declared an offence under the Computer Fraud and Abuse Act, 1984. [66] Although hacking is the oldest technique, it is still used to hack the websites or the smart phones even with sending a missed call as done by Pegasus Spyware.

Initially the term was used in a positive sense for those who invented new things in the computer world but with the passage of time, the term was misunderstood and mixed with 'crackers'[67] and people used to employ the terminology for those who were involved in illegal activities.[68] It can be classified as simple hacking and aggravated hacking. When a person logs into a computer without any authority or permission but makes no changes or causes no damage thereto, the act of such illegal access is termed as simple hacking.[69] Simple hacking can be conducted by the teenagers who do it just for fun or to prove themselves in front of their friends.[70] Causing damage to a computer system after illegal access to a computer falls within the category of aggravated hacking and is more serious offence than simple hacking.[71] Some offences that are committed by hackers are: theft of confidential information related to state or private businesses, destruction or damage to computer systems, and spoofing.[76]

[65] Majid Yar, *Cybercrime and Society* (London: Sage Publications, 2013), 30-31.
[66] Brenner, *Cybercrime and the Law,* 23-24.
[67] The actual term used for the one who is involved in criminal activities through misuse of someone else's computer. Jon Erickson, *Hacking: The Art of Exploitation,* 2nd ed. (San Francisco: No Starch Press, 2008), 3.
[68] Majid Yar,*Cybercrime.* 2nd ed. (London: Sage Publications, 2013), 22-23; Cross, *Scene,* 44.
[69] Muhammad Masum Billah, "Sufficiency of Omani Laws to Suppress Cybercrimes in Light of the UN Comprehensive Study on Cybercrimes", *Arab Law Quarterly* 32: 2 (Quarterly, 2018), 167.
[70] Cross, *Scene,* 19.
[71] Billah, "Sufficiency of Omani", 167. [76]
Yar, *Cybercrime,* 29-30.

1.6.4 Computer Malware

Computer malware is a combination of computer viruses and computer worms.[72] Computer viruses are infectious software programs that can spread from one computer to another and disturb the computer operations.[78] Computer worms not only effect the host computer to spread, they can also spread through network affecting the computers linked to that particular network. A computer malware can cause computer infection, mismanagement or stealing of data or information resulting in causing a loss.[73] Computer malware can be termed as an advanced form of hacking with the difference that sometimes the virus or worm does not grant access to the offender rather it just destroys computer data.[80] The initial version of computer malware appeared in ARPANET as programs began self-replicating. The first computer virus is called "the Creeper Virus".[74] It appeared for a short while in the form of a message on the computer which caused billions.[75]

The computer viruses can also be spread by political or terrorists groups to achieve their goals or propagate their massage to the world or to cause serious damage to a state or organization.[76] When such acts are done by terrorist groups, the offence shall fall within the category of cyber terrorism which means use of the cyber technology for terrorist activities.

[72] Billah, "Sufficiency of Omani", 169. [78]
Mali, *Text Book*, 49.
[73] Billah, "Sufficiency of Omani", 169. [80]Ibid,
167-168.
[74] Hill and Marion, *Introduction to Cybercrime*, 29.
[75] Gabriel Weimann, "Cyberterrorism How Real Is the Threat? Special Report", 5, accessed 13 May, 2022. https://usip.org/sites/default/files/sr119.pdf.
[76] Ibid.

1.7.4 Spam/Unsolicited Emails

This category of cybercrimes includes the act of sending emails for selling products, spreading malware or identity theft. The advertisement of products through emails is not an illegal act but unwanted emails can cause wastage of time and money of the receiver.[77] It is estimated that about 80% spam emails are sent through virus infected computer systems or botnets.[78] The targeted email addresses are mostly collected through websites, chat groups, newsgroups, and viruses that harvest customers' address books.[79] The collected addresses are then sold to the spammers who use it to fulfill their required targets.[80] A study conducted in the US revealed that spam caused loss of US$ 8.9 billion in the year 2002.[81] Unsolicited emails can also be a way of infecting computer systems by spreading malware or stealing sensitive information.[82]

1.8.4 E-Mail Bombardment

Another important technique employed by the offenders to damage the victims is email bombardment. It can be denoted as an attack of sending massive number of emails to a particular user or a system causing the system or user's account to jam most of the time resulting in huge loss to the system.[83] Sometimes the hackers automatically subscribe victim's email to a huge list of sites that send bulk emails

[77] Billah, "Sufficiency of Omani", 171-72.

[78] Akash Kamal Mishra, *An Overview of Cybercrime and Society,* vol. 1 (Chennai: Xpress Publishing, 2017), 18.

[79] Amir Manzoor, *E-Commerce: An Introduction* (Saarbrücken: LAP Lamburt Academic Publishers, 2010), 82.

[80] Mishra, *An Overview*, 18.

[81] Alan Davidson, *The Law of Electronic Commerce* (New York: Cambridge University Press, 2009), 284.

[82] Billah, "Sufficiency of Omani", 171-72.

[83] Cross, *Scene,* 493.

causing the id to jam.[84] Denial of Service attacks can also be the result of such email bombardment.

1.9.4 Identity Theft

Stealing any other person's sensitive information and causing damages thereafter falls within the definition of identity theft which is an old crime that prevailed even before the advent of internet. This crime has become easier with the advancement in technology. Cybercriminals present themselves as bank representatives or government officials and send emails or messages forcing the people to share their personal financial information thus causing huge damages to the victims.[85] Such loss can be in the form of loss of credit or the offender can get medical and other kinds of legal benefits allowed to the victims[86] but most of the time bank frauds occur by this method.

1.10.4 Facebook Tracking

Facebook predation or Facebook tracking is another technique applied by the offenders to steal anyone's identity or to harass someone. The advancements in technology and innovation of social websites have increased the risk of illegal and dishonest use of personal identities to defame or damage anyone. Passwords can be easily hacked from these social linking sites paving way for the offenders to cause damage.[87]

[84] Ibid, 494.

[85] Billah, "Sufficiency of Omani", 75-76.

[86] "Identity Theft," *USA.gov*, accessed 08 February, 2022, https://www.usa.gov/identity-theft

[87] Barry Sandywell, "On the Globalisation of Crime: The Internet and New Criminality", in *Handbook of Internet Crime,* ed. Yvonne Jewkes and Majid Yar, 2nd ed. (New York: Routledge, 2011), 48.

The application of above mentioned techniques does not always require the use of internet and sometimes the act can cause damage by using computer alone like for instance, distortion of computer data or stealing confidential information. These methods can, whether applied solely or combined with other methods, create many problems or crimes to be described in the coming section. In the similar way, an act of hacking a website may lead to large scale system jam causing great economic loss or same act of hacking can be applied by the terrorists to get their demands fulfilled along with same act of hacking can be used the political activists to propagate their cause to the world causing no physical damage. In other words, use of even one single technique can be a way of committing several numbers of cybercrimes.

1.5 Different Categories of Cybercrimes

Cybercrimes, when conducted by the use of internet, are mostly managed by Dark web that is an enormous collection of websites where anonymity tools are used to carry out the work. In addition to this, Dark web also ensure anonymity thus providing ease to the criminals to carry out their activities without any fear of being detected. Dark web is most commonly used to carry out various illegal activities including sale of illegal goods like weapons and drugs and also for child pornography. [88] Cybercrimes are increasing at a faster pace and many counties of the world are cooperating with each other to deal with the issue.[89] It is vital to discuss the different categories of cybercrimes that have emerged due to illegal use of the modern communication technology. This section deals with a detailed discussion of illegal

[88] "Global Program on Cybercrime", *UNODC,* accessed 15 January, 2022. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

[89] Jobel Kyle P. Vecino, "United by Necessity: Conditions for Institutional Cooperation against Cybercrime", *The Cyber Defense Review* (Quarterly, Special Edition 2019), 123.

acts committed by the application of any or all of the previously mentioned techniques.

1.5.1 Cyber Terrorism

Terrorists use internet and its allied components in the same way as normal people use it.[90] Although terrorists can carry out their activities through hacking of computer system or data, virus attacks or denial of service attacks but these methods are of less importance to the terrorists as their basic motive is to create anarchy in the physical world so they use internet as a supporting tool to achieve their target. They make plans, raise funds for their organizations or propagate their cause on the internet.[91] An important incident of the use of internet in terrorist activities is the use of e-mail by the terrorists for coordinating their activities for the preparation of 9/11 attack in the US.[92] London Tube Bombings in 2005 is also another important instance of the use of advanced information technology for the terrorist activities.[93]

1.5.2 Hacktivism

The term 'hacktivism' need not to be confused with the term 'hacking'. The hackers do not have any political agenda rather they hack the computers through different ways in order to gain economic benefits. Hacktivism means hacking of a computer system by political activist groups in order to propagate their message to the world.[94] The recognition of hacktivism as an offence depends on the political agenda forwarded. For instance, promotion of western philosophy and propagation of the

[90] Javier Argomaniz, "European Union Responses to Terrorist Use of the Internet", *Cooperation and Conflict* 50: 2 (Quarterly, 2015), 251.

[91] Julie E. Mehan, *Cyber War, Cyber Terror, Cybercrime and Cyber Activism*, 2nd ed. (Cambridgeshire: IT Governance Publishing, 2014), 55.

[92] Argomaniz, "European Union", 252.

[93] Sandywell, "On the Globalisation", 53.

[94] Yar, *Cybercrime and Society*, 45.

political agenda that resulted in rebellions in Tunisia and Egypt are welcomed by the West and not declared an offence but when some Islamic organization promotes its ideologies, they are declared a danger to Western domination[95] and declared as information terrorists.[96]

Hacktivism should not also be confused with cyber terrorism as both have difference of targets and goals. Terrorists' basic goal is to create anarchy and disturbance in the society while hacktivists' basic goal is to achieve their political agenda without disturbing the society in a peaceful way. But the line of distinction between both activities is not very clear because when terrorists enter in some political parties and create disturbance in peaceful agitation activities, the situation becomes very difficult. Hacktivism can be carried through different ways including email attacks, web jacking, or through computer malware as well.[97]

1.5.3 Web-Jacking

Web jacking signifies getting hold of a website through force with the purpose of satisfying political or financial goals. These aims are satisfied from the website's owner as ransom to free the website.[105] This sort of web jacking is done through different ways like for instance, e-mail bombarding or swarming. Swarming refers to collapsing a system by simultaneous access of that particular site by a huge number of people. E-mail bombarding can also jam a website as happened in July 1997 against Institute of Global Communications (IGC). The system was blocked by sending huge number of emails at one time. They demanded removal of certain websites from the network of IGC and as a consequence of not fulfilling the demand, the web-jackers

[95] Ibid, 46.

[96] Ibid, 45.

[97] Weimann, "Cyberterrorism", 4-5. [105] Mali, *A Text Book,* 59.

threatened to clog remaining system of IGC as well. Their demands were fulfilled after few days.[98]

1.5.4 Cryptocurrency Fraud

Cryptocurrency also called as virtual currency is the virtual form of real money convertible into real currency. These currencies are of many kinds including Bitcoin, Etheruem and Litecoins. Among these Bitcoin is the most popular and commonly used cryptocurrency. Mostly the cryptocurrencies are not regulated by the state governments so they are ways of tax evasion with the chances of these amounts to be used by the terrorists.[99] The system of cryptocurrencies is mostly based on blockchain system ensuring anonymity thus having the chances of fraud. Many instances of frauds conducted through cryptocurrencies especially bitcoin have been experienced throughout the world in the recent years.[100]

In a report issued by Cypher Trace, a US based Block chain forensic company, stated that about $480 million loss has been reported at different incidents of cryptocurrency scams worldwide. Of these, Japan's BIT Point exchange faced a hack of $30 million.[101] Pakistan has also faced a Bitcoin scam in 2021 to be discussed in detail under the head of Pakistan. The increasing rate of people's involvement in cryptocurrency trading and the huge losses incurred as reported by the Cypher Trace report has created an alarm for the international community and the states are try to regulate and monitor the use of cryptocurrencies either by banning or regulating them.

[98] Weimann, "Cyberterrorism", 4-5.

[99] Ayesha Afzal and Aiman Asif, "Cryptocurrencies, Blockchain and Regulation: An Overview", *The Lahore Journal of Economics* 24: 1 (Biannual, Summer 2019), 104-5.

[100] Ibid, 112-113.

[101] CypherTrace, *Cryptocurrency Anti-Money Laundering Report, 2019 Q2*(Los Gatos: CypherTrace, July 2019), 13, accessed 28 September, 2022. https://ciphertrace.com/wpcontent/uploads/2019/08/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q2-1.pdf

1.5.5 Bank Fraud

Bank fraud is a kind of white collar crime that can be committed internally by the bank employees in the form of wrong electronic transfer of funds for their personal benefits or it can be committed by third persons in the form of defrauding the account holders thus inducing them to disclose their identity or transfer funds to such persons.[102] Several online forums are also available on the internet that deal in sharing stolen credit cards, bank details and other technology for receiving the required information. An important instance is the forum "Dark Market" which deals in providing the technology to be used in bank fraud and also transacted in stolen credit cards and shared stolen bank details of people.[103]

1.5.6 Child Pornography

Child pornography is the heinous form of cybercrime offences committed through internet as it sabotages the innocence of the child and results in grave emotional and psychosomatic issues for the child.[104] It has become easier to perform these activities with the aid of software, to perform mixing and editing of images even on an inexpensive computer system.[105] Child pornography is one of the largest profit earning industries of the world[106] and committed in a very organized manner mostly by formation of groups for sharing such material. Child pornography is declared as a violation of the rights of children under the UN Convention on the Rights of the Child

[102] Joseph J. Norton and George A. Walker, ed., *Banks: Fraud and Crime*, 2nd ed. (Oxon: Routledge, 2000), 1.
[103] Peter Grabosky. "The Evolution of Cybercrime, 2004-2014", *RegNet Research Paper* 58(2014), 6, accessed 05 May, 2022. https://dx.doi.org/10.2139/ssrn.2535605
[104] Sarah Sternberg, "The Child Pornography Prevention Act of 1996 and the First Amendment: Virtual Antitheses", *Fordham Law Review* 69: 6 (Bimonthly, 2001), 2785.
[105] Ibid, 2788.
[106] Ibid, 2787.

(CRC). Most of the countries declare child pornography as a punishable offence either under their state laws or have criminalized it under the cybercrime laws.[107]

1.5.7 Cyber Defamation and Harassment

With the progress and development of information technology, the criminals are also using the advanced technology to achieve their criminal objectives.[108] Today, it has become very easy to defame any person or organization by using internet. The victim's internet account is hacked and emails are sent from that account to the victim's contact emails and other unknown email addresses as well. The emails contain vulgar language or they can also contain some information which can degrade the image of the victim.[109] The Internet is also used to harass or create anger in an individual or a group of persons. Messages, images or other related contents are sent to the victim either to harass him or to annoy that person so that he may get depressed or angry.[110]

1.5.8 Denial of Service Attacks

When provision or access to internet services is made inaccessible by some illegal sources, such problem is termed as denial of service attacks.[111] Reason of such denial could be computer bugs, poor coding or unintentional errors sharing gigabytes memory resulting in crashing the entire computer system.[112] Spam emails or email bombardment can also be a cause of such denial of service attacks as the system is flooded by impracticable traffic signals causing the system to jam initiating denial of

[107] Billah, "Sufficiency of Omani", 173.
[108] Yar and Steinmetz, *Cybercrime and Society*, 4.
[109] Kaur, "Introduction", 437.
[110] Ibid.
[111] Billah, "Sufficiency of Omani", 170.
[112] H. L. Armstrong, "Denial of Service and Protection of Critical Infrastructure", *Journal of Information Warfare* 1: 2 (Quarterly, 2001), 24.

such services to their related users.[113] An important instance of such denial of service attack happened in February 2000 when important websites of Yahoo were bombarded with enormous request making it impossible for the sites to respond thus causing a jam in the system causing a loss of US$ 1.2 billion.[114] It is very difficult to locate the prime source of denial of service attacks as anonymity is guaranteed by fake IP addresses.[115] Cyber-attacks are sometimes conducted at governmental level as well, for instance, launch of cyber-attacks on the government servers in Estonia with possible support from Russia.[116]

1.5.9 Digital Piracy

Advanced technology has not only made our lives easier along with it has provided us the ease to access and download any sort of media files. There are many websites through which these copyrighted files or programs can be accessed without any payment. This provision of copyrighted files without permission from the actual copyright holder is an offence termed as digital piracy.[117] Such pirated content can be any reading material or a program or a movie.[118] It has become very easy for the pirates to conduct piracy with the use of internet without the fear of being identified by the real author or the law enforcement agencies.[119] Digital piracy has affected the copyright holders' in terms of monetary loss incurred due to the sharing of pirated content. In 2013, International Federation of Phonographic Industry (IFPI) stated that

[113] Mishra, *An Overview*, 11.
[114] Armstrong, "Denial of Service", 24.
[115] Ibid, 30.
[116] Grabosky, "The Evolution", 7.
[117] Susan Meyer, *Understanding Digital Piracy* (New York: Rosen Publishing, 2014), 4.
[118] Ibid, 7.
[119] Sandywell, "On the Globalisation", 49-50.

their sales have been heavily affected by unpaid access of one third internet users to the pirated contents.[120]

1.5.10 Conducting Illegal Business

Internet has made it easier for the offenders to conduct illegal businesses at international level. The sale and purchase of illegal drugs and banned medicines is an important instance of such crimes. Although medicines are being sold by different authorized companies through doctor's prescription but the illegal pharmaceutical business has incurred a great loss as they sell medicines without any prescription and they also sell those medicines that are banned to be sold. Along with pharmacies, internet has become an easy hub for the sale of narcotics and drugs as the element of 'anonymity' has made it easier to conduct such business without any fear. An important instance is an illegal online pharmacy based in Oklahoma that was closed down in 2001 with the cooperation of federal and local authorities of the US.[121]

1.6 Conclusion

Cybercrimes are the result of developments of information technology beginning with the invention of computer and internet. There is no comprehensive and settled definition of the terminology due to the background referred by different authors and the way they understand the terminology according to their own perspective. Efforts at national and international level are in progress to handle cybercrimes to be discussed in coming chapters. Cybercrimes are committed by employing different techniques that can be applied solely to cause damage or they can be mixed with each other to commit a crime. It is not necessary that a single technique leads to a particular

[120] Frances P. Bernat and David Makin, "Cybercrime Theory and Discerning if There is a Crime: The Case of Digital Piracy", *International Review of Modern Sociology* 40: 2 (Biannual, 2014), 102.

[121] Cross, *Scene,* 25-26.

category of crime besides a single technique can be used to perform one or more crimes. In other words, one technique may lead to achievement of multiple illicit objectives. It need to understand the techniques applied to commit cybercrimes in order to make comprehensive laws for controlling cybercrimes at national and international level.

CHAPTER 2

International Legislative Framework on Cybercrimes

2.1 Introduction

International law is rapidly changing with the development of technology, invention of modern communication devices and emergence of new domains of international criminal law. International criminal law is developing to control new sophisticated crimes conducted with the aid of advanced technology.[122] It is estimated that these sophisticated crimes, termed as cybercrimes or computer-crimes, will cause a loss of approximately US$6 billion per year through 2021.[123] Cybercrimes are mostly of transnational nature so international cooperation is a necessity for effective law making regarding such crime.[124] Capabilities of the states also differ and multinational cooperation can be more effective to mitigate cybercrimes rather than dealing with the issue at individual level.[125] An important instance of cooperation at international level is the formation of institutions like Europol to be discussed in detail in the coming sections.

This chapter deals with the cybercrimes legislation at international and regional level. The efforts of different counties and organizations have also been analyzed and discussed in detail in the forthcoming discussion. In the present discussion, international legislations have been discussed first and then regional approaches to tackle with the problem have been analyzed in detail. Lastly, legislative attempts carried out by different countries have also been discussed. The chapter

[122] Judge Marilyn J. Kaman et al., "International Criminal Law", *The International Lawyer*41: 2 (Quarterly, Summer 2007), 324.

[123] Vecino, "United by Necessity", 123.

[124] Clough, "A World of Difference", 700.

[125] Vecino, "United by Necessity", 123

concludes with the result that cybercrimes are tried to be dealt in a serious manner by all the countries.

2.2 International and Regional Legislations

The transnational nature of cybercrimes has made it problematic for the states to deal with the cybercrimes. Many attempts have been done to make comprehensive laws at the international level by holding Conventions and creating institutions yet no comprehensive law, to be followed by all states without any prejudice, has been made. The reason for such lack of consensus is the desire of every state to have its own laws being protected and its own ideologies being implemented within their states. [126] Global and regional legislation against cybercrimes has been categorized into five classes by the United Nations Office on Drugs and Crime (UNDOC). [127] The categorization by UNDOC is as under:

i. Legislations which have been created in perspective of the Convention, for instance, Commonwealth Model Law on Computer and Computer Related Crime;

ii. Legislations carried out by the Commonwealth of Independent States (CIS);

iii. Laws proposed by the Arab countries in the League of Arab States' Arab Convention on Combatting Information Technology Offences and other associated laws; iv. Laws proposed by African countries comprise fourth category of legislations. This category includes the Draft African Convention on the Establishment of a Legal Framework; and

[126] Clough, *Principles*, 23-24.

[127] Clough, "A World of Difference", 730.

v. The last but most important legislative efforts are the UN instruments.[128] In the absence of UN's Convention, cybercrimes are dealt under the UN's Convention against Transnational Organized Crime (UNTOC)[129] that covers and deals with crimes of serious and transnational nature.[130]

Along with the discussion on legislative efforts at different levels, it is vital to discuss holding of conferences and Conventions as legislations are always the result of these conferences.

2.2.1 Conference on Criminological Aspects of Economic Crime, 1976

The first and foremost step taken in the Europe to curtail cybercrimes was the Council of Europe's Conference on Criminological Aspects of Economic Crime in 1976. The Conference was the first initiative on international level that discussed different categories of cybercrimes, like phreaking, emerging due to developments in the information and communication technology. As an outcome of the Conference, a committee of experts was appointed in 1985 by the Council of Europe to analyze cybercrimes and provide a guideline for national legislatures in order to make laws dealing with the issue of cybercrimes. The committee presented its recommendations in 1989 and based on these recommendations, a series of regulations concerning cybercrimes was initiated by the Council of Europe in 1995.[131]

[128] Clough, "A World of Difference", 730-731.

[129] "Catalogue of Cases UN Doc", *UNODC*, accessed 25 January, 2022. https://www.unodc.org/documents/treaties/organized_crime/COP5/CTOC_2010_CRP5/CTOC_COP_2 010_CRP5_E.pdf.

[130] Clough, "A World of Difference", 730-731.

[131] Andreea Verteşolteanu, "Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime", *Journal of Eastern-Europe Criminal Law* 1 (Biannual, 2014), 85-86.

2.2.2 The Council of Europe's Cybercrime Convention, 2001

In 1997, a Committee of Experts on Crime in Cyberspace was established by the Council of Europe to frame guiding principles in order to prepare a Convention.[132] Owing to these developments in international criminal law, Convention on

Cybercrime was signed by the Council of Europe in 2001 and entered into force in 2004.[133] The Council of Europe's Cybercrime Convention is an important example of international cooperation to fight cybercrimes.[134] The Convention was originally recognized as a regional agreement but the inclusion of non-European states has raised its standard to that of a leading multinational binding instrument.[135] It provides opportunities to the member states to update their national cybercrime laws even if the Convention is silent regarding that issue. So along with the emphasis on the member states to cooperate with each other in the war against cybercrimes at international level, it also provides them opportunities to make their national laws without any restriction from the Convention.[136] The Convention has proved effective in international cooperation for investigation of cybercrimes and the developments in Europol can be seen as important example. Two effective steps were taken by Europol with the establishment of European Cybercrime Centre and its joint Cybercrime Action Taskforce in 2013 and 2014 simultaneously facilitating investigations of critical cybercrime threats faced during recent years.[137]

[132] Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal* 18: 1 (Quarterly, 2003), 429.
[133] Verteşolteanu, "Evolution of the Criminal", 86-87.
[134] Kaman, "International Criminal", 323.
[135] Zahid Jamil, "Global Fight against Cybercrime: Undoing the Paralysis", *Georgetown Journal of International Affairs* Cyber Issue II (Biannual, 2012), 113-114.
[136] Clough, "A World of Difference", 703.
[137] Jaffery and Feakin, "Underground Web", 6.

2.2.3 Geneva Declaration and Geneva Plan of Action, 2003

In 2001, the General Assembly of the UN permitted holding of World Summit on the Information Society (WSIS) in two phases.[138] It is declared as an important effort of the international community to sit jointly and discuss the formation of a safe information society.[139] Initially first phase of the Summit was held in 2003 resulting in Geneva Declaration of Principles and Geneva Plan of Action. The Geneva Plan of Action provided for steps to be taken by governments with the cooperation of private sector to control cybercrimes.

2.2.4 The Tunis Agenda for Information Society, 2005

Second phase of the World Summit on the Information Society was held in 2005 at Tunis. The Summit resulted in the Tunis Agenda for Information Society mentioning that governments should make laws regarding cybercrimes keeping in view not only the Convention but other regional efforts as well.[140]

2.2.5 Additional Protocol to the Convention, 2006

In 2006, another important step was taken by the Council of Europe when it presented an Additional Protocol on Hate Speech to the Convention. This Protocol has been signed by 33 states as updated till May 2021. The Protocol binds the ratifying states to prohibit and outlaw the use and publication of racist and xenophobic material through any mode including computer as well. Racist and Xenophobic material has

[138] "Basic about WSIS", *ITU,* accessed 30 January, 2022. https://www.itu.int/net/wsis/basic/about.html

[139] "ITU History-Overview 8", *ITU,* accessed 30 January, 2022. https://www.itu.int/en/history/Pages/ITUsHistory-page-8.aspx

[140] "Basic About WSIS", *ITU,* accessed 30 January, 2022. http://www.itu.int/net/wsis/basic/about.html

been defined in the Protocol as any form of content that provokes hate, inequity or violence towards any person or organization.[141]

2.2.6 Global Cyber Security Agenda, 2007

An important step was taken by the International Telecommunication Union (ITU)[142] in 2007 with the launch of Global Cyber security Agenda (GCA). GCA emphasized on the need of harmonization of international cyber laws and need of cooperation between countries.[143] The strategy to be adopted was divided into five categories including legislative measures, technical steps, capacity building, formation of organizations and most important of all is the cooperation at international level. GCA established a High-Level Experts Group (HLEG) in order to achieve its objective of fighting with cybercrimes.[144] Details about HLEG shall be discussed in the next chapter in detail under the head of ITU.

2.2.7 UN Resolutions Related to Cyber Security

During process of the passage of above mentioned Conventions and Protocols, some resolutions of the UN's General Assembly passed at different times played an important role to deal with cybercrimes in an effective way. The resolutions passed in 2001 and 2002 are the initial steps in this process. Both of these resolutions were passed with the purpose of combating with the unlawful use of information

[141] Robert Smith and Mark Perry, "Fake News and The Convention on Cybercrime", *Athens Journal of Law* 7: 3 (Quarterly, July 2021), 339, accessed 25 February, 2022. Https://Doi.Org/10.30958/Ajl.7-3-4

[142] It is an old age institution established in 1800's to make rules and regulations regarding latest technological developments. Muzammil M. Hussain, "Digital Infrastructure Politics and Internet Freedom Stakeholders after the Arab Spring", *Journal of International Affairs* 68: no1 (2014), 39.

[143] Clough, "A World of Difference", 726.

[144] Rolf H. Weber and Ulrike I. Heinrich, *Anonymization* (London: Springer Publishing, 2012), 53-54.

technology.[145] The resolution passed in 2001 stated that advancements in information technology have paved way for new sophisticated crimes and there is a need of cooperation between states and the private sector to fight with cybercrimes. The resolution focused on the need of mutual collaboration of the states to tackle cybercrimes in an efficient way. Some important steps to be followed by the states have also been mentioned in the resolution. Most important points in these guiding principles were cooperation in investigation and exchange of information with other states in the cases of cybercrimes. It was also asserted that states should make strict national laws to deal with cybercrimes and provide good training to their law enforcement agencies to deal with the situations arising out of cybercrimes.[146] In the resolution passed in 2002, the UN again focused on international cooperation and also asked the states to follow the work of the Commission on Crime prevention and Criminal Justice and the methodology followed by other regional and international organizations when framing their national laws.[147] Two new resolutions were passed in 2003 and 2004 to accelerate the legislative process. The resolution passed in 2003 asked the member states to make strategy for upcoming phases of WSIS and also stressed on the creation of a universal culture of cyber security by prescribing important elements to be followed by all states.[148] The resolution of 2004 emphasized on the need of adopting a global culture of cyber security, by protection of critical information infrastructures and promotion of the transfer of information technology

[145] "UN Resolutions", *ITU,* accessed 03 February, 2022. https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

[146] A/RES/55/63

[147] A/RES/56/121

[148] A/RES/57/239

to the developing countries.[149]Another important resolution was passed in 2010 which provide a self-assessment strategy to be followed by the states to evaluate effectiveness of their efforts at national level.[150]

2.2.8 Regulations of the European Union on Cyber Security

In 1999, the European Union issued a Directive on Data Protection in order to harmonize national laws of the European Union states on the protection of data. Another important objective of the Directive was to stop the states from discriminating other states on the grounds of data protection. In 2002, the European Union issued a Monitoring Framework on Telecommunication and along with it also issued a Commandment on E-Privacy in the same year. These set of rules provided for different security steps to be followed by the service providers including report of cyber incidents to the authorities. The European Union also made laws to contend with the issue of online sexual abuse of children in 2011.[151] The European Union published its detailed policy on cyber security (Cybercrime Directive) in 2013 with the aim to provide measures that can be adopted to remain protected from cybercrimes.[152]

2.2.9 Legislative Efforts of the Group of 8 (G-8)

G-8 has played a very effective role in solving different international issues.[153] The group is not a formal organization rather it is a meeting group of world's greatest or

[149] A/RES/58/199

[150] A/RES/64/211

[151] Luukas K. Ilves et al., "European Union and NATO Global Cybersecurity Challenges: A Way Forward", *PRISM* 6: 2 (Quarterly, 2016), 131.

[152] Elaine Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation* 5: 1 (Quarterly, 2014), 49.

[153] Sussmann, "The Critical Challenges", 476.

strongest economic powers belonging to different continents including Asia as well[154] who conduct their meeting once a year. First initiative was taken at the meeting of information ministers of the G-8 in 1995. It was decided that information technology shall be promoted through international cooperation and also announced some pilot projects for this cause to be funded by the G-8.[155] These recommendations were sanctioned at Lyon Summit in 1996 and the working group was named as "Lyon Group". Most important point of these recommendations was advice to member countries to review their existing laws and modify them according to the emerging trends of computer crimes. International cooperation and solution of jurisdictional issues was also asserted in the recommendations. An important achievement is the formation of a group named "G-8 Subgroup on High-tech Crime" to make rules for cybercrimes.[156] A comprehensive action plan related to cooperation by all states in the investigation and prosecution of high-tech crimes was adopted in 1998 at the annual Summit of G-8 with the basic aim of leaving no safe haven for the abusers of cyber technology.[157]

An international training conference was also held in 1998 to promote exchange of computer related knowledge. In 2004, G-8 organized "Conference on High-Tech Crime" which provided distinction between attacks on computer infrastructure and crimes conducted with the help of computer.

[154] Soran K. Omer, "The Role and Future of G8", *Journal of Process Management and New Technologies* 7: 1 (Biannual, 2019), 49.

[155] Jaffery A. Hart, "The G8 and The Governance of Cyberspace", in *New Perspectives On Global Governance: Why American Needs the G8*, ed. Michele Fratianni et al., (Hampshire: Ashgate Publishing, May 2005), 139.

[156] Sussmann, "The Critical Challenges", 482. [165] Ibid, 476-477.

[157] Ibid. 484-485.

2.2.10 Legislative Approaches Adopted by Common Wealth

Common wealth, an association of 54 independent states, [158] has also played a significant role to combat cybercrimes. The Model Law on Computer and Computer Related Crime is an important achievement by the Common wealth [159] made by following the pattern provided in the Convention on Cybercrime.[160] The law provided a framework to be followed by the member states while making their national laws and criminalizing different problems emerging due to use of computer and internet.[161] The detailed account of legislative approaches adopted at international and regional level reveals significance of the issue and the need for serious efforts to be done by all the states at national and international levels. After discussing international and regional efforts, next sections deal with legislations of some countries adopted at national level.

2.3 Legislation by Different Countries at National Level

The safety of information technology systems is a necessity and states must make laws to deal with the cybercrimes that can be conducted by the breach of such security. Along with legislation, the states must keep their legal and prosecution systems updated with ever-changing cyber trends.[162] In the present part, national laws made by some countries to deal with cybercrimes at domestic level have been mentioned.

[158] "About Us", The Common Wealth, accessed 04 February, 2022, https://thecommonwealth.org/about-us

[159] "Model Law on Computer Related Crime", *The Commonwealth,* accessed 04 February, 2022. https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Com puter_Related_Crime.pdf

[160] Gillespie, *Cybercrime*, 19.

[161] "Model Law on Computer Related Crime", *The Commonwealth,* accessed 04 February, 2022. https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Com puter_Related_Crime.pdf

[162] Francesco Calderoni, "The European Legal Framework on Cybercrime: Striving for an Effective Implementation", *Crime, Law and Social Change* 54: 5 (Monthly, 2010), 341.

The countries that have been discussed include the US and the United Kingdom being the countries that have participated in cyber development since invention of computer and also due to the reason that these states are examined and kept in view while making most of the legislation in Pakistan.

2.3.1 Legal Framework of the United States of America

Being one of the pioneers of internet and related information technology, it would be necessary to discuss the legislations done by the US, at national level, in order to fight with the negative impacts of the advancements of information technology. The US is a federal state so its laws are divided into two categories, federal laws and state laws made by respective legislative organs.[163] The present section deals with some cybercrime legislations done by the US Congress. First step was the Computer Fraud and Abuse Act, 1984 which became the basis of cybercrime legislation in the US, but failed to attain popularity on account of certain defects in it. All the later laws brought changes in the said Act to be discussed in detail in forthcoming discussion.

2.3.1.1 The Computer Fraud and Abuse Act, 1984

The legislative process started in Congress in 1984 [164] that resulted in the passage of the Computer Fraud and Abuse Act (CFFA).[165] The Act provided for seven categories of computer related offences providing no specific investigatory regulations.[166] Its basic aim was to prosecute the makers of computer viruses, worms and Trojan horse

[163] Article VI, Clause 2 of the US Constitution, also called Supremacy Clause, states that federal laws are applicable to whole of the state while state laws are applicable to the respective territory. In case of conflict between both laws, except violation of human rights, the federal laws shall prevail.

[164] Kerr, "Cybercrime's Scope", 1616.

[165] James T. Graves, Alessandro Acquisti and Ross Anderson, "Perception versus Punishment in Cybercrime",*The Journal Of Criminal Law And Criminology* 109: 2 (Quarterly, 2019), 314.

[166] Salil K. Mehra, "Law and Cybercrime in the United States Today", *The American Journal of Comparative Law*58: Suppl_1 (Quarterly, 2010), 661.

that resulted in serious consequences for the computer systems.[167] The legislation could not gain popularity and was heavily criticized on grounds of abuse during prosecution.[168] Owing to the criticism, the law was completely revised in 1986. Since then changes have been made in the law for eight times. This amendment widened scope of the Act by the addition of new offences. The law was again fully revised in 1996 forming current structure of the law.[169] The scope of the Act was widened by amendments but it did not prove fruitful on account of ambiguities in the law[170] paving way for future legislations. The Identity Theft and Restitution Act, 2008, to be discussed under coming heads, is responsible for major amendments in the CFFA.[171]

2.3.1.2 Economic Espionage Act, 1996

The developments in information technology and emerging cybercrimes necessitated the need of protection of trade secrets from being stolen by any means including the internet. The Economic Espionage Act, 1996 not only aimed at prohibiting misappropriation of trade secrets under the head of theft of trade secrets while it also forbade economic espionage meaning transfer of any one's trade secrets to a foreign person or body. In other words, the law makes the owner as having sole authority over his secrets of his business thus creating a property-based approach in relation to trade secrets.[172]

[167] Aaron Burstein, "A Survey of Cybercrime in the United States",*Berkeley Technology Law Journal*18: 1 (Quarterly, 2003), 321.
[168] Graves, Acquisti and Anderson, "Perception Versus", 314.
[169] Reid Skibell, "Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act", *Berkeley Technology Law Journal* 18: 3 (Quarterly, 2003), 912-914.
[170] Ibid, 916.
[171] Eoghan Casey, *Digital Evidence and computer Crime: Forensic Science, Computers and the Internet*, 3rd ed. (Waltham: Elsevier Publishing, 2011), 86.
[172] Burstein, "A Survey of Cybercrime", 323.

2.3.1.3 The Digital Millennium Copyright Act, 1998

Latest technological trends have provided more sophisticated and advanced ways of illegal sharing of a copyrighted work. The promulgation of copyright Act is not new in the US, for instance the Lanham Act, 1946 has provided a basis for protection of trade marks.[173] The Digital Millennium Copyright Act (DMCA) passed in 1998 is a step to deal with the latest trends of digital piracy. The DMCA was passed with the objective of providing control to the actual owners or authors from illegal or unauthorized access or replication of their work.[174] The law not only provides long term legal protection to the authors along with it has also provided a right of 'fair usage' of the copyrighted works without any permission for the certain purposes like educational research, criticism, commentary and news reporting.[175]

2.3.1.4 The US Patriot Act, 2001

The 9/11 attacks[176] provided an opportunity to the US to frame new laws in order to stop terrorism. The US Patriot Act, 2001 is also a series of such attempts and it has not only widened the powers of law enforcement authorities, along with it has provided absolute right to detain foreigners merely on the basis of suspicion or mistrust. [177] The Patriot Act also widened the scope and applicability of the CFAA.[178]The Patriot Act made it easier for the law enforcement agencies to frame charges of felony against a cybercriminal. The presence of any ambiguities and

[173] Casey, *Digital Evidence,* 102.

[174] Neil W. Netanel, "Why has Copyright Expanded? Analysis and Critique", in *New Directions in Copyright Law,* ed. Fiona Macmillan, vol. 6 (Cheltenham: Edward Elgar Publishing, 2007), 9.

[175] Blayne Haggart, *Copyfight: The Global Politics of Digital Copyright Reform* (Toronto: University of Toronto Press, 2014), 96.

[176] The attack on World Trade Centre in the US on September, 11, 2001.

[177] Cary Stacy Smith and Li-Ching Hung, *The Patriot Act: Issues and Controversies* (Illinois: Charles C. Thomas Publisher, 2010), 32.

[178] Yar, *Cybercrime,* 51.

deficiencies in the Patriot Act have been tried to overcome by enactment of the Cyber Security Enhancement Act. The newly passed law directs the Sentencing Commission to strictly upgrade penalties provided under the CFAA.[179]

2.3.1.5 Identity Theft Enforcement and Restitution Act, 2008

The issue of identity theft is a danger to national security of any state. Seriousness of this category of cybercrimes was seriously felt by the US government after 9/11. The ratification of Identity Theft Enforcement and Restitution Act, 2008 is also a series of such attempts that were done to stop terrorist attacks in the US.[180] The law has been passed with the intention of bringing an end to some modern cybercrimes like phishing, identity theft and spam. The jurisdictional issues faced in previous legislations related to cybercrimes have been lifted and now the federal government has the jurisdictional power to deal with such cases without any ambiguity. Botnets have also been targeted by the Act and the definition of cyber extortion has been widened by adding new categories of extortion in it. The law was welcomed by the officials on account of provision of more space to the prosecution of criminals and the compensation of victims of such incidents.[181]

2.3.1.6 Laws for Protection of Children from Online Exploitation

Advanced technological devices have made it easier to make photos or videos of anyone without one's consent. To protect the children from exploitation by these advanced technological instruments, several attempts have been carried out by the US government. In 1977, the Protection of Children against Sexual Exploitation Act was passed criminalizing the act of taking visuals of any minor revealing sexual behavior

[179] Skibell, "Cybercrimes", 916-17.

[180] Mehra, "Law and Cybercrime", 661.

[181] Richard Acello, "Technology: Feds Ready to Tackle Cybercrime: New Law Gives U.S. Another Weapon", *ABA Journal* 95: 2 (Monthly, 2009), 37.

thus making child pornography a punishable offence.[182] In 1984, Child Protection Act was passed by Congress following Supreme Court's ruling[183] in *New York v. Ferber.*[184] The Supreme Court stated that First Amendment did not cover child pornography however the Court identified two major harms to be inflicted by the pornographic material even not obscene. First harm is the physical and mental harm inflicted to the child during the preparation of such material and second harm is conducted by sharing of such images.[185]Another category of harm was identified by the Supreme Court in *Osborne v. Ohio,* where the Court stated that along with infliction of harm by the creation and distribution of pornographic material, prohibiting the possession of such material shall be helpful in reducing such incidents in future.[186] The 1984 Act outlawed child pornography and possession of such material depicting sexual conduct by children even if the visual do not fall within the definition of obscenity. The 1984 Act is of importance as the modern technology has made the recording, sharing and possession of any material including child pornographic material very easy thus inflicting a physical and psychological stress on the children.

In 1986, two new legislations were passed by the Congress. These laws were The Child Sexual Abuse and Pornography Act and the other law was titled as The Child Abuse Victims' Rights Act. First law banned any sort of ads for child pornography while the second law held the pornographers responsible for

[182] Sarah Sternberg, "The Child Pornography", 2795.
[183] Ibid.
[184] 458 U.S 747 (1982)
[185] Carissa Byrne Hessick, "Setting Definitional Limits for the Child Pornography Exception", in *Refining Child Pornography Law: Crime. Language and Social Consequences,* ed. Carissa Byrne Hessick (Ann Arbor: University of Michigan Press, 2016), 60.
[186] 495 U.S. 103 (1990)

compensating the child victims involved in such pornographic advertisements. In 1988, Congress passed The Child Protection and Obscenity Enforcement Act with the object of declaring the use of computer in child pornography as illegal.[187] Supreme Court supported the view of declaring possession of child pornography materials as a criminalized act in the *Ohio case*.[188] Based on this ruling, Congress passed a new law in 1990 titled as Child Protection Restoration and Penalties Enhancement Act prohibiting possession of such items. An important step taken by Congress to outlaw child pornography is the Child Pornography Prevention Act, 1996. Child pornography has been redefined in a new style as pornographic material can be produced without the use of real children.[189] The Protect Act, 2003 banned child pornography and also amended Article 18 of US Code by adding paragraph (a) (3) in Section 2252A.[190] This step is a good attempt to outlaw the use of computer and other modern technology for child pornography.

2.3.1.7 Cybersecurity Information Sharing Act, 2015

A general law to regulate information sharing from non-federal entities to the Federal Government in cases of cyber threats was also a need of the time. This problem was solved by the Cybersecurity Information Sharing Act, 2015. The Act was further updated in October 2020.[191] The law has enhanced and provided proper procedure for information sharing in matters related to information technology.

[187] Sternberg, "The Child Pornography", 2795-96.

[188] 495 U.S. 103 (1990).

[189] Sternberg, "The Child Pornography", 2796.

[190] Mehra, "Law and Cybercrime", 664.

[191] "Cybersecurity Information Sharing Act 2015", *CISA*, accessed 07 February, 2022. https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-andguidance.

Apart from these national level legislative attempts, many cybercrimes laws have been made by the US states not to be discussed here as it is not of our concern. Our research is just restricted to legislations at national, regional and international level so a municipal legislative approach is not appropriate to be discussed here.

2.3.2 Legal Framework of United Kingdom

The United Kingdom is an important partner in the development of information technology. The United Kingdom has also been subject to cyber threats from hostile actions by states like Russia and Korea so the attempts to make cyber laws started in the country long before the developing countries.[192] It also became member of different international organizations and participated in their legislative process and in the meantime it has taken practical steps to formulate effective cybercrime laws in the country.

2.3.2.1 Data Protection Act, 1984

The information technology has made it easier for people to coordinate with each other while placing them at a risk of data disclosure. The International community realizes need for data security and for making laws in this regard.[193] The United Kingdom has also taken steps to protect the data of people linked through latest technology. Data Protection Act, 1984 is of great significance amongst earliest data protection legislations of the world. The law was later repealed but holds importance as it was made compulsory for the data users to get registered with the office of Data Protection

[192] Conrad Prince and James Sullivan, "The UK Cyber Strategy: Challenges for the Next Phase", *Royal United Services Institute* (Annual, 2019), 14.

[193] Anneliese Roos, "Core Principles of Data Protection Law", *The Comparative and International Law Journal of Southern Africa* 39: 1 (Tri-annual, 2006), 103.

Registrar. A proper procedure for registration of data was provided by the said Act.[194] Data Protection Act, 1984 was repealed and a new law Data Protection Act, 1998 was passed to deal with the data management of all those people who share their data through internet[195] in order to protect them from cyber threats like identity theft, online fraud or online harassment due to disclosure of their personal information that they have shared with some company or individual on the internet.[196]

2.3.2.2 Data Protection Act, 1998

The law of data protection in the United Kingdom cannot be understood in isolation and there is a need to study and apply the law with other enactments applicable in the state like Human Rights Act, 1998. [197] Present law deals with holding, alteration and use of computer-related information by individuals.[198] In addition to computer based records, manual records and data have also been included within the ambit of new legislation. Strict rules have been provided for transfer and processing of data until it complies with the restrictions mentioned in the law. Without satisfaction of these conditions, transfer of data is strictly banned to any country outside European Economic Area.[199]

2.3.2.3 Copyright Designs and Patent Act, 1988

The concept of copyright is not a new notion in the United Kingdom as printers were granted printing rights by Royal prerogatives in 15th and 16th centuries. First company to obtain a publishing right in England was "The Stationers" who obtained publishing

[194] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law*, 3rd ed. (Oxford: Oxford University Press, 2009), 4.

[195] "Data Protection Act, 1984 Repealed 1.3.2000", *Legislation.gov.uk*, accessed 05 March, 2022. https://www.legislation.gov.uk/ukpga/1984/35/section/19.

[196] Satapathy, "Law for Computer Misuse", 2639.

[197] Carey, *Data Protection*, 13.

[198] Satapathy, "Law for Computer Misuse", 2639.

[199] Carey, *Data Protection*, 9-10.

rights by the Royal Charter of 1557 and copies of books were only allowed to be given to the registered members. First copyright Act was passed in 1710 titled 'Statute of Anne.' The law granted 14 years copyrights to the publishers.[200] Several amendments were brought in the copyright laws by new enactments[211] [201]but as computer were not present in those days so there was no concept of copyrights of computer software and programs. Original Computer programs have been granted copyright protection from being pirated through online resources by passing Copyright Designs and Patent Act, 1988. The only condition to get copyright is the originality and not a copied work.[202] Copying substantial quality part of a computer program is also declared illegal by the law.[203] For the first time in English legislative history writers or creators of the work were granted moral rights, along with it abolished differentiation between 'work' and 'subject matter' and declared all creations to fall within the ambit of work. The advancements in information technology have made it easier for the cybercriminals to share the copyrighted work without authorization through internet causing loss to owner of the original work. To keep in pace with the latest trends in digital piracy and to follow the European Union's regulations, the law has been amended from time to time.[204]

2.3.2.4 Computer Misuse Act, 1990

Invention of computer has positive and negative both impacts. In order to stop the negative impacts by misuse of computer, like hacking, the United Kingdom has passed

[200] Tanya Aplin and Jennifer Davis, *Intellectual Property Law: Text, Case and Materials,* 2nd ed. (Oxford: Oxford University Press, 2013), 48.

[201] Ibid, 49

[202] David I. Bainbridge, "The Scope of Copyright Protection for Computer Programs", *The Modern Law Review* 54: 5 (Bimonthly, 1991), 643-44.

[203] Ibid, 646.

[204] Aplin and Davis, *Intellectual Property,* 50.

the Computer Misuse Act, 1990 which is the principal law applicable in the United Kingdom in relation to computer crimes. It is the first law in Europe that has specifically dealt with computer related offences.[205] This Act was presented with the primary purpose of making a law to stop misuse of computers. The law deals with different kinds of frauds committed through the misuse of computers. It is not a limited Act as it is applicable to the cybercrimes committed through internet outside England as well. Amendments have been made in the said Act by Police and Justice
Act, 2006 and Serious Crime Act, 2007.[206]

The United Kingdom is trying to improve its cyber policies. Its policies have proved extremely effective in combating cybercrimes as compared to rest of the world on account of being ahead of many states in the information technology. It needs to further strengthen its national cyber policies leaving no space for the cybercriminals to break its security.[207]

2.4 Legal Framework of Russia

Russia is considered as one of the most dangerous cybercrimes countries of the world[208]. Internet was introduced in Russia in 1994, a little late than the European states[209] but cybercrimes were reported long before the invention in Russia of internet in the country. An example of such incidents is the intrusion into computer system of an automobile factory in 1983.[210] Russia introduced cybercrime laws in 1996 with the insertion of chapter 28 in the new Criminal Code of the Russian

[205] Casey, *Digital Evidence*, 126.

[206] Casey, *Digital Evidence*, 127.

[207] Prince and Sullivan, "The UK", 17.

[208] Roman Dremliuga, Olga Dremliuga and Pavel Kuznetsov, "Combating the Threats of Cybercrimes in Russia: Evolution of the Cybercrime Laws and Social Concern", *Communist and Post-Communist Studies* 53: 3 (Quarterly, 2020), 133.

[209] Ibid, 123.

[210] Ibid, 124.

Federation.[211] But provisions of the law was not comprehensive as different cybercrimes especially by the use of internet were not clearly mentioned providing opportunities for the cybercriminals.[212] Due to ineffective legislative measures, cybercrimes grew at a faster rate inside Russia and many international hacker groups also appeared in Russia in 2000s.[213] This prompted the Russian government to make laws at national level and also to cooperate with the international community. Commonwealth of Independent states signed an agreement on the cooperation of states in cases of cybercrimes in 2001 and Russia also signed it in 2008 to cooperate with these state in cases of cybercrimes.[214] Many provisions of the Criminal Code have been revised by addition of new offences in the Code along with the provision that use of internet in any of these criminal activities would result in a double punishment.[215] Strict rules have been made in Russia even about collection of private data and same law has resulted in blocking of LinkedIn in Russia by an order of court in 2016.[216]

The steps taken by Russian government have resulted in decrease in cybercrime rates in Russia in 2016 as compared to 2000s.[217] The continuously developing nature of cybercrimes is needed to be dealt with more strict laws in order to control cybercrimes not only in the country but also outside Russia to create a positive image.

[211] Ibid, 124.
[212] Ibid, 124-25.
[213] Ibid, 129.
[214] Ibid, 129.
[215] Ibid, 130-31.
[216] Ibid, 132.
[217] Ibid, 132.

2.5 Conclusion

Cybercrimes are complicated offences needed to be dealt with the application of effective strategies at national and international levels. Many states have made laws to deal with cybercrimes at national planes but as the crime is of transnational nature, it is impossible for a single state to effectively deal with it. It is vital for the states to coordinate and cooperate with each other by regional and international legislative efforts. Many organizations have been made and international agreements and Conventions have emerged making legislative strategies to be followed by member states. Global cybercrimes strategy has been further developed by the resolutions of the UN and the Summits of WSIS organized by ITU in collaboration with the UN. The Model Law on Computer and Computer-Related Crime by the Common wealth, formation of G-8 Subgroup on High-Tech Crime and Conference on High Tech Crime are also important milestones in the development of international and regional cybercrimes law. In addition to these international and regional instruments, national laws made by different countries are also helping the states to fight with cybercrimes at their municipal levels. It is concluded that cybercrimes are dealt as a serious problem and legislative attempts are in progress to solve the problems faced due to misappropriation of cyber technology.

Chapter 3

Strategies Adopted by International and National Bodies to Reduce Cybercrimes

3.1 Introduction

Cybercrimes having universal nature are difficult to be dealt by one state alone, requiring international cooperation of the states with each other to fight cybercrimes.[218] The need for international cooperation against cybercrimes has been seriously comprehended by the global community and apart from the role played by international organizations like UN and the Council of Europe, different states are also coordinating to make a comprehensive policy by entering into treaties or making new organizations like for instance Strategic Alliance Cyber Crime Working Group formed by different western countries to combat cybercrimes. Efforts of INTERPOL and Europol to address the issue of cybercrimes cannot also be ignored.[219] Many complexities have been faced by the nations during this process making it difficult for the states to effectively deal with the issue of cybercrimes.

Present chapter is an analysis of the challenges posed to the states at international and national level along with a discussion of the role of some international and national organizations to overcome these challenges. In the coming sections, role of national and international bodies to deal with cybercrimes has been analyzed, and then different strategies applied in this regard by the international

[218] Vecino, "United by Necessity", 123.

[219] Mehan, *Cyber War*, 73.

community have been examined in detail. Last part of the chapter deals with the challenges faced by the nations around the globe to encounter cybercrimes.

3.2 Role of International and Regional Bodies to Combat Cybercrimes

The ever changing nature of cybercrimes has made it necessary for the world to act seriously and take practical steps apart from legislation alone. Practical implication of such laws is the next step without which the laws cannot prove effective. The global community is dealing with the issue by holding conferences, entering into joint ventures and formation of organizations at national and international level. In this fight against cybercrimes, a leading role has been played by different international and regional organizations and groups including the UN, the European Union, the Council of Europe and many other organizations. Role played by such organizations has been discussed in detail in the present section along with steps taken to counter cybercrimes.

3.2.1 The Council of Europe

Most important and early steps at the international level were taken by the Council of Europe so it would be important to begin the discussion with Council's role in the fight against cybercrimes. The Council of Europe was formed by a Statute signed in 1949 at London by different European countries creating two organs of the Council.[220] Basic purpose of the creation of the Council was to promote and strengthen coordination between different states of Europe in order to promote social and

[220] A. H. Robertson, "The Council of Europe, 1949-1953: I", *The International and Comparative Law Quarterly* 3:no 2 (Quarterly, 1954), 235.

economic development of the member states.[221] The initial step to pave the way for criminalization of cybercrimes was the organization of the Conference on Criminological Aspects of Economic Crime by the Council of Europe in 1976.[222] It was an important step toward international cooperation to curb cybercrimes. The Council of Europe's Convention on Cybercrime[223] is a landmark achievement.[224] The Convention was more elaborated by Additional Protocol to the Convention presented in 2006.[225] The Convention signed by different countries of the world including non-European states encompasses provisions related to criminal law and procedure to be followed during investigation and prosecution of cybercrimes. It has also focused on the need for international cooperation.[226] The Convention is declared as a landmark and followed by different countries while framing their national cyber security laws. The legal frame work provided by the Convention has also proved a good example for the law makers.

3.2.2 The United Nations

The UN is also an important platform that has participated in the formation of international strategy against cybercrimes. UNODC[227] has been established with the purpose of promoting international cooperation and research to deal with cybercrimes in an effective manner.[228] UNODC has established an interstate expert group with the objectives of conducting comprehensive study on cybercrimes by exchange of

[221] Robertson, "The Council of Europe", 236.
[222] Verteşolteanu, "Evolution of the Criminal", 85-86.
[223] Kaman. "International Criminal",323.
[224] Verteşolteanu, "Evolution of the Criminal",87.
[225] Smith and Perry, "Fake News", 339.
[226] Verteşolteanu, "Evolution of the Criminal", 87.
[227] United Nations Office on Drugs and Crime.
[228] "Cybercrime", *UNODC*, accessed 23 February, 2022. https://www.unodc.org/unodc/en/cybercrime/index.html.

information on practices, technical expertise and legislations applied in the member states.[229] To regulate the problems arising due to developments of information technology, the General Assembly of the UN organized the World Summit on Information Technology in two phases.[230] These two plans have already been discussed in detail in the previous chapter. Other achievements include attachment of ITU with the UN in 1952[231] and the launch of GCA in 2007.[232] Since its succession with the UN, ITU has provided support and technical assistance to the developing nations along with providing training to IT staff of these countries.[233] The Plenipotentiary Conference organized by ITU in 2006[234] also holds importance as it set out the future role of ITU. ITU holds this conference after every four years to draft new policy according to emerging cyber trends.[235]

3.2.3 The European Union

The role of the European Union cannot also be ignored in the efforts to control the increasing ratio of cybercrimes at regional and international level. Several directives and legal frameworks have been issued at different times by the European Union to be followed by the member states.[236] An important step taken by the European Union in combatting cybercrimes was the establishment of the European Network and

[229] "Global Program on Cybercrime", *UNODC,* accessed 23 February, 2022. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

[230] "World Summit on Information Society: Geneva 2003-Tunis 2005", *ITU,* accessed 24 February, 2022. https://www.itu.int/net/wsis/basic/about.html.

[231] "Overview of ITU's History 8", *ITU,* accessed 25 February, 2022. https://www.itu.int/en/history/Pages/ITUsHistory-page-8.aspx.

[232] Clough, "A World of Difference", 726.

[233] "Overview of ITU's History 8", *ITU,* accessed 25 February, 2022. https://www.itu.int/en/history/Pages/ITUsHistory-page-8.aspx.

[234] Ibid.

[235] "About PP-22", *ITUPP,* accessed 25 February, 2022. https://pp22.itu.int/en/about/aboutpp22/

[236] Ilves, "European Union", 131.

Information Security Agency (ENISA) in 2004.[237] Initial focus of the ENISA was research and training in information technology but with the passage of time it has widened its role and at present the ENISA aggregates the reports of cyber incidents.[238] Establishment of Europol as Law Enforcement Agency of the European Union to combat transnational crimes including cybercrimes is also a noteworthy attempt. In 2017, Europol became official law enforcement agency of the European Union.[239] In 2013, a European Cybercrime Centre (EC3) has been launched at the Europol with the purpose of mainly dealing with the cyber-attacks[240] and to implement Stockholm Program.[241]

The Cybercrime Centre is playing an effective role by cooperating with law enforcement agencies of other states also to combat cybercrimes. Its collaboration with FBI and different US private companies like Microsoft is an instance of its coordinating capabilities leading to investigations at international level [242] thus enhancing its rank from regional to international level. The EC3 also issues Internet Organized Crime Threat Assessment (IOCTA) mentioning main concerns to be followed in the coming years by European Multidisciplinary Platform against Criminal Threats (EMPACT).[243] The European policy issued in 2021 for the period

[237] Argomaniz, "European Union", 256.

[238] Ilves, "European Union", 131.

[239] "About Europol", *Europol,* accessed 14 February, 2022. https://www.europol.europa.eu/about-europol.

[240] Argomaniz, "European Union", 256.

[241] Fahey, "The EU's Cybercrime", 52.

[242] Ilves, "European Union", 134.

[243] "Cybercrime", *Europol,* accessed 14 February, 2022. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime.

2022-2025 stating priorities for EMPACT has included cybercrimes in its priority list for the said tenure.[244]

Apart from the above mentioned organizations, other regional organizations and countries have also participated in the struggle to countermand the increasing trend of cybercrimes. Role of G-8 and the Common wealth cannot be ignored in this regard.

Their efforts have been mentioned in the previous chapter with detail under page no 47.

3.3 Strategies Adopted by International and National Bodies

The complex nature of cybercrimes has made it essential for the world community to adopt comprehensive and wide-ranging policy to counter this intricate issue. All countries realize the seriousness of the issue of cybercrimes and the consequences of the failure to deal with it at both international and national levels. They also understand that national efforts cannot prove effective if they do not cooperate with other states. Different strategies have been adopted by the states to mitigate instances of cybercrimes and to halt such criminal practices in future. The need for having a consolidated policy has been seriously felt by the international community so in order to achieve this goal, cross-border partnerships have been made and different institutions have been formed to involve participation of law enforcement agencies and IT experts to lessen the increasing ratio of cyber incidents. The strategies followed by the states to make this world a safer place have been analyzed and discussed in the coming sections.

[244] "EU Policy Cycle EMPACT", *Europol,* accessed February 14, 2022. https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.

3.3.1 Consolidation of International Policing and Cross-National Partnership

Consolidation of international policing is the most important and leading strategy applied by the international community. An important illustration of such cross border cooperation is Strategic Alliance Cybercrime Working Group which has been formed to fight with cybercrimes. This working group comprised of criminal investigation agencies and police of different countries including the US, the United Kingdom, Canada, New Zealand and Australia.[245] The organizations included in the Group comprise: Serious Organized Crime Agency of the United Kingdom, FBI, and the Police of New Zealand, Canada and Australia.[246] Collective efforts are being done by the Alliance to counter with the cybercrime threats at international level and to share information and strategies to combat this crime.[247] Europol and INTERPOL are also part of this series of cross-national cooperation to counter cybercrimes.

3.3.2 Institutional Ecosystem

Formation of working groups or alliances cannot solely prove successful towards formation of an effective policy in combating cybercrimes. It is needed that organizations having crime squads with them must be trained to control the rising rate of cybercrimes. Positive initiative has been taken in this regard and along with legislation, international monitoring is being strengthened through different agencies like European Police Office (Europol) and International Criminal Police Organization (INTERPOL) who focus on dealing with cybercrimes through sharing of information at global level.[248] INTERPOL is an international organization having 195 member states formed with the objective of helping police of all member states in order to

[245] Hill and Marion, *Introduction to Cybercrime*, 121.
[246] Mehan, *Cyber War*, 73.
[247] Ibid.
[248] Yar, *Cybercrime*, 16.

mitigate crimes at international level.[249] Moreover it has established a global catalogue of cybercrimes detectives and provided cyber security training at individual level in collaboration with other international organizations. It strongly emphasizes on the need for cyber security trainings and adoption of strict security measures at international level.[250] Europol was established by the European Union with the purpose of meeting the challenges faced by transnational crimes.[251] It has also participated in the fight against cybercrimes by establishment of institutions [252] and issuance of policies such as IOCTA.[253] Apart from including cybercrimes in its priority list to be followed from 2022-25,[254] an online web portal Check The Web (CTW) has also been launched by the Europol in order to cope with terrorism conducted through the use of internet.[255] Another important agency ENISA established in 2004 by the European Union is also focused to help in coordination of information exchange in cases of cybercrimes though it is not a directly investigating agency.[256]

3.3.3 Formation of National Security Agencies and Emergency Response Teams

All states are taking serious measures to counter cybercrimes. Formation of Security agencies at national level can be regarded as a positive step towards making a secure cyber world. Steps are being taken by these Security agencies to create public

[249] "What Is INTERPOL", *Interpol.int,* accessed 15 February, 2022. https://www.interpol.int/en/Who-we-are/What-is-INTERPOL.

[250] Mehan, *Cyber War,* 73.

[251] Vecino, "United by Necessity", 124.

[252] Argomaniz, "European Union", 256.

[253] "Cybercrime", *Europol,* accessed 14 February, 2022. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime.

[254] "EU Policy Cycle EMPACT",*Europol,* accessed 14 February,2022. https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.

[255] Argomaniz, "European Union", 258.

[256] Yar, *Cybercrime,* 16.

awareness regarding cyber incidents.[257] An important instance is the statement of President Obama in 2009 about formation of White House Cyber Security Office with the main objective of security of country's digital infrastructure. He also emphasized for promotion of cooperation between private and public sector without restricting and influencing private sector's security plans.[258] The formation of Computer Emergency Readiness Team (CERT) Portal, to be discussed in next chapter, by Pakistan Telecommunication Authority (PTA), the principal regulatory authority of telecommunication services, in Pakistan is also an attempt of prevention of its users from cybercrimes.[259]

These response teams related to reporting, detecting and handling of cyber incidents are sometimes called CIRT[260] while sometimes they are termed as CERT.[261]The CIRT/CERT is basically a group of IT experts assigned with the task of responding in case of any cyber incident. Such CIRTs/CERTs are mostly hired by large organizations or at governmental level and they are assigned with the task of responding without any wastage of time or taking permission in cases of any cyber breach. The CIRTs/CERTs prepare formal plans to be followed in cases of cyberattack and also help to identify cyber response ability of that particular organization.[262] A team of computer experts from member states of the European Union named as The Computer Emergency Response Team (CERT-EU) was established by the European

[257] Kshetri, *The Global*, 16.

[258] Ibid, 17.

[259] "Media Center", *PTA*, accessed 03 March, 2022. https://www.pta.gov.pk/en/mediacenter/single-media/pta-launches-cert-portal-for-telecom-industry--050421.

[260] Computer Incident Response Team.

[261] Computer Emergency Response Team.

[262] Darril Gibson and Andy Igonor, *Managing Risks in Information Systems*, 3rd ed. (Burlington: Jones & Bartlett Learning, 2022), 379.

Union in 2010 responsible to deal with the security of the European Union Institutions. CERT-EU is playing a very effective role in different collaboration networks at international level.[263] A report published by ENISA in February 2011 has provided an excellent guide that can be followed by CIRTs/CERTs for achieving better management of cyber incidents. There is a need that working of such incident response teams of CIRTs/CERTs be enlarged from national level to the international scale.[264]

3.3.4 Efforts for Public-Private Partnership

Cybercrimes having complex character are difficult to be traced and dealt by the entities at individual levels therefore it is necessary that a policy of public-private partnership be formulated in order to deal with cybercrimes more effectively at national level. With the expansion of information technology, the private sector is handling public-facing set-up through computers and therefore they are a target to cyber-attacks as much as public sector is at risk of such attacks. Along with, various private information technology companies have great expertise in cyber security tools and approaches like Microsoft.[265265] Likewise, many companies hire cyber experts or they form cyber response units to deal with threats of cyber-attacks and the situations related there to.[266]

3.4 Challenges of Fighting Cybercrimes

The developments of information technology have created positive and negative impressions on the lives of individuals. It has benefited the human race but as the criminal mind-set is always there, the criminals have invented new methods to benefit

[263] Ilves, "European Union", 131.

[264] Audrey Guinchard, "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy", *Journal of Strategic Security* 4: no2 (Quarterly, Summer 2011), 79.

[265] Vecino, "United by Necessity", 128.

[266] Peter N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10: no 2 (Bimonthly, 2001), 248.

themselves through illegal ways resulting in a new challenge for the world.[267] This challenge of cybercrimes has been tried to be solved by the global community as discussed earlier. Many hurdles and complications have been faced in the formulation of a comprehensive policy at national and international both levels. Present discussion is an analysis of the challenges faced by the international community during the fight against cybercrimes.

3.4.1 Transnational Nature of Cybercrimes

Internet has made it easier for the criminals to coordinate with each other and commit crimes at far off places without being physically present at the crime scenes.[268] With just few taps on the keyboard, the crime can be committed causing incalculable loss. This results in origination of complex situations for the law enforcement agencies during investigations of the crime.[269] The UNODC revealed in its report that more than 50% cybercrimes are of transnational nature that cannot be dealt effectively by the criminal laws due to jurisdictional constraints.[270] This scenario has created a very difficult situation for the law enforcement agencies and has intensified the need for harmonization of law to deal with such crimes of transnational nature.[271]

3.4.2 Absence of Updated Criminal Statutes and Blockade by Existing Laws of the State

An important issue faced by the nations while dealing with issue of cybercrimes is the absence of a criminal statute able to cope with the newly emerging crimes. Studies

[267] Ibid.

[268] Clough, *Principles*, 8.

[269] Allison Peters and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", *Third Way* (2019), 4-5, accessed 15 March, 2022. http://www.jstor.org/stable/resrep20150.

[270] United Nations Office on Drugs and Crime, *Comprehensive study on cybercrimes*, 2013,

[271] Clough, *Principles*, 8.

have revealed the absence of laws to deal with cybercrimes, as becomes apparent from the example of "I love you" virus.[272] Sometimes existing laws of the country also become an impediment for the new cybercrimes laws, for instance, in the US, Communication Decency Act, 1996 [273] was overturned as some of the Constitutional guarantees, provided by the Constitution of the US, like freedom of speech and expression seemed to be endangered by the said law.[274] Communication Decency Act, 1996 banned the transmission of any obscene or indecent messages to a recipient whose age is less than 18 years but this restriction was declared as an attack on human rights so the law was invalidated by the Supreme Court.[275]

3.4.3 Deficiency of Procedural Powers

Lack of competent procedural guidelines to deal with the suspects of cybercrimes is also another problem for the states. Denial of Service attack in 2002 is an important instance that created problems for the law enforcement agencies to track the roots of such denial.[276] To deal with future cyber-attacks, High Tech Crime Centre has been formed by Europol. Even though the Centre has been formed, experts think that this step is not sufficient to deal with cyber-attacks that are boosting in more sophisticated way with the passage of time.[277]

3.4.4 Lack of Cooperation between Countries

The cybercrimes are of transnational nature, so jurisdictional issues often arise when dealing with the crimes. A lacuna is created in the investigations as location of

[272] Weber, "The Council", 426.

[273] The law

[274] Yar, *Cybercrime,* 16-17.

[275] Amy B. Jordan, "Children's Media Policy", *The Future of Children* 18: 1 (2008): 240, accessed 10 September, 2022. http://www.jstor.org/stable/20053126. [276]Weber, "The Council", 426-427.

[276] Weber, "the Council", 426-427

[277] Ibid, 427.

cybercriminals outside the country demands cooperation from the other country where there can be chances that the foreign government is not willing to cooperate or is unable to do so on account of absence of any legislation to cooperate with a foreign state in such circumstances.[278] In such situations, lack of cooperation between states becomes a noticeable impediment to the prosecution of cybercriminals. [279] Cyberattack on the US banking system in 2000 and Russian non-cooperation in the investigation of the suspected Russian hackers is an important instance in this regard. [280] Many international Conventions have been passed to deal with such noncooperation like Council of Europe's Convention on Cybercrime and the UN's Convention on Transnational Organized Crime.[281]

3.4.5 Cyber Security Policies of States

Cyber security policies issued by different states of the world also create differences at international level increasing non-cooperation in dealing with the issue of cybercrimes. When cybercrime policy of one state mentions its monopoly or superiority of a group of states, it becomes difficult for the other states to digest that policy and to follow it. For instance, heavy investments are done by the US in creating cyber weapons, like a computer virus named Stuxnet worm that was used by the US and Israel to target computer system of Iran's nuclear system,[282] in order to keep its

[278] Allison Peters and Anisha Hindocha, "US Global Cybercrime Cooperation: A Brief Explainer", *Third Way* (2020), 4, accessed 20 February, 2022. http://www.jstor.org/stable/resrep25041.
[279] Weber, "The Council", 427.
[280] Weber, "The Council", 427-28.
[281] Fawzia Cassim, "Formulating Specialized Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study", *Potchefstroom Electronic Law Journal* 12:no 4 (Monthly, 2009), 41, accessed 05 March, 2022. ISSN 1727-3781
[282] Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs* 175:no 5 (2013), 35.

military dominance in the world.[283] This attempt is not acceptable for other powerful states like Russia and China. They have also done attempts to compete with the US in reply to the US policy.

3.4.6 Absence or Lack of Expertise and Resources to Deal with Cybercrimes

Lack of expertise in law enforcement agencies to deal with a crime makes it difficult for them to tackle the issue. There may be chances that law enforcement agencies do not have the required technical equipment's to deal with the problems arising out of misuse of digital technology. Such deficiency of equipment or knowledge makes it difficult to track cyber incidents and capture the culprits.[284] It has been revealed in researches conducted on cybercrimes that police often lack technical knowledge so they feel it difficult to deal with cybercrimes within the parameters of normal criminal system of the state.[285]

Financial issues or lack of budget is also one of the important reasons for such technical inadequacies as most of the countries have allocated more budgets to terrorism and other related crimes as compared to cybercrimes as they have not prioritized cybercrimes over other categories of crimes.[286] For instance, the United Kingdom has allocated £1.3 billion for five years to tackle cybercrimes[287] while the same budget has allocated £2 billion per year for terrorism incidents showing the basic priority for the government.[288] It can be observed that basic priority of the world's

[283] Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game", *Strategic Studies Quarterly* 6:no 4 (2012), 105.

[284] Clough, *Principles*, 16-17.

[285] Yar, *Cybercrime*, 16.

[286] Peters and Jordan, "Countering the Cyber", 9.

[287] United Kingdom Comptroller and Anditor General, *Progress of the 2016-2021 National Cyber Security Programme*, UNITED KINGDOM NATIONAL AUDIT OFFICE, 4 (Mar. 15, 2019), accessed 05 March, 2022. https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-20162021-National-Cyber-Security-Programme-Summary.pdf.

[288] Peters and Jordan, "Countering the Cyber", 9.

governments has been shifted to terrorism although cybercrimes are of almost same destructive nature at some occasions. At the same time private sector is focused to fight cybercrimes as a priority but such efforts cannot be a substitute to national level efforts.[289]

3.4.7 Jurisdictional Issues

Generally, crimes are dealt by the national or regional legislations making international crimes a distinct and different category of laws. But the global characteristic of cybercrimes has crossed the national boundaries creating worldwide impacts generating problems for the global community at large.[290] There have been many instances that one country declares certain act as illegal while the other country recognizes it as a legitimate act which makes it difficult to prosecute an offender who has committed a crime which has caused loss in one state but the other country does not declare it as an offensive act. For instance, online gambling is prohibited in some states while some states recognize it as a source of income and declare it legal. [291] The 'love bug' virus attack can be taken as an important instance which effected twenty countries across the globe but the criminal could not be prosecuted on account of absence of recognition of the act as a crime in Philippines. This event strengthened the need for comprehensive international cybercrime laws for a successful investigation and prosecution in cybercrime incidents.[292]

[289] Peters and Jordan, "Countering the Cyber", 9.
[290] Cassim, "Formulating Specialised", 39.
[291] Grabosky, "Virtual Criminality", 247.
[292] Cassim, "Formulating Specialised", 39.

3.4.8 Difficulty in Locating Country of Origination of Cyber Attack

In cyber-attacks, it becomes very difficult to track the origin of the cybercrimes as cybercrimes initiated from one state can practically take place in any other state. Instances of such mystified attacks have been observed around the globe when the attacks instigated from one place used a complex network to conduct the crime at a remote place. Recent example is the attack on major websites of the US and South Korea in 2009. Investigations revealed that computer systems of 74 countries were used to conduct the attack while the commanding server was using a United Kingdom based IP address as well as it was also found that the master server was located in the US.[293] In this instance, it can be observed that the country of origin differed from the place of actual damage and also that the system used belonged to more than one state creating puzzlement about jurisdiction of the crime and also the law under which the offenders are to be tried. Such complex jurisdictional issues have created ambiguity for the states to trace and deal with the crime with precision and accuracy.

3.4.9 Concealment of Identity

Most important feature benefitting offenders is "anonymity" which is a major hurdle in effective progress against cybercrimes. Internet can help anyone to hide his identity and a person can use 'proxies' to reach a site where access is not allowed. Use of proxy makes it easier for the offenders to commit crime without any fear of being identified.[294] This concealment creates many problems for the states to identify the real culprit involved in a particular cybercrime.

[293] Kshetri, *The Global,* 8.

[294] Yar, *Cybercrime*, 54.

3.4.10 Non-Reporting of Majority of Cybercrime Incidents

Best cybercrime policy is also dependent on data of cybercrime incidents in the country. In the US, FBI reports that only one percent of the cybercrimes are reported while the rest goes unreported to the authorities. It has been identified by the European Union that even the mechanisms made by the governments for tracking cyber incidents are not sufficient to get complete report about such incidents due to various reasons.[295] Many victims of cyber-attacks do not report the incidents to authorities either due to mistrust in the authorities or due to fear of exposure of their incapability to deal with such situations.[296] In case of banks and companies, these institutions do not report their victimization of online fraud or any threats due to fear of damage to their reputation in public. On the other hand, individuals do not report such incident due to unawareness of benefits of cybercrime reporting.[297] As a result of such non-reporting of the cybercrimes, the victim may again suffer a larger loss than the first one and also creates a hurdle in formulation of a better strategy to fight cybercrimes by the law enforcement agencies.[298]

3.4.11 Lack of Public-Private Partnership at National Level

As a national policy cannot prove successful without certain help from international factors, it also requires the cooperation of private sector with the government to make a comprehensive cybercrime policy. Due to complexity of cybercrime tactics, it is difficult for one sector to deal seamlessly with cybercrimes. Lack of public-private cooperation and partnership has resulted in a weak strategy against such incidents

[295] Peters and Jordan, "Countering the Cyber", 10.
[296] Završnik, "Cybercrime", 13.
[297] Guinchard, "Between Hype", 80.
[298] Završnik, "Cybercrime", 13.

therefore it is needed that anti-cybercrimes policy must be framed in the style to provide more opportunities for public-private partnerships.[299]

3.4.12 Limited Statistical Collections

Limited resources at governmental level and diversity of methods adopted for assessment of cybercrime incidents result in the production of jumbled results and even sometimes produce wrong statistical analysis. It results in wrong analysis of the cybercrimes and inadequate policy measures for future incidents.[300] It is needed that the statistical analysis should not be based on a single department rather all departments of the state including public and private even military should coordinate with each other to form an accurate statistics in order to formulate a precise cybercrime policy of the state.[301] In addition to such cooperation in data formulation, organizations should conduct regular penetration tests by using the tools and methods that can be predicted to be used by the cyber attackers. Such penetration tests can form a good data to be kept in consideration while preparing a strategy for dealing with possible attacks.[302]

3.4.13 Difficulty in Evidence Collection

Another important obstruction experienced by the law enforcement bodies while dealing with cyber incidents is the collection of evidence in order to bring the culprit into court. The advancements in information technology like Cloud-based data storage have made it difficult for the law enforcement agencies to collect digital evidence as cloud based data collection centers can be based in diverse jurisdictions requiring the

[299] Vecino, "United by Necessity", 128.

[300] Guinchard, "Between Hype", 78.

[301] Guinchard, "Between Hype", 78-79.

[302] Ok Enigbokan and N Ajayi, "Managing Cybercrimes through the Implementation of Security Measures", *Journal of Information Warfare* 16: 1 (Quarterly, 2017), 114.

need for a complex procedure to be followed for evidence collection. In such cases it becomes necessary for the law enforcement agencies to get permission from that particular state with the help of national government making prosecution in cybercrimes a complex issue. In addition to this, the process is time consuming and costly making it difficult to collect evidence. This problem is needed to be tackled in order to provide easy approach of law enforcement agencies to evidential proofs of the cybercrime. An important step has been taken in this regard by the passage of Clarifying Lawful Overseas Use of Data, 2018 in the US.[303] Yet it is a good attempt but still more legislation is needed to be done by other countries of the world.

Another difficulty faced during the process of evidence collection is inability to access mobile phone records due to security App added in the phones as default setting. Such inability has created hindrance in accessing data of criminals or any other evidence leading to criminals creating problems especially in terrorism related cases. This problem needs a serious solution but yet no attempt has been made. Law enforcement agencies have tried to find a solution by application of technology but it is a costly process and also requires regular updates as mobile phone companies update their software on a regular basis.[304] Governments should pay serious attention to solution of this problem in order to make it easier for the law enforcement ageneies to collect evidence in cyber-attacks and other offences as well.

[303] Neil Desai, and Centre for International Governance, "Tackling Cyber-Enabled Crime Will Require Public-Private Leadership", *Governing Cyberspace during a Crisis in Trust: An Essay Series on the Economic Potential — and Vulnerability — of Transformative Technologies and Cyber Security*, Centre for International Governance Innovation (2019), 11, accessed 10 March, 2022. https://www.cigionline.org/static/documents/documents/Cyber%20Series%20Web2.pdf

[304] Ibid 11-12

3.3.14 Lack of Public Awareness

Public awareness is the key to successful application of a law. It is vital for the success of legislation that the public is fully guided about it and the positive impacts of the law be communicated to the public. Same is the case with cybercrime laws. As mentioned earlier, the cybercrime incidents are most of the time not reported by the public mostly due to their non-awareness about the law and the need for such reporting. [305] Cybercrimes are counted among one the most unreported crimes mostly due to lack of knowledge among general public about the laws. [306]

3.4 Conclusion

Cybercrimes, being of transnational characteristic, have created many problems for the world with new innovations at a faster pace and these problems are becoming complex with the advancements in technology. Despite strict measures adopted by the international community, many complications and obstacles have been faced. The challenges faced by the world during this struggle have been discussed in the last part of the chapter. It is concluded that more efforts are required with regular updates of the cybercrime strategies as cybercrimes are progressing at a faster pace and new crimes are generated with the advancements in technology.

[305] Guinchard, "Between Hype", 80.

[306] Porcedda et al, "Transaction", 46

Chapter 4

Lesson for Developing Countries and Specifically for Pakistan

4.1 Introduction

The cybercrime threat has activated the whole world to take steps against it. The steps taken by developed nations have proved more effective while the developing states lag far behind in this struggle mainly due to technical and economical incompetence. Legislative attempts are being made by developing countries to deal with increasing cybercrime threats. The Convention on Cybercrime has provided guidelines to the developing countries while framing their national cybercrime laws.[307] First part of the chapter deals with attempts taken by some neighboring developing countries including India and Bangladesh keeping main focus on Pakistan. Pakistan is using all the available resources to deal with the issue. Pakistan has made laws to face the problems that have arisen due to cybercrimes and also to stop such practices in future but the list is not so long. Many problems have been faced by Pakistan in this struggle. Second part of the chapter is a detailed analysis of cybercrime trends in Pakistan and the legislative attempts to deal with the situation. Necessary changes to counter the cybercrime threats have also been suggested in present research.

4.2 Progress of Cybercrimes Laws in Developing States

India, Pakistan and Bangladesh were united under British rule before August, 1947. These countries have inherited same British made legislations as their civil, criminal and family laws without any amendments. Same laws dealing with telephone and

[307] Zahid, "Global Fight", 109-110.

telegraph, being modern modes of telecommunication at that time, were inherited by these countries including the Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933. These laws have been discussed under the head of cybercrime legislations in Pakistan. Later legislative attempts were made by the parliaments of these countries to deal with the developments of information technology and the newly originated crimes.

4.2.1 Cybercrime Laws of India

India is also facing cybercrimes with the increasing use of information technology in the country. The need to control cybercrimes has paved way for the promulgation of cyber laws in India.[308] India enacted its first cybercrime legislation in 2000 titled as "The Information Technology Act, 2000". The preamble of said law has mentioned the development of electronic commerce in the country and has not stated cybercrimes in general, while Chapters IX and XI of the said legislation deal with cybercrimes and the related issues. So it can be said that the lawmakers have tried to make a comprehensive legislation.[309] Despite such hard work certain loopholes remained in the law making it difficult for the law to effectively deal with the newly originated cybercrimes. In order to solve the issue, the law was amended in 2008 including the matters that were not covered by the mother cybercrime legislation.[310] The Indian courts are playing an important role to clarify the ambiguities about the Information Technology Act and include new crimes and devices in the list of cybercrimes as the High Court of Andhra Pradesh held that the mobile phone comes within the category

[308] Mishra, *An Overview, 3.*

[309] Munir, "Electronic", 191.

[310] Mishra, *An Overview*, 6-7.

of computer and a computer source code maintained by the cell phone operator is a valid evidence.[311]

A report was issued by Symantec, a software company that also works for enhancement of cyber security, about ranking of the countries that faced cyber threats in 2017. India was ranked at third number in the world regarding detection of cybercrimes and in terms of spam, phishing and targeted cyber-attacks, India is at second number.[312] The cyber security report issued by Norton Life lock[313] in 2019 has revealed that about Rs. 1.2 trillion have been stolen from Indians by cybercriminals and most of the Indians do not have adequate knowledge about actions to be taken in case of such cybercrime incidents.[314] These reports indicate that the present legislation is not enough to deal with the increasing cybercrimes in India therefore the law must be amended and stricter and up to date laws be passed to protect the country from cybercrimes.

4.2.2 Cybercrime Laws of Bangladesh

Use of internet began in Bangladesh in 1993[315] while it was introduced in the neighboring states of India in 1986 [316] and Pakistan in 1995 [317]. As compared to these countries, there were a little number of users and only two service providers in

[311] *Syed Asifuddin and Others V. State of Andhra Pradesh and Another,* 2005 CrLJ 4314.
[312] Dr. V. Henry Jerome, *Cybercrime Victimization* (Delhi: Blue Rose Publications, 2021), 9.
[313] A cyber security company of the US. "Corporate Profile", *Norton LifeLock,* accessed 15 March,2022. https://www.nortonlifelock.com/us/en/corporateprofile/
[314] Jerome, *Cybercrime,* 11.
[315] Md. Abu Hanif, "Cybercrime and Cyber Law: Growth of the State Concerns and Initiatives in Bangladesh", *Journal of Logistics, Informatics and Service Sciences* 5: 2 (Biannual, 2018), 20, accessed 20 March, 2022. ISSN 2409-2665
[316] Aiswarya Vijayan, "Digital India: A Roadmap to Sustainability", *International Journal of Innovative Technology and Explaring Engineering* 8: 5 (Monthly, March, 2019), 571. ISSN: 2278-3075, Volume-8 Issue-5 March, 2019
[317]Shaukat, "Developments", 260.

Bangladesh[318] but the increasing usage of information technology created cybercrimes in Bangladesh in the same style as it happened in Pakistan and India. To overcome this problem, Bangladesh also took measures through legislations. Most notable example of these attempts is The Information and Communication Technology Act (ICT), 2006 passed to promote and facilitate information technology in Bangladesh. This legislation has tried to cover all possible cybercrimes and provided a legal remedy to the cybercrime victims. The law is not only applicable to Bangladesh but its scope is also extended to cybercrimes executed outside Bangladesh. Certain rules to regulate Information and Communication Technology in Bangladesh were enacted in 2010 and ICT Act, 2006 was amended in 2013.

Another important step was taken by the Government of Bangladesh in 2013, with the setting up of "Special Tribunal" under ICT Act, 2006 to deal with cybercrimes in a speedy manner.[319] In order to increase the compatibility of cyber laws in the country by the addition of new laws for digital crime identification, Digital Security Act, 2018 was passed.[320] The cybercrimes ratio is also increasing with the increase in internet users in Bangladesh[321] so the need for more comprehensive laws is also a requirement of the changing circumstances.

India and Bangladesh both have made cybercrime laws and also trying to overcome the cybercrime threat although they also haven't reached the standard needed to deal with such crimes. Global Cybersecurity Index (GCI) of 2017 has placed

[318] Hanif, "Cybercrime, 20-21

[319] Hanif, "Cybercrime", 23-24.

[320] Kudrat-E-Khuda (Babu), "Cyber Property Rights, Its Present Status and Challenges: Bangladesh Context", *International Journal on Emerging Technologies* 11: 2 (Biannual, 2020), 739.

[321] Ibid.

India and Bangladesh at 23rd and 53rd position respectively while Pakistan stands at 66th[322] making it evident that Pakistan lags behind from India and Bangladesh both.

4.3 Application and Use of Cyber Technology in Pakistan

Pakistan is a developing country with limited resources. At the time of independence from British, there was no concept of using a computer even there was no electric typewriter in Pakistan. All the office work was done manually and the official records were maintained through manual typewriters. Telephone and telegram were the only modern means of communication in the country.[323] Computer was used for the first time in 1957 by "Packages Ltd" becoming the pioneer of Information Technology (IT)revolution in the country.[324] With the passage of time, Government of Pakistan gave incentives and application of computer began in important governmental departments.[325] The banking sector including Muslim Commercial Bank, Habib Bank and United Bank started using computer in 1965.[326] With the reduction in import duties on hardware and software, large scale computer usage began in the country since 1985 and people started using computers in their offices. Real IT revolution in Pakistan can be seen in early 90's with the removal of custom duties on computers. Provision of internet facility started in 1995 and since then the usage of computer and information technology is increasing at a faster rate in Pakistan. This development of

[322] Muhammad Riaz Shad, "Cyber Threat Landscape and Readiness Challenge of Pakistan", *Strategic Studies* 39: 1 (Quarterly, 2019), 15.

[323] Shaukat, "Developments", 259-260.

[324] Muhammad Shaukat, Muhammad Zafarullah, and Rana Abdul Wajid. "Information Technology in Pakistan: An Analysis of Problems Faced in IT Implementation by Pakistan's Banking and Manufacturing Companies", *Pakistan Journal of Social Sciences* 29: 1 (Biannual, June 2009), 14.

[325] Shaukat, "Developments", 260.

[326] Shaukat, Zafarullah and Wajid, "Information", 14.

IT sector has benefited and affected all fields of life in Pakistan. Government of Pakistan is also focused to promote IT sector by funding and establishment of institutes in the country.[327] It has also formed a separate ministry to deal with Information Technology.[328]

The application of cyber technology in different fields has created both positive and negative impacts. Pakistan is also facing different categories of cybercrimes like rest of the world. The issue of terrorism is the most challenging for the country and use of cyber space by terrorists has added fuel to the fire and increased difficulties for Pakistan. The terrorists' attacks in Pakistan since it has begun active cooperation with the US and use of cyber technology by the terrorists is an important instance of the danger faced by Pakistan.[329] Other categories of cyber threats faced by Pakistan consist of hacking, computer malware, and identity theft.[330] India is always seeking for an opportunity to hack computer system of Pakistan, for instance India hacked more than 36 official websites of Pakistan including website of Pakistan Navy.[331] Despite its limited resources, Pakistan has been successful in corresponding to these Indian attacks.[332]

4.3.1 Examples of Cybercrimes Experienced by Pakistan

The need for effective cybercrime legislation and competent policies to secure the cyberspace of Pakistan from international cyber-attacks can be clearly understood by some examples of cyber-attacks either on the national institutions or through leakage

[327] Shaukat, "Developments", 260.
[328] Ibid, 261.
[329] Adil Adeel and Rafi us Shan, "Global Cyber Terrorism: Pakistan's Cyber Security in Perspective", *Pakistan Journal of Terrorism Research* II: I (Bianuual, Jan-June, 2020), 128.
[330] Shad, "Cyber Threat", 9-14.
[331] Muhammad Shabbir, "Cyber Security in Pakistan: Emerging Threats and Preventive Measures", *The Journal of Governance and Public Policy* VI: II (Biannual, 2013), 30.
[332] Ibid.

of personal informational of national leaders. The most recent example is the audio leak of conversation between present Pakistani Prime Minister Shahbaz Sahrif and a government official on 24 September, 2022.[333] Despite the contents of conversation, the matter of audio leak of a high Pakistani official from his official phone is a serious threat to Pakistan's security.

An investigation on spy leaks conducted in 2021 by different international news agencies including The Guardian and The Washington Post revealed hacking of mobile phones of more than 50,000 people around the globe including Pakistan's the then Prime Minister Imran Khan's phone. It was claimed that the hacking was conducted by Pegasus, a spyware made by Israel.[334] This incident raised a question at the world's security systems regarding their leaders and important officials.

The virtual currency (crypto currency) fraud committed in Pakistan in 2021 is an important instance of fraud committed through use of cyber space. A large number of people had invested in these currencies through mobile Apps but these Apps stopped working in December, 2021 causing loss of more than Rs. 17.7 billion after which people contacted FIA or spread the matter through social media.[335] Another noteworthy example is the effort to create anarchy in Pakistan by India is the 2k tweets on two hours making '#CivilWarinPakistan' as the top trendy tweet. This

[333] Zulqernain Tahir, "PM's Purported Audio Reveals Request to 'Facilitate' Relative", *DAWN,* 25 September, 2022. https://www.dawn.com/news/1711847

[334] Craig Timber et al., "On the List: Ten Prime Ministers, Three Presidents and a King", *The Washington Post,* 20 July, 2021. https://www.washingtonpost.com/world/2021/07/20/heads-of-statepegasus-spyware/

[335] Imtiaz Ali, "Crypto Firm in FIA Crosshairs over Rs17.7bn scam", *DAWN,* 08 January, 2022. https://www.dawn.com/news/1668228

trend was initiated from India after the protests of Tehreek-e-Labbaik, a religious cum political party, in April, 2021 with the intention to create chaos in Pakistan.[336]

In order to understand the cyber security measures of Pakistan to deal with the cyber threats faced by Pakistan at national and public level, legislation alone is not the solution. Some other practical steps including formation of institutions or forces to deal with cybercrimes are also needed to support the law. Coming sections are a detailed account of the steps taken by Pakistan to deal with cybercrimes along with the problems faced in this process.

4.4 Cybercrime Legislation in Pakistan

The increasing trend of usage of information technology in almost every field of life in Pakistan, including banking sector, educational field, trade and many other fields as well, has given rise to new security challenges. In order to meet these challenges, Pakistan is taking necessary steps to make a comprehensive Cybersecurity network.[337] Guidelines for developing countries have been provided by the European Union's Convention on Cybercrime. Pakistan has considered the Convention as a guiding model while framing the Electronic Transaction Ordinance, 2002 on account of its being the only international effective piece of legislation to be followed.[338] The Electronic Transaction Ordinance, 2002 is the first attempt to regularize cyber transactions in Pakistan along with some other laws of British era were also made operative in Pakistan to manage telecommunication sector. Present section deals with

[336] Muhammad Nadeem Mirza and Muhammad Shahzad Akram, "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare", *Strategic Studies* 42: 1 (Quarterly,
[337] Aamna Rafiq, "Challenges of Securitising Cyberspace in Pakistan", *Strategic Studies* 39: 1 (Quarterly, 2019), 95.
[338] Zahid. "Global Fight", 109-110.

the cyber laws implemented in Pakistan including pre-independence and post-independence era.

4.4.1 Pre-Independence Cyber Laws

Before independence, telephone and mostly telegraph were important means of communication of information. [339] The Telegraph Act, 1885 and the Wireless Telegraphy Act, 1933 were promulgated to safeguard people from the abuse of these inventions in communication technology.[340] The basic objective of Telegraph Act was to provide power to Government or the license holder to manage the placement and management of telegraph lines.[341] The Wireless Telegraphy Act was made with the objective of managing the possession and use of wireless telegraphy devices that is applied for wireless communication and not otherwise. The law also makes it obligatory to get a license for keeping and controlling a wireless communication device and prescribes procedure for issuance of such permit.[342] These two laws helped in prevention of crimes through telegraph and telephone, the initial inventions of the modern telecommunication devices. These laws were adopted by the new dominions of India and Pakistan without alterations although amended later.

4.4.2 Post-Independence Laws

The modern trend of cybercrimes started in Pakistan with the advent of computer and internet technology in the country after 1990's that made it necessary to make laws in

[339] Shaukat, "Developments", 260.

[340] Joseph Wilson, "Liberalizing the Telecommunications Sector: Making Pakistan an Information Economy Final Report", *LIRNE Asia Six Country Multi-Component Study 2006-07* (2007), 4, accessed 10 April, 2022. https://lirneasia.net/wp-content/uploads/2007/10/wilson-

[341] Ibid

[342] "Wireless Telegraphy Act 1933", *Pakpost,* accessed 03 March, 2022. https://www.pakpost.gov.pk/pdfForms/25-04-2020-The-Wireless-Telegraphy-Act-1933-pdf.

order to control cybercrimes in Pakistan. In order to regulate use of cyber technology and to protect the consumers and service providers from any abuse, President of Pakistan issued an Ordinance titled "Electronic Transaction Ordinance, 2002" (ETO). The basic objective of the issuance of this first legislative instrument was to provide recognition to electronic transactions, records and documents along with providing a proper procedure for official recognition of the service providers.[343] An analysis of the Preamble of ETO makes it clear that the said Ordinance had no intention to criminalize cybercrimes rather the scope was limited to electronic transactions without leaving space for newly emerging cybercrimes. [344] The Ordinance gave full recognition to e-documents and different laws including Qanun-e-Shahadat Order, 1984 was amended to give evidentiary value to e-documents. [345] Although the Ordinance could never reach the status of an Act of parliament and had a limited scope, it provided a good example and approach for future cybercrime legislations.[346]

4.4.2.1 Cyber Laws of 2007

In 2007, the need for a specific cyber law was felt that resulted in promulgation of an Ordinance to deal with electronic crimes and an Act of Parliament for safety from online frauds. The President of Pakistan promulgated the "Prevention of Electronic Crimes Ordinance, 2007" making it the first legislation in Pakistan to specifically deal with cybercrimes. This Ordinance was a detailed legislative attempt to deal with newly emerging cybercrimes. Like the previous Ordinance ETO, 2002, it also failed

[343] "ETO", *Pakistan Law*, accessed 04 March, 20022. https://www.pakistanlaw.com/eto.pdf

[344] Nadia Khadam, "Seriousness towards Cyber Crime Laws in Pakistan", *The News*, 20 August, 2016.https://www.thenews.com.pk/print/143812-Seriousness-towards-cyber-crime-laws-inPakistan.

[345] Munir, "Electronic", 193.

[346] Umair Pervaiz Khan and Muhammad Waqar Anwar, "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward", *Cyberpolitik Journal* 5: 10 (Biannual, Winter 2020), 208-10.

to become an Act of parliament and was repealed in 2009. After its annulment, cyber related issues again started to be dealt under ETO, 2002[347] leaving room for an effective legislation to be made in Pakistan to deal with cybercrimes.

The Parliament passed law in 2007 to deal with only one specific category of cybercrimes instead of adopting a comprehensive cyber law. The Payment and Electronic Fund transfer Act, 2007 deals with only a specific area of money transfer through electronic devices like debit cards and ATMs. The Act provides supervision and regulation of electronic money transfers within Pakistan providing protection to the consumers and determines the rights and obligations of the Service Providers and the consumers.[348]

4.4.2.2 The Prevention of Electronic Crimes Act (PECA), 2016

The Prevention of Electronic Crimes Act, 2016 (PECA) is the outcome of 18 months of hard work by legal practitioners and IT experts.[349]The basic purpose of the law is to provide protection against unsanctioned access, use and transmission of computer data and its related technology and to criminalize such acts. Different categories of cybercrimes have also been dealt by prescribing punishments for the crimes [349] including spoofing, hate speech, spamming, cyber stalking, child pornography, attempt to endanger modesty of any person, online fraud, unauthorized use and manipulation of computer and its data and many other crimes as well. The law also declared it offensive to make, supply or obtain any device for using in cybercrimes. Formation of an institution to deal with cybercrimes was also proposed

[347] Khadam, “Seriousness towards Cyber Crime”.

[348]“Documents”, *State Bank of Pakistan*, accessed 04 March, 2022. https://www.documents.pk/file/State%20Bank%20of%20Pakistan%20(SBP)%20-%20Payment%20Systems%20and%20Electronic%20Fund%20Transfer%20Act%202007.pdf [349] Khan and Anwar, “Cybersecurity”, 208-10.

[349] Rafiq, “Challenges”, 95.

in the legislation.[350] The PECA, 2016 acts a guide for the Cybercrime Wing (CCW) formed as a result of the Act. CCW directly receives the complaints through its complaint desk and takes effective action being the only competent authority of its kind in the country. Different Governmental departments have also been guided and helped by CCW to increase their capacity of dealing with cybercrime threats.[351] Cooperation with international community for the purpose of prevention from cybercrimes has also been emphasized by the said Act.[352] Although said law is an excellent attempt and much needed legislation for the country but it has been hotly debated by different sections of society declaring it an attack on freedom of speech and expression guaranteed by Article 19[353] of the Constitution of Pakistan. Section 37 of PECA, 2016 has given powers to PTA to delete all kinds of online content that comes within the category of hate speech, online harassment or extremism. The adversaries of the Act state that Article 19 has been left at the will of PTA who will decide what kind of freedom of expression is allowed and which is not.[354] There is a need to remove this ambiguity by making some more amendments in the law as some restriction on freedom of expression is needed keeping in view the situation of extremism and hatred in the country.

[350] "Documents", *National Assembly of Pakistan,* accessed 03 March, 2022. https://na.gov.pk/uploads/documents/1472635250_246.pdf.

[351] "Cybercrime Wing", *FIA,* accessed 04 March, 2022. https://fia.gov.pk/ccw

[352] "Documents", *National Assembly of Pakistan,* accessed 03 March, 2022. https://na.gov.pk/uploads/documents/1472635250_246.pdf

[353] Article 19 of the Constitution of Pakistan state: Every citizen shall have the right to freedom of speech and expression, and there shall be freedom of the press, subject to any reasonable restrictions imposed by law in the interest of the glory of Islam or the integrity, security or defense of Pakistan or any part thereof friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, [commission of] or incitement to an offence.

[354] Farieha Aziz, "Pakistan's Cybercrime Law: Boon or Bane?" *BOELL,* 14 February 2018. https://www.boell.de/en/2018/02/07/pakistans-cyber-crime-law-boon-or-bane

4.4.2.3 Pakistan Electronic Crimes Ordinance, 2022

An important recent development in cybercrime laws of Pakistan is amendment in PECA, 2016 by promulgation of an Ordinance on 18 February, 2022. It is titled as Pakistan Electronic Crimes (Amendment) Ordinance, 2022 and promulgated with the objective of bringing a halt to online defamation. Section 20 of PECA 2016 has been amended making online defamation as a cognizable, non-bail able offence. A new Section 44-A[355] has also been inserted in the Ordinance with the purpose of speedy trial in the High Court. Federal Law Minister Farogh Naseem commented on the law and declared the law as an upright measure to stop fake news.[356] The Ordinance has been severally criticized by lawyers, political parties and media organizations.[357] The basis of criticism is mostly based on Section 20 as the amendment has made a critique of the fake news and a person making such a comment can be arrested without warrant and jailed for five years without having a chance of getting bail.[358] The Ordinance was declared as draconian law and has been challenged in Islamabad High Court and Lahore High Court on 21 February, 2022.[359] Islamabad High Court announced its decision on 08 April, 2022 and declared the said Ordinance as unconstitutional on grounds of having violated the fundamental rights provided by the Constitution of

[355] Title of Section 44-A of PECA Ordinance - Timeline to conclude the trial and supervision by the High Court.

[356] Naveed Siddiqui, "President Promulgates Ordinance to Regulate Social Media as Minister Warns Against Indulging In 'Fake News'", *Dawn,* 20 February, 2022. https://www.dawn.com/news/1676116

[357] News Desk, "PECA Ordinance Draconian in Present Form: AGP Khalid Javed Khan", *The News,* 23 February, 2022. https://www.thenews.com.pk/print/935956-peca-ordinance-draconian-inpresent-form-agp.

[358] Sadaf Khan, "PECA, The Powerful, and the Petty", *The News,* 22 February, 2022. https://www.thenews.com.pk/print/935630-peca-the-powerful-and-the petty

[349] News Desk, "PECA Ordinance Draconian".

Pakistan.[360]

4.5 Steps Taken by Pakistan to Deal with Cybercrimes

The cybercrime incidents faced by the world at different intervals of time[361] have instigated the international community to make laws and other practical steps as discussed earlier. Pakistan, also exposed to cyber threats, is trying to deal with cybercrimes by taking effective measures despite many challenges faced by it.

4.5.1 Formation of the Cybercrime Wing (CCW)

Federal Investigation Agency (FIA), initially formed under FIA Act, 1974[362] for dealing with smuggling, offences related to currency, immigration, passport, narcotics and other crimes of serious nature,[363] widened its scope and created a special department to deal with cybercrime threats named as "Cybercrime Wing (CCW)" formed in 2007. It was the first step towards formation of a specialized department to deal with cybercrime incidents. Section 29 of the Pakistan Electronic Crimes Act, 2016 has mandated the federal government to either establish or designate a law enforcement agency for investigation of offences under this law. The government, through the Prevention of Electronic Crimes Investigation Rules, 2018, designated the Federal Investigation Agency (FIA) for this purpose. At present, Pakistan Electronic Crimes Act, 2016 acts as a guiding law for the CCW. The Wing directly receives the complaints through its complaint desk and takes

[360] Awais Yousafzai, "PECA Ordinance Declared Unconstitutional by IHC", *The News,* 08 April, 2022. https://www.thenews,com.pk/latest/498485-peca-ordinance-declared-null-by-ihc

[361] Sadia Rasool, "Cyber Security Threat in Pakistan: Causes Challenges and Way Forward", *Elixir Social Studies* 89 (Monthly, 2015), 37237.

[362] The Act was passed with the purpose of formation of a Federal Agency in order to investigate crimes related to foreigners, Smuggling, Narcotics, Currency Offences and the crimes related to provincial jurisdictions. "Act", *FIA,* accessed 05 March, 2022. https://www.fia.gov.pk/act

[363] "About", *FIA,* accessed 04 March, 2022. https://fia.gov.pk/about

effective action being the only competent authority of its kind in the country. Different Govemmental departments have also been guided and helped by the CCW to increase their capacity of dealing with cybercrime threats.[364]

4.5.2 National Response Centre for Cybercrimes (NR3C)

Another important achievement by FIA is the formation of National Response Centre for Cybercrime (NR3C). The basic purpose of establishment of NR3C is a competent cyber law enforcement agency that provides exceptional digital forensic facilities making itself a role model for the police force. The center conducts seminars, workshops and provides training to different sectors of society in the area of cyber security. Most important initiative taken by NR3C is the creation of "Cyber Scouts" with the objective of providing training to students of dealing with computer emergencies.[365] The effectiveness of NR3C has lessened due to ignorance of people about cyber laws and the procedure to file complaints in such incidents.[366] Despite these problems, the center is playing an effective role in the fight against cybercrimes by helping different organizations in building cyber security strategy for them.

4.5.3 National Center for Cyber Security (NCCS)

In 2018, Govemment of Pakistan took an important step towards an effective policy against cybercrimes by establishment of National Centre for Cyber Security (NCCS). This project is a joint venture of Higher Education Commission and Planning Commission. The aim of this project was the fonnation of Research and Development (R&D) labs in selected universities of Pakistan[367] with the objective of securing Pakistan's cyber space from cybercriminals with the help of skilled professionals.

[364] "Cybercrime Wing", *FIA*, accessed 04 March, 2022. https://fia.gov.pk/ccw
[365] "About Us", *NR3C*, accessed 04 March 04, 2022. https://nr3c.gov.pk/about_us.html
[366] Rasool, "Cyber Security", 37238.
[367] *NCCS*, accessed 05 March, 2022. https://www.nccs.pk/

Other objectives include creating cyber awareness by holding workshops and conferences about cybercrimes and cyber security.[368] Till date NCCS has setup its labs in eleven universities of Pakistan and is effectively imparting knowledge and creating experts in the field of cyber security.[369]

4.5.4 Computer Emergency Readiness Team (CERT) Portal by PTA

An important initiative has been taken by PTA to counter cyber threats with the publication of updated regulations titled as "Critical Telecom Data and Infrastructure Security Regulations, 2020". The basic purpose of these regulations is to provide security to its license holders and to protect telecom data of the state.[370] In order to achieve these objectives, PTA has established CERT portal[371] in April, 2021 for its license holders.[372] This portal shall help in the improvement of security standards of Telecom Sector and safety of National Telecom Data and its infrastructure[373]. Initially, the Telecom license holders shall be facilitated and guided by PTA about emerging cyber security trends.[374]

4.5.5 National Cyber Security Policy, 2021

The Government of Pakistan has approved a National Security Policy, 2021 in order to take stern action regarding cyber-attacks on government departments declaring it

[368] "Objectives", *NCCS*, accessed 05 March, 2022. https://www.nccs.pk/nccs/nccs-objectives

[369] "Academic Partners", *NCCS*, accessed 05 March, 2022. https://www.nccs.pk/collaborations/academic-partners

[370] "Critical Telecom Data", *PTA*, accessed 05 March, 2022. https://www.pta.gov.pk/assets/media/critical_telecom_data_reg_20112020.pdf

[371] The portal was established for sharing of information between PTA and its consumers about latest cyber threats and security alerts. "Media Center", *PTA*, accessed 08 March, 2022. https://pta.gov.pk/en/media-center/single-media/pta-launches-cert-portal-for-telecom-industry--050421

[372] "Media Center", *PTA*, accessed 08 March, 2022. https://pta.gov.pk/en/media-center/singlemedia/pta-launches-cert-portal-for-telecom-industry--050421

[373] Mehtab Haider, "PTA Launches CERT Portal for Telecom Sector", *The News*, 06 April,

as attack on national sovereignty. Two steps have been intended to be taken to guarantee proper execution of the Security Policy. First step is the formation of Cyber Governance Policy Committee and the other step is the order to FIA for establishing a Cyber Patrolling Unit (CPU) to be entrusted with the task of keeping an eye on emerging trends of cybercrimes and cyber security across the globe.[375]

4.5.6 Collaboration of FIA with State Bank of Pakistan

State Bank of Pakistan also plays an important role to deal with online frauds and money laundering. A meeting was hosted by Governor of State Bank of Pakistan with FIA and Presidents of other banks to discuss the issue on 20 November, 2021. In a press release issued by External Relations Department of the State Bank of Pakistan, it was notified that the Governor of State Bank of Pakistan emphasized on the need for close cooperation of all institutions. Director General FIA offered support in strengthening cyber security at banks and suggested that the banks should carry out Information Security (IS) audit of their systems. The suggestion was welcomed by the Governor of State Bank of Pakistan and said that audit is regularly carried out by the banks however the suggestions by FIA will be taken into consideration. Different steps for strengthening cooperation were also discussed at the meeting.[376]

Apart from the above mentioned endeavors by the Government of Pakistan, private sector is also contributing in this battle against cybercrimes and many public-private ventures have been undertaken by provision of guidelines by the

[375] Akhtar Ali Shah, "Cybersecurity through Laws in Pakistan", *Tribune*, 17 November, 2021. https://tribune,com.pk/story/2329721/cybersecurity-through-laws-in-pakistan

[376] "External Relations Department: State Bank of Pakistan", *SBP*, accessed 09 March, 2023. https://www.sbp.org.pk/press/2021/Pr-20-Nov-2021.pdf

Government in this regard. Lawyers' community is also participating and some lawyers have made NGO's to enhance public knowledge regarding cyber security and cybercrimes. But these efforts cannot be declared as large scale efforts and major task of cyber security is placed on the shoulders of Public sector.

4.6 Challenges Faced by Pakistan

Continuous efforts to deal with the fast changing trends of cybercrimes are in progress but the problems faced during this struggle are massive in number making it difficult for the developing states to deal with the issue as effectively as developed countries are dealing. Pakistan is also faced with the cybercrime threat, and increasing use and application of information technology has led to more sophisticated crimes. Although Government of Pakistan is making efforts to deal with cybercrimes but lack of information and resources have proved important hurdles in this struggle. This section deals with the challenges faced by Pakistan to combat cybercrimes.

4.6.1 Insufficient Cyber Laws

Pakistan is making laws from time to time to increase cyber security structure of the state but consistently changing cybercrime trends have made it very difficult for the laws to effectively deal with newly emerging cybercrimes. Pakistan is facing many types of security threats at one time which make it difficult for the government to keep cyber security as a priority.[377] National Cyber Security Policy, 2021 acknowledges insufficiency of existing cyber legislations to cope with increasing threats of cybercrimes. Government of Pakistan aims at adopting an adequate mechanism to amend existing laws to protect digital assets of the state.[378]

[377] Khan and Anwar, "Cybersecurity", 207.

[378] "National Cyber Security Policy, 2021", *MOITT*, accessed 05 March, 2022. https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Fina l.pdf

4.6.2 Lack of Institutional Structure and CERTs to Deal with Cybercrimes

Comprehensive infrastructure comprised of substantial network of institutions play an important role in effective cyber security policy. Pakistan has entrusted the task of dealing with cybercrimes mainly to FIA which has created special departments to deal with cybercrimes.[379] In addition to this, different universities have been entrusted with the task of educating students and organization in IT security areas. [380]These topics have been discussed in detail in the previous section. PTA has also given an initiative of formation of CERT[380] to stop cyber threats but such CERTs are needed at large scale to counter the problem. Although Pakistan is making efforts to strengthen its Cyber security but the trans-border, ever changing nature of the crime demands establishment of more organizations to deal with the issue in a competent manner.

4.6.3 Imperfections in Judicial System

A proper judicial system encompassing updated system of investigation free of political influence is an important element in successful implementation of cyber laws in the country.[381] Lack of unblemished democratic system in Pakistan has influenced investigative and judicial process as well creating difficulty in FIRs, hurdles in investigations and awkward delays of cases by the judges. All these factors combine to form an imperfect judicial system resulting in problems in cybercrime investigations.[382]

[379] “About Us”, *NR3C,* accessed 04 March, 2022. https://nr3c.gov.pk/about_us.html

[379]*NCCS*, accessed 05 March, 2022. https://www.nccs.pk/

[380] Haider, “PTA Launches CERT”.

[381] Ghulam Muhammad Kundi, Allah Nawaz and Robina Akhtar, “Digital Revolution, CyberCrimes and Cyber Legislation: A Challenge to Governments in Developing Countries”, *Journal of Information Engineering and Applications* 4: 4 (2014), 68, accessed 10 March, 2022. ISSN 2224-5782 [382] Khan and Anwar, “Cybersecarity”, 206.

[382] Kundi, Nawaz and Akhtar, “Digital Revolution”, 68.

4.6.4 Lack of Private Sector's Support

A successful cyber security policy can only attain its objectives with the cooperation of public and private sector. In Pakistan, the burden of having a fool proof cyber security framework lies on the shoulders of Government on account of lack of support from private sector. Government helps the private sector and financially supports them to build an effective cyber security network. This task has been entrusted to NR3C under FIA and a non-government agency named as Pakistan Information Security Association (PISA). The basic aim of PISA is to promote awareness among people of Pakistan about cyber security and laws.[383] These two entities guide and support the private sector leaving them mainly responsible for the task of cyber security. Effective measures are needed to increase financial and technical cooperation by private sector to join hands in this struggle against cybercrimes. In addition to this, an effective cooperation between military and civil agencies is also needed to strengthen the cyber security infrastructure of Pakistan. [384]

4.6.5 Use of Cyber Space by Terrorist Organizations

Pakistan is subject to terrorists' attacks after it has joined hands with the international community in fight against terrorism. It has lost thousands of precious civilian and military lives leaving behind grief and sufferings for their families. The advancements in information technology have benefitted the terrorist organizations to preach their propaganda and communicate with each other without physical contact. The incident of Bacha Khan University in 2016 is an important example of cyber technology's usage by neighboring country as the planners of the incident were not present in Pakistan and they instructed the performers through information technology while

[383] "Home", *PISA,* accessed 10 July, 2022. https://www.pisa.org.pk/public/Home/index

[384] Khan and Anwar, "Cybersecurity", 208.

sitting at a far off place.[385] Along with, the terrorists sometimes hack important websites to achieve their goals either by putting some demands to the government or they deface the websites. Pakistan has also faced such attacks like hacking of 36 websites of Pakistani government by Indian hackers in 2010[386] as a response to Mumbai attacks. Similar incidents of website hacking happened in 2014 when website of Lahore High Court was defaced[387] and in 2019 when website of Pakistan Foreign Ministry became inaccessible in many countries.[388] Although such attacks happen on both sides of border but Pakistan needs to pay more attention to the issue as Pakistan is facing the dual danger of terrorism from India and Afghanistan both.

4.6.6 Lack of Public Awareness and Identity Theft

In the way of implementation of an effective policy to counter cybercrimes, Pakistan faces another important problem of lack of public awareness about data protection. This lack of awareness gives rise to identity theft [389]and the public becomes prey of the cybercriminals who steal their identity causing huge financial damage to the victims. In 2019, a large scale data theft occurred when data was stolen from Punjab Information Technology Board causing damage to millions of citizens. In Pakistan, citizens' records are managed and kept by National Database & Registration Authority (NADRA) but identity theft occurs when data is linked with some government projects[390] and data is stolen by hacking their website or people give their

[385] Khan and Anwar, "Cybersecurity", 206-7.

[386] Jahanzaib Haque, "Cyber Warfare: Indian Hackers Take Down 36 Govt Websites", *Tribune,* 01 December, 2010. https://tribune.com.pk/stroy/84269/cyber-warfare-indian-hackers-takedown-36-govt-websites

[387] Ibid, 208.

[388] Naveed Siddiqui, "Ministry of Foreign Affairs Website Hacked, Inaccessible in Several Countries", *Dawn,* 16 February, 2019. https://www.dawn.com/news/1464217

[389] Khan and Anwar, "Cybersecurity", 207.

relevant information to criminals suspecting them as officials. Banking sector of Pakistan is also faced with the threat of identity theft causing grave financial loss to banks and their customers. Even personal information of thousands of account holders of Pakistani Banks is accessible on Dark Web.[390]

4.6.7 Lack of Public Involvement in Legislative Process

A comprehensive legislation needs to be made with the suggestions and recommendations from all segments of society. In Pakistan, laws are made only with the involvement of ruling party and their favored bureaucrats resulting in objections and protests. PECA, 2016 is also objected on various grounds due to absence of coordination and assistance of different sections of society. Even some of the critics have declared the law as a tool to hamper freedom of speech and expression in the country.[391] Another example on non-involvement of public in cybercrimes legislation is the Pakistan Electronic Crimes (Amendment) Ordinance, 2022 which is being greatly protested all across the country.[392] The law has been challenged in the High Court and rejected as well so there is a need that the government should seek advice from different sections of society especially lawyers, judges and media persons while making cybercrimes legislation.

4.6.8 Technical Incompetency

The rapidly growing nature of cybercrimes has made it necessary for the states to adapt such a mechanism that can be updated without delay. Pakistan lacks the most updated mechanism to deal with cybercrimes that paves way for different cybercrimes

[390] Rafiq, "Challenges", 95.

[391] Khan and Anwar, "Cybersecurity", 207.

[392] News Desk, "PECA Ordinance Draconian".

including theft of data at the top. Such attack on data security can also result in great hardships to society.[393] Pakistan's 66th position[395] out of 193 countries according to GCI, 2017 makes it clear that Pakistan does not have the required international standards of technical competence to secure its cyberspace.[394] There is a dire need that Pakistan should deal with cyber threats as a priority to counter different emerging trends of cybercrimes especially cyber terrorism and cyber warfare.

4.6.9 Violation of the Right of Privacy

The citizens of Pakistan have been provided right of privacy through Article 41 (1)[395] of the Constitution of Pakistan. Many incidents of violation of right of privacy have been reported by Pakistani and international media including audio leak of telephonic conversation of Pakistani Prime Minister Shahbaz Sharif as discussed earlier. On 16 February, 2023 an audio of Supreme Court Judge was leaked[396] indicating violation of privacy despite being high officials of the country. There is a need of having rules and regulation to stop such violations to protect privacy of people

4.7 Conclusion

Cybercrimes are increasing at a faster pace with the increasing development of information technology. Pakistan is a developing state having limited resources to counter cybercrimes even then it is struggling to develop a comprehensive framework for dealing with different cybercrimes emerging due to increasing use of information

[393] "National Cybersecurity Policy, 2021", 4.

[395] Shad, "Cyber Threat", 15.

[394] Rafiq, "Challenges", 95.

[395] Article 14 (1) states: The dignity of man and, subject to law, the privacy of home, shall be inviolable.

[396] Nasir Iqbal, "SC judges take up audio leak involving brother judge", *DAWN*, 19 February, 2023. https://www.dawn.com/news/1737943

technology in the country. Pakistan lags behind from India and Bangladesh as evident from the GCI, 2017 so it is needed that Pakistan should take more steps to protect its cyber space from criminals and the rival states especially India who is always working to target Pakistan. Legislatives attempts in Pakistan cannot be ignored that started with the promulgation of Ordinances resulting in Prevention of Electronic Crimes Act, 2016 as presently working cyber law of the state. Recently an amendment has been made by Ordinance but it has been declared unconstitutional by the Islamabad High Court. To increase the efficacy of laws in the country, government has also created cybercrime departments giving the major responsibility to FIA that is burdened with loads of cases so there is need of institution building to deal with cybercrimes as independent branch of crimes. In addition to these efforts, public-private coordination is also required to educate people about cyber safety and enhancement of capacity building of public and private sector. Pakistan has adopted a successful policy to counter cybercrimes but more effort is required in this regard as the ever changing nature of cybercrimes has made it impossible for any country to claim that it has attained a perfect protection against the threat.[397]

[397] Shad, "Cyber Threats", 15.

CONCLUSION

In the present research, cybercrimes have been analyzed in detail keeping main focus on the steps taken by Pakistan to protect the country from threat of cybercrimes. The research has led to some suggestion followed by conclusion of the research.

Conclusion

Cybercrimes are developing at a fast pace with the advancements in information technology. The transnational and sophisticated nature of the crime requires adoption and application of updated strategies and the cooperation of international community in order to deal with the problem in an effective manner. Most important and dominant international achievement is the Council of Europe's Cybercrime Convention, 2001 that has also provided a guideline for developing countries while framing their national cybercrime laws. Some states like Russia do not recognize Cybercrime Convention but majority of the World's states follow and recognize it. Apart from the Convention, many organizations like the UN, the G-8, the European Union and the Common wealth are also playing important role by passing resolutions, holding conferences and creating special institutions to counter cybercrimes at international level.

Many problems are being faced by the states making it difficult for them to formulate effective international cybercrime policy to deal with the cybercrimes threat in the present day and future both. The challenges faced by international community have been tried to be resolved by application of different strategies having been discussed in detail. The international community is cooperating with each other to fight cybercrimes but the cybercrimes developing at fast speed with developed mechanism has created hardships thus international bodies are being set up with more stabilized tools and capabilities.

Pakistan lags far behind in cyber security measures of the world especially its neighboring states of India and Bangladesh. Cooperation with international community can also pave way for increasing the standard of intelligence organizations in the country as the experience and assistance by developed countries can be helpful to a developing country like Pakistan having limited resources and technical expertise. Although the government of Pakistan is taking special steps with the help and coordination of civil and military both but there is still a lot of work to be done in order to secure the cyber space of Pakistan.

Recommendations

Amendments should be made in different laws including Qanun-e-Shahadat Order and the Code of Criminal Procedure 1984. A separate chapter related to digital evidence, its collection, preservation, presentation in the courts and its acceptability should be added in Qanun-e-Shadat Order.Speedy justice mechanism must be introduced for victims of cybercrimes. Pakistan Penal Code must also be amended to add new offences and punishments dealing with the different categories of cybercrimes like web-jacking, spamming, virus attacks, e-mail frauds and many other newly emerging cybercrimes.

Amendment made under PECA, in 2016 is not sufficient until formation of special courts and adoption of separate procedure for cybercrime cases. A separate department and ministry should be created to deal with cybercrimes. Separate cybercrime courts should be established across the country at district level. The judges having comprehensive knowledge about cyber laws, cybercrimes should be appointed in these courts.

The law must provide an opportunity of being heard to the person accused of having done any act of hate speech, blasphemy or violation of any other's rights through internet. Such opportunities to express their views shall not only protect the accused from any injustice that can be caused if detained and not heard by the officials along with the trend of arrest of personal or political opponents without arrest warrant shall also come to an end. The absolute restriction of freedom of speech as imposed by Pakistan Electronic Communication (Amendment) Ordinance, 2022 did not prove effective so the cybercrime laws in Pakistan should be amended with the consent and assistance of the persons having expertise in legal and technical field to make comprehensive and acceptable law at the level of state.

Public-private coordination must be enhanced for increasing cyber security infrastructure of government and private organizations. In addition to this, such cooperation can also result in promoting awareness about cyber laws among their staffs and also among general public dealing with these organizations. Most of the people of Pakistan do not have knowledge about safety from cybercrimes so they become easy victims by identity theft, spamming and spoofing. General public should also be educated about cybercrimes and should be informed about ways of protection from such attacks. Media can also play an effective role in imparting such awareness among general public.

Computer is being taught in almost all institutions in Pakistan but the standard of IT education imparted by most of the institutions especially at the level of higher studies doesn't meet international standard required to produce skillful IT experts. There is a need to keep a check on the IT institutes to improve their standard of education. Judges, lawyers and law students should also be provided training to enhance their knowledge and capabilities about cybercrimes and its related areas. Let's start with cybercrime law and make it a part of the syllabus of LLB.

FIA has been burdened with the assignment of an additional task of cybercrimes. There is a need to add more work force in the FIA having legal and technical knowledge of cybercrimes so that FIA can handle cybercrimes in an efficient manner. The IT industry of Pakistan does not meet the international standards despite having fiber telecommunication infrastructure of international standard. There is a need to make new plans for development of IT hardware industry and up gradation of software industry to excel in this field.

Bibliography

Articles

Acello, Richard. "Technology: Feds Ready to Tackle Cybercrime: New Law Gives U.S. another Weapon". *ABA Journal* 95: 2 (Monthly, 2009), 37-37.

Adeel, Adil, and Rafi us Shan. "Global Cyber Terrorism: Pakistan's Cyber Security in Perspective". *Pakistan Journal of Terrorism Research* II: I (Biannual, JanJune, 2020), 119-141.

Afzal, Ayesha, and Aiman Asif. "Cryptocurrencies, Blockchain and Regulation: An Overview". *The Lahore Journal of Economics* 24: 1 (Biannual, Summer 2019),

Argomaniz, Javier. "European Union Responses to Terrorist Use of the Internet". *Cooperation and Conflict* 50: 2 (Quarterly, 2015), 250-268.

Arief, Budi, Mohd Azeem Bin Adzmi, and Homas Gross. "Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1 – Attackers". *IEEE Security & Privacy* 13: 1 (2015), 71-76.

Armstrong, H.L. "Denial of Service and Protection of Critieal Infrastructure". *Journal of Information Warfare* 1: 2 (Quarterly, 2001), 23-34.

Babu, Kudrat-E-Khuda. "Cyber Property Rights, Its Present Status and Challenges: Bangladesh Context". *International Journal on Emerging Technologies* 11: 2 (Biannual, 2020), 735-745.

Bainbridge, David I. "The Scope of Copyright Protection for Computer Programs". *The Modern Law Review* 54: 5 (Bimonthly, 1991), 643-63.

Bernat, Frances P., and David Makin, "Cybercrime Theory and Discerning if there is a Crime: The Case of Digital Piracy". *International Review of Modern Sociology* 40: 2 (Biannual, 2014), 99–119.

Billah, Muhammad Masum. "Sufficiency of Omani Laws to Suppress Cybercrimes in Light of the UN Comprehensive Study on Cybercrimes". *Arab Law Quarterly* 32: 2 (Quarterly, 2018), 158-84.

Brenner, Susan W. "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships". *North Carolina Journal of Law & Technology* 4: 1 (Biannual, Fall 2002), 1-50.

Burstein, Aaron. "A Survey of Cybercrime in the United States".*Berkeley Technology Law Journal*18: 1 (Quarterly, 2003), 313-38.

Calderoni, Francesco. "The European Legal Framework on Cybercrime: Striving for an Effective Implementation". *Crime, Law and Social Change* 54: 5 (Monthly, 2010), 339-357.

Cassim, Fawzia. "Addressing the Spectre of Phishing: Are Adequate Measures in Place to Protect Victims of Phishing?" *The Comparative and International Law Journal of Southern Africa* 47: 3 (Tri-annual, 2014), 401-28.

Cassim, Fawzia. "Formulating Specialised Legislation To Address The Growing Spectre Of Cybercrime: A Comparative Study". *Potchefstroom Electronic Law Journal* 12: 4 (Monthly, 2009), 36-79. ISSN 1727-3781

Clough, Jonathan. "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation". *Monash University Law Review* 40: 3 (Tri-annual, 2014), 698-736.

Crosston, Matthew. "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game". *Strategic Studies Quarterly* 6: 4 (Quarterly, 2012), 100118.

Enigbokan, Ok, and N Ajayi. "Managing Cybercrimes through the Implementation of Security Measures". *Journal of Information Warfare* 16: 1 (Quarterly, 2017), 112-29.

Fahey, Eliane. "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security". *European Journal of Risk Regulation* 5: 1 (Quarterly, 2014), 46-60.

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to address Cybercrime".*Homeland Emergency & Security Management* 10: 1 (Tri-annual, 2013), 1-27.

Furnell, S.M. "Categorising Cybercrime and Cybercriminals: The Problem and Potential Approaches". *Journal of Information Warfare* 1: 2 (Quarterly, 2001), 35-44.

Gervais, Michael. "Cyber Attacks and the Laws of War". *Journal of Law & Cyber Warfare* 1: 1 (Biannual, 2012), 8-98.

Gjelten, Tom. "First Strike: US Cyber Warriors Seize the Offensive".*World Affairs* 175: 5 (Quarterly, 2013), 33–43.

Gordon, Sarah, and Richard Ford. "On the Definition and Classification of Cybercrime". *Journal in Computer Virology* 2 (Quarterly, 2006), 13-20.

Grabosky, Peter. "The Evolution of Cybercrime, 2004-2014". *RegNet Research Paper* 58 (2014), 2-16.

Grabosky, Peter. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10: 2 (Bimonthly, 2001), 243-49.

Graves, James T., Alessandro Acquisti, and Ross Anderson. "Perception versus

Punishment in Cybercrime". *The Journal of Criminal Law and Criminology* 109: 2 (Quarterly, Spring 2019), 313-364.

Guinchard, Audrey. "Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy". *Journal of Strategic Security* 4: 2 (Quarterly, Summer 2011), 75-96.

Hanif, Md. Abu. "Cybercrime and Cyber Law: Growth of the State Concerns and Initiatives in Bangladesh". *Journal of Logistics, Informatics and Service Sciences* 5: 2 (Biannual, 2018), 11-41. ISSN 2409-2665

Hussain, Muzammil M. "Digital Infrastructure Politics and Internet Freedom Stakeholders after the Arab Spring". *Journal of International Affairs* 68: 1 (Biannual, 2014), 37-56.

Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau. "European Union and NATO Global Cybersecurity Challenges: A Way Forward". *PRISM* 6: 2 (Quarterly, 2016), 127-141.

Islam, Zia ul, Muhammad Aqeel Khan, and Muhammad Zubair. "Cybercrime and Pakistan". *Global Political Review* IV: II (Quarterly, Spring 2019), 12-19.

Jaffery, Callum, and Tobias Feakin. "Underground Web: The Cybercrime Challenge". *Australian Strategic Policy Institute* (2015), 1-16.

Jordan, Amy B. "Children's Media Policy". *The Future of Children* 18: 1 (2008), 235–53. http://www.jstor.org/stable/20053126.

Jamil, Zahid. "Global Fight against Cybercrime: Undoing the Paralysis". *Georgetown Journal of International Affairs*Cyber Issue II (Biannual, 2012), 109-20.

Kaman, Marilyn J., Craig Resnick, Mark Winston, and Bruce Zagaris. "International Criminal Law". *The International Lawyer*41: 2 (Quarterly, Summer 2007), 317-27.

Kaur, Er. Navneet. "Introduction of Cybercrime and its Types". *International Research Journal of Computer Science* 8: 5 (Monthly, August 2018), 435-39.

Khan, Umair Pervaiz, and Muhammad Waqar Anwar. "Cybersecurity in Pakistan: Regulations, Gaps and a Way Forward". *Cyberpolitik Journal* 5: 10 (Biannual, Winter 2020), 205-18.

Korai, Abdul Ghaffar, Abdul Samad, Ahad Ghaffar, Javed Ahmed and Imtiaz Ahmed Memon. "Cybercrime, Internet and Cybercrime Legislation: A study of Pakistan". *Psychology and Education* 57: 7 (Tri-annual, 2020), 118-27.

Kshetri, Nir. "The Simple Economics of Cybercrimes". *IEEE Security and Privacy* 4: 1 (Bimonthly, January/February, 2006), 33-39.

Kundi, Ghulam Muhammad, Allah Nawaz, and Robina Akhtar. "Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge to Governments in Developing Countries". *Journal of Information Engineering and Applications* 4: 4 (2014), 61-70. ISSN 2224-5782

Mehra, Salil K. "Law and Cybercrime in the United States Today". *The American Journal of Comparative Law*58: Suppl_1 (Quarterly, 2010), 659-85.

Mirza, Muhammad Nadeem, and Muhammad Shahzad Akram. "3-Cs of Cyberspace and Pakistan: Cyber Crime, Cyber Terrorism and Cyber Warfare". *Strategic Studies* 42: 1 (2022), 62-80.

Munir, Muhammad Amir. "Electronic Crimes Ordinance: An Overview of Its Preamble and Extent". *Pakistan Journal of Criminology* 2: 1 (Quarterly, January 2010), 189-202.

Munir, Asad, and Ghulam Shabir. "Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation".*Global Political Review* III: II (Quarterly, Fall 2018), 84-97.

Omer, Soran K. "The Role and Future of G8". *Journal of Process Management and New Technologies* 7: 1 (Biannual, 2019), 49-56.

Prince, Conrad, and James Sullivan. "The UK Cyber Strategy: Challenges for the Next Phase". *Royal United Services Institute* (Annual, 2019), 1-19.

Rafiq, Aamna. "Challenges of Securitising Cyberspace in Pakistan". *Strategic Studies* 39: 1 (Quarterly, 2019), 90-101.

Rasool, Sadia. "Cyber Security Threat in Pakistan: Causes Challenges and Way Forward". *Elixir Social Studies* 89 (Monthly, 2015), 37237-43.

Robert, Ebi. "Attempting a Definition of Cybercrime". (April 20, 2021), 1-5, accessed 15 February, 2022.http://ssrn.com/abstract=3830589.

Robertson, A.H. "The Council of Europe, 1949-1953: I". *The International and Comparative Law Quarterly* 3: 2 (Quarterly, 1954), 235-55.

Roos, Anneliese. "Core Principles of Data Protection Law". *The Comparative and International Law Journal of Southern Africa* 39: 1 (Tri-annual, 2006), 102–30.

Shabbir, Muhammad. "Cyber Security in Pakistan: Emerging Threats and Preventive Measures". *The Journal of Governance and Public Policy* VI: II (Biannual, 2013), 25-38.

Shad, Muhammad Riaz. "Cyber Threat Landscape and Readiness Challenge of Pakistan".*Strategic Studies* 39: 1 (Quarterly, 2019), 1-19.

Shaukat, Muhammad. "Developments of Information Technology, Telecom and ECommerce in Business Environment of Pakistan: An Analysis of Banking and Manufacturing Sectors".*Pakistan Journal of Social Sciences* 29: 2 (Biannual, December 2009), 259-78.

Shaukat, Muhammad, Muhammad Zafarullah, and Rana Abdul Wajid. "Information Technology in Pakistan: An Analysis of Problems Faced in IT Implementation by Pakistan's Banking and Manufacturing Companies".*Pakistan Journal of Social Sciences*29: 1 (Biannual, June 2009), 13-22.

Skibell, Reid. "Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act". *Berkeley Technology Law Journal* 18: 3 (Quarterly, 2003), 909-44.

Smith, Robert, and Mark Perry. "Fake News and the Convention on Cybercrime".*Athens Journal of Law* 7: 3 (Quarterly, July 2021), 335-358.

Sternberg, Sarah. "The Child Pornography Prevention Act of 1996 and the First Amendment: Virtual Antitheses".*Fordham Law Review* 69: 6 (Bimonthly, 2001), 2783-2823.

Sussmann, Michael A. "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium".*Duke Journal of Comparative & International Law* 9 (Tri-annual, 1999), 451-89.

Tabansky, Lior. "Cybercrime: A National Security Issue"?*Military and Strategic Affairs*4: 3 (December 2012), 117-136.

Vijayan, Aiswarya. "Digital India: A Roadmap to Sustainability". *International Journal of Innovative Technology and Exploring Engineering* 8: 5 (Monthly, March, 2019), 571-76.

Vecino, Jobel Kyle P. "United by Necessity: Conditions for Institutional Cooperation against Cybercrime". *The Cyber Defense Review* (Quarterly, Special Edition 2019), 123-44.

Verteşolteanu, Andreea. "Evolution of the Criminal Legal Frameworks for

Preventing and Combating Cybercrime".*Journal of Eastern-Europe Criminal Law* 1 (Biannual, 2014), 84-96.

Viktor, Sheshtak, and Koscheeva Darya. "Cyber Crime during the COVID-19 Pandemic: Key Trends and Ways to Solve the Problem".*Moscow: Institute of Legislation and Comparative Law* (October 20, 2021), 1-8.

Weber, Amalie M. "The Council of Europe's Convention on Cybercrime". *Berkeley Technology Law Journal* 18: 1 (Quarterly, 2003), 425-46.

Wilson, Joseph. "Liberalizing the Telecommunications Sector: Making Pakistan an Information Economy Final Report".*LIRNEAsia Six Country MultiComponent Study 2006-07* (August, 2007), 1-54.

Yamin, Tughral. "Cyberspace Management in Pakistan". *Governance and Management Review* 3: 1 (Biannual, 2018), 46-61.

Završnik, Aleš. "Cybercrime Definitional Challenges and Criminological Particularities".*Masaryk University Journal of Law and Technology* 2: 2 (Biannual, 2008), 1-29.

Books

Abbate, Janet. *Inventing the Internet.* Cambridge: Massachusetts Institute of Technology, 1999.

Aplin, Tanya, and Jennifer Davis. *Intellectual Property Law: Text, Case and Materials.* 2nd ed. Oxford: Oxford University Press, 2013.

Bidgoli, Hossein. *Handbook of Information Security.* vol. 1. New Jersey: John Wiley & Sons, 2006.

Blank, Andrew G. *TCP/IP Jumpstart: Internet Protocol Basics.* San Francisco: Sybex, 2002.

Bory, Paolo. *The Internet Myth: From the Internet Imaginary to Network Ideologies.*

London: University of Westminster Press, 2020.

Brenner, Susan W. *Cybercrime and the Law: Challenges, Issues and Outcomes.* Boston: North Eastern University Press, 2012.

Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace.* California: Praeger Publishers, 2010.

Carey, Peter. *Data Protection: A Practical Guide to UK and EU Law.* 3rd ed. Oxford: Oxford University Press, 2009.

Casey, Eoghan. *Digital Evidence and computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. Waltham: Elsevier Publishing, 2011.

Clough, Jonathan. *Principles of Cybercrime.* 2nd ed. Cambridge: Cambridge University Press, 2015.

Cross, Michael. *Scene of the Cybercrime.* 2nd ed. Burlington: Syngress Publishing, 2008.

Davidson, Alan. *The Law of Electronic Commerce.* New York: Cambridge University Press, 2009.

Dubrawsky, Ido. *How to Cheat at Securing Your Network.* Burlington: Syngress Publishing, 2007.

Erickson, Jon. *Hacking: The Art of Exploitation.*2nded. San Francisco: No Starch Press, 2008.

Gibson, Darril, and Andy Igonor. *Managing Risks in Information Systems.* 3rd ed. Burlington: Jones & Bartlett Learning, 2022.

Gillespie, Alisdair A. *Cybercrime: Key Issues and Debates.* New York: Routledge, 2016.

Grimes, Roger A. *Malicious Mobile Code: Virus Protection for Windows.* Sebastopol: O'Reilly Media, 2001.

Haggart, Blayne. *Copyfight: The Global Politics of Digital Copyright Reform.* Toronto: University of Toronto Press, 2014.

Hart, Jaffery A. "The G8 and the Governance of Cyberspace". In *New Perspectives on*

Global Governance: Why American Needs the G8, edited by MicheleFratianni, John J. Kirton, Alan M. Rugman, and Paolo Savona, 137152. Hampshire: Ashgate Publishing May 2005.

Hessick, Carissa Byrne. "Setting Definitional Limits for the Child Pornography Exception". In *Refining Child Pornography Law: Crime. Language and Social Consequences,* edited by Carissa Byrne Hessick, 57-80. Ann Arbor: University of Michigan Press, 2016.

Hill, Joshua B., and Nancy E. Marion. *Introduction to Cybercrime: Computer Crimes, Laws & Policing in the 21st Century.* Santa Barbara CA: Praeger Publishers, 2016.

Jerome, Dr. V. Henry. *Cybercrime Victimization.* Delhi: Blue Rose Publications, 2021.

Kshetri, Nir. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* Heidelberg: Springer Publishing, 2010.

Neil W. Netanel. "Why has Copyright Expanded? Analysis and Critique".In*New Directions in Copyright Law,* edited by Fiona Macmillan, 3-34, vol. 6. Cheltenham: Edward Elgar Publishing, 2007.

Mali, Prashant. *A Text Book of Cybercrime and Penalties.* Indiana: Repressed Publishing, 2006.

Manzoor, Amir. *E-Commerce: An Introduction.* Saarbrücken: LAP Lamburt Academic Publishers, 2010.

Mehan, Julie E. *Cyber War, Cyber Terror, Cybercrime and Cyber Activism.* 2nd ed.

Cambridgeshire: IT Governance Publishing, 2014.

Meyer, Susan. *Understanding Digital Piracy.* New York: Rosen Publishing, 2014.

Mishra, Akash Kamal. *An Overview of Cybercrime and Society.* vol. 1. Chennai: Xpress Publishing, 2017.

Moore, Robert. *Cybercrime: Investigating High-Technology Computer Crime.* 2nd ed. Oxon: Routledge, 2015.

Myers, Steven. "Introduction to Phishing".In *Phishing and Countermeasures,* edited by Markus Jakobsson and Steven Myers, 1-29. New Jersey: Wiley Publishing, 2007.

Norton, Joseph J. and George A. Walker. ed. *Banks: Fraud and Crime.* 2nd ed. Oxon: Routledge, 2000.

Porcedda, Maria Grazia. "Transatlantic Approaches to Cybersecurity and Cybercrime". In *The EU-US Security and Justice Agenda in Action*, edited by Patryk Pawlak, 41-54. Paris: European Union Institute for Security Studies, 2011.

Sandywell, Barry. "On the Globalisation of Crime: The Internet and New Criminality". In *Handbook of Internet Crime,* edited by Yvonne Jewkes and Majid Yar, 38-66, 2nd ed. New York: Routledge, 2011.

Smith, Cary Stacy, and Li-Ching Hung. *The Patriot Act: Issues and Controversies.* Illinois: Charles C. Thomas Publisher, 2010.

Theoharis, Athan G. "A Brief History of the FBI's Role and Powers". In *The FBI: A Comprehensive Guide,* edited by Athan G. Theoharis, Tony G. Poveda, Susan Rosenfeld and Richard Gid Powers, 1-48. Arizona: Oryx Press, 1999.

Tiller, James S. *A Technical Guide to IPSec Virtual Private Networks.* Boca Raton: CRC Press, 2001.

Weber, Rolf H., and Ulrike I. Heinrich. *Anonymization.* London: Springer Publishing, 2012.

Yar, Majid, and Kevin F. Steinmetz. *Cybercrime and Society.* 3rd ed. London: Sage Publications, 2019.

Yar, Majid. *Cybercrime.* 2nd ed. London: Sage Publications, 2013.

Yar, Majid. *Cybercrime and Society.* London: Sage Publications, 2013.

Case Laws

New York v. Ferber. 458 U.S. 747 (1982)

Osborne v. Ohio, 495 U.S. 103 (1990)

Syed Asifuddin and Others v. State of Andhra Pradesh and Another, 2005 Cri LJ 4314.

Statutes

The Child Abuse Victims' Rights Act, 1986

The Child Protection Act, 1984

The Child Sexual Abuse and Pornography Act, 1986

The Computer Fraud and Abuse Act, 1984.

The Computer Misuse Act, 1990

The Copyright Designs and Patent Act, 1988.

The Cybersecurity Information Sharing Act, 2015.

The Data Protection Act, 1984

The Data Protection Act, 1998

The Digital Security Act, 2018

The Economic Espionage Act, 1996

The Electronic Transaction Ordinance, 2002

FIA Act, 1974

The Identity Theft and Restitution Act, 2008

The Information and Communication Technology Act, 2006

The Information Technology Act, 2000

The Protect Act, 2003

The Protection of Children against Sexual Exploitation Act, 1977

The Telegraph Act, 1885

Pakistan Electronic Crimes Ordinance, 2022

The Payment and Electronic Fund transfer Act, 2007

The Prevention of Electronic Crimes Act (PECA), 2016

The US Patriot Act, 2001

The Wireless Telegraphy Act, 1933