CYBER CRIMES: A CASE STUDY OF LEGISLATION IN PAKISTAN IN THE LIGHT OF OTHER JURISDICTIONS.

A dissertation submitted in partial fulfillment of the requirements for the degree of LL.M (Corporate Law)

Submitted by:

Mahboob Usman

Registration no:

423-FSL/LLMCL/F13

Supervised by: **Syed Amjad Mahmood**

Department of Law

Faculty of Shariah and Law

International Islamic University Islamabad

2015/1437

Table of Contents

1. cyber-law and legislation

Bismillah

بسم الله الرحمن الرحيم

Dedicated to

My elder brother **Mohammad Asif**, who is a source of inspiration for me

Copyright

Approval Sheet

CYBER CRIMES: A CASE STUDY OF LEGISLATION IN PAKISTAN IN THE LIGHT OF OTHER JURISDICTIONS.

By

Mahboob Usman

Accepted by the Faculty of Shariah and Law, International Islamic University Islamabad (IIUI) in partial fulfillment of the requirements for the award of the Degree of LLM (Corporate Law)

Viva committee:

Supervisor

Syed Amjad Mahmood

Assistant Professor, Department of Law, IIUI

Internal Examiner

Ataullah Khan Mahmood

Assistant Professor, Department of Law, IIUI

External Examiner

Mr. Ghufran Ahmad

Declaration

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

Mahboob Usman

Acknowledgement

All Praise be to Allah, the Sustainer of the worlds, the Merciful, the Compassionate! By whose grace and help this thesis has been completed. May His everlasting blessings and peace be upon Muhammad, the last of His Messengers!

I would like to extend my gratitude to my honorable teachers and mentors, I would have never been able to reach this milestone without their help and support, especially the support and guidance provided by honorable Professor Imran Ahsan Khan Nyazee, who has been a major source of inspiration for me regarding legal research and writing. I am highly obliged to him; because he kept guiding me before and during my thesis irrespective of his other engagements. Without his push I would have not been able to complete my thesis within a short period. I am also thankful to my supervisor Sir Syed Amjad Mahmood, because of him today, I am able to understand, think critically, shape my ideas and compile them into my LLM research.

In addition I would also like to offer special gratitude to Dr. Muhammad Mushtaq Ahmad (Associate Professor Law) and Mr. Attaulllah Khan Mahmood (Assistant Professor Law) who taught me and always encouraged me. I am also thankful to the university in general and the faculty of Shariah & Law in particular for providing me this environment of research and encouraging me to achieve academic excellence

I would like to offer my gratitude to my family for supporting me while affording every kind of trouble to sponsor my studies. Special gratitude to my elder brother Mohammad Asif who has been very supportive and encouraging. He inscribed in my heart the love for seeking knowledge and always encouraged me (and still he encourages me) to get education in prestigious institutions of the country. It is the dream of my brother that I achieve excellence in academics. I do not know if this humble effort can be considered a step towards that goal or not?

And finally, I must acknowledge the contribution of my friends who supported me in writing my thesis. I must mention here the support of Ayesha Maria, Khalid Mahmood, Wajid Aziz and Sohail Khan for reading this research work and providing me with honest feedback. I am also thankful to Noman, Ali, Sharif, Amir, Safdar, and Farooq (FSL Staff) for their cooperation.

List of Abbreviations

ARPANET	The Advanced Research Projects Agency Network
BNS	Backbone Network Service
CCCP	Corporate Cyber Crime Program
CE	Council of Europe
CNN	The Cable News Network
CSNET	Computer Science Network
CTITF	Counter-Terrorism Implementation Task Force
CTOC	Convention against Transnational Organized Crime
DDoS	Distributed Denial of Service
DOS	Denial of service
FBI	Federal Bureau of Investigation
FIA	Federal Investigation Agency
GVTF	Global Virtual Taskforce
ICC	International Criminal Court
ICJ	International Court of Justice
ICT	Information and Communication Technology
ISI	Inter Services Intelligence

ISPs	Internet service providers
IT	Information Technology
ITU	International Telecommunication Union
IW	Information warfare
JANET	Joint Academic Network
MoIT	Ministry of Information Technology
NIST	National Institute of Standards and Technology
NR3C	National Response Centre for Cyber crimes
NSA	National Security Agency
NSF	National Science Foundation
NSFNET	National Science Foundation Network
NTFS	New Technology File System
PTA	Pakistan Telecommunication Authority
PTCL	Pakistan Telecommunication Company Limited
RATs	Remote Administration Trojans
UK	The United Kingdom
UN	The United Nations

UNODC	United Nations Office on Drugs and crime
US	United States
USC	United States Code
VoIP	Voice over Internet Protocol
WIPO	World Intellectual Property Organization
WWW	World Wide Web

Table of Statutes

Pakistani Statutes

Anti-Money Laundering Act, 2010

Associated Press of Pakistan Corporation Ordinance, 2002

Code of Civil Procedure, 1908

Code of Criminal Procedure, 1898

Constitution of the Islamic Republic of Pakistan, 1973

Copyright Ordinance, 1962

Electronic Media Regulatory Ordinance, 1997

Electronic Transactions Ordinance, 2002

Federal Investigation Act, 1974

Federal Investigation Agency (Inquiries &Investigation) Rules, 2002

Federal Investigation Agency Act, 1974

Freedom of Information Ordinance, 2002.

Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance, 2002

Pakistan Penal Code 1860

Pakistan Telecommunication (Re-organisation) Act, 1996

Patents Ordinance, 2000

Prevention of Electronic Crimes Ordinance, 2009

Registered Designs Ordinance, 2000

The Certification Council Transaction of Business Regulations, 2004

The Payments Systems and Electronic Fund Transfers Act 2007

The Telegraph Act, 1885

The Wireless Telegraphy Act, 1933

Trade Marks Ordinance, 2001

American Statutes

Adam Walsh Child Protection & Safety Act of 2006

Anti-Counterfeiting Amendments Act of 2004

Anti-Counterfeiting Consumer Protection Act of 1996

Check Clearing for the 21st Century Act (Check 21 Act)

Child Protection Act of 2012

Computer Fraud and Abuse Act of 1986

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CANSPAM ACT) of 2003

Cyber Intelligence Sharing and Protection Act (CISPA) 2013.

Digital Millennium Copyright Act of 1998.

Dot-Kids Implementation and Efficiency Act of 2002.

Economic Espionage Act of 1996

E-Government Act of 2002

Electronic Communications Privacy Act (ECPA) 1986

Electronic Communications Privacy Act Amendments Act of 2011

Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E–PRIVACY) Act, 2001

Enforcement of Intellectual Property Rights Act of 2008

Enhanced Consumer Protection against Spyware Act of 2005

Fair and Accurate Credit Transactions Act (FACTA) of 2003

Family Entertainment and Copyright Act of 2005

Federal Cable Communications Policy Act (Section 546)

Foreign Intelligence Surveillance Act of 1978 (FISA)

Fraud and Related Activity in Connection with Computers of 1996

Homeland Security Act of 2002

Identity Theft and Assumption Deterrence Act of 1998

Justice Enhancement and Domestic Security Act of 2003

Personal Data Privacy and Security Act of 2005

Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act).

Prioritizing Resources and Organization for Intellectual Property Act of 2008

Privacy Protection Act of 1980

Protection of Children from Sexual Predators Act of 1998

Ryan Haight Online Pharmacy Consumer Protection Act of 2008'

Social Security Misuse Prevention Act of 2001

Spyware Control and Privacy Protection Act of 2000

Telecommunications Act of 1996

The Communications Decency Act (CDA) of 1996

The National Information Infrastructure Protection Act of 1996

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Unlawful Internet Gambling Enforcement Act of 2006

Abstract

This thesis appraise that cyber legislation has become a constant dilemma of Pakistan. Cyber crimes cause a great loss to national and international business community. Every day more and more digital crimes are being committed, while causing billions of dollar loss to corporations and individuals. Existing legislation does not cope with the advancement of technology. In most of the cases courts fail to find significant proof or suitable legislation to punish the criminals, eventually offenders are released. Extreme demand is emerging from Pakistani society to protect them from cyber crimes and to punish the offenders. So far, Pakistan does not have sufficient legislation to deal with such offenders.

First chapter of this research will be based on general concepts of cyber crimes, such as definition, origin of the internet and evolution of it, kinds, jurisdiction issue, cyber crimes in developing and developed countries. Second chapter will be based on role of Pakistan and International community in the cyber world, further the forensic science will also be discussed in this chapter. In third chapter, the legislation of U.S will be compared with Pakistani legislation and at the end of this chapter findings will be given. On the basis of previous chapters recommendations will be given in chapter four.

Electronic crimes can only be stopped if existing laws are amended and new legislation is introduced. Therefore, it is important to bring existing legislation conformity with International standards to enable law enforcement agencies to tackle different kind of criminals and bring them before the competent court of justice for punishments.

Thesis Statement

Pakistani laws on cyber crimes are not keeping pace with the advancement in modern technology, therefore, it is necessary to legislate on cyber crimes to punish the offenders.

Chapter 1:

CYBER CRIMES: AN OVERVIEW

Introduction

Rapid evolution of information technology is transforming our society and its institutions which have created many problems, inter alia, is a Cyber Crime. It has a wide range of applications in every walk of life, and has directly or indirectly affected almost all the sectors of society. Developing countries (like Pakistan, India and Afghanistan) are not much familiar with technology and these lag in technological progress leads to computer crimes and other related problems. Technological crimes are not covered under any adequate legislation in Pakistan. Therefore, these crimes will be studied in the light of UN, ITU, UNODC and U.S work on this subject, after studying these works, main principles will be adopted for Pakistani legislation.

1.1 Definition of Cyber Crimes

The term "cyber crime" is also used synonymously with technological crime, high tech crime, high technology crime, internet crime, economic crime, electronic crime, digital crime, *inter alia*, labels used by people to describe crimes committed with computers or the Information Technology devices.[1]

The major problem for the cyber crime's study is the absence of consistent definition for the term cyber crimes, however some jurists have worked on it to describe it to some extent. It is generally described as "cyber crime is a generic term that refers to all criminal activities done using the

[1] *Encyclopedia of Cybercrime.* eds. Samuel C. and McQuade (Westport: Greenwood Press, 2009), s.v. "Cybercrime".

medium of computers, the internet, cyber space and the worldwide web."[2] In other words it is defined as a crime in which a computer is the target of the crime or is used as a tool to commit an offense.[3] This definition is also not comprehensive to all related matters, because sometimes mobile phone is also used to commit this crime and this definition does not include the mobile. Dr. Debarati Halder and Dr. K. Jaishankar have given a useful definition which covers few other areas of modern day technology. Their definition of cyber crime is;

> offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).[4]

Above mentioned definition covers all aspects of cyber crimes which are prevailing in Pakistani society. Instead of trying to grasp cybercrime as a single phenomenon, it might be better to view the term as signifying a range of illicit activities whose 'common denominator' is the central role played by networks of information and communication technology (ICT) in their commission.[5]

1.2 Origin of the Internet

Cyber crimes have come about and evolved with the Internet and other advances in IT that have afforded people new ways to cause harm in society.[6] It begins with the advancement of the Internet, assuming that without the latter, the former could and would not exist. It is the Internet that

---

[2] Prashant Mali, *A Text Book of Cyber crime and Penalties* (Indiana: Repressed Publishing LLC, 2006), 3.
[3] http://www.techopedia.com/definition/2387/cybercrime (accessed on 10th December 2014).
[4] Debarati Halder and K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* (Hershey: Information Science Reference, 2012), 15.
[5] Majid Yar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006), 9.
[6] *Encyclopedia of Cyber crime, s.v. "Cyber crime".*

provides the essential electronically generated atmosphere in which it takes place. It is because we use the Internet for communication purposes, therefore we face many problems hence lose billions of dollars annually in online transactions.[7]

History of cyber crimes can be traced to the development of a network, The Advanced Research Projects Agency Network (ARPANET),[8] sponsored by the U.S military in the 1960s, main purpose of ARPANET was to establish means by which secure and resilient communication and coordination of military activities could be made possible in the threat of nuclear confrontations.[9] The ARPANET's technology would allow communications to be broken up into 'packets' that could then be sent via a range of different routes to their destinations, where they could be reassembled into their original form.[10] Establishment of ARPANET played significant role in the advancement of the internet, which opened the doors for research.

1n the 1970s other networks parallel to the ARPANET, UK's Joint Academic Network (JANET) and USA's American National Science Foundation Network (NSFNET), were established; during this era the Electronic email was introduced.[11]

In 1981, when National Science Foundation (NSF) funded the Computer Science Network (CSNET), then access to ARPANET was expanded and in 1982 on the ARPANET, the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol.[12] In early 1980s the NSF funded the establishment of national supercomputing centers at several universities, and

---

[7] Yar, *Cyber Crime and Society,* 83.

[8] The internet has a very interesting history, which brought a new era and renaissance for the whole world. As history of the internet is not my topic, I have just highlighted the history briefly. Detail history can be found in a book titled "*A Brief History of the Future The origins of the Internet,* written by John Naughton and published by Orion Books Ltd, London in 2001 ".

[9] Yar, *Cyber Crime and Society,* 7.

[10] Ibid.

[11] http://en.wikipedia.org/wiki/History_of_the_Internet (last accessed on 30th December 2014)

[12] Ibid

provided interconnectivity in 1986 with the NSFNET project, which also created network access to the supercomputer sites in the United States for research and education organizations.[13]

Commercial Internet Service Providers (ISPs) began to emerge in 1980s,[14] and Private connections to the Internet by commercial entities became widespread quickly, the ARPANET and the NSFNET were decommissioned in 1990 in 1995 respectively, removing the last restrictions on the use of the Internet to carry commercial traffic. Since the mid-1990s, the Internet has had a revolutionary impact on culture and commerce. The research and education community continues to develop and use advanced networks such as NSF's very high speed Backbone Network Service (BNS), Internet2, and National Lambda Rail.[15]

Netscape browser was the first commercial browser which was launched in the year 1994 by the Microsoft by its own browser the Internet Explorer.[16] Since the commercialization of the Internet it has created many problems for the whole world. This is the turning point in the internet history which has created many problems for the world.

1.3 Computer Crimes

Developing countries (such as India, Bangladesh, Pakistan, Afghanistan and third world countries) generally lag behind on technological advances, whereas computer has presented a new and complex situation like white-collar computer crimes. Computer crimes "occur within the white-collar crime, which is a special domain of financial crime".[17] It is a crime against property for

[13] Ibid.
[14] Ibid.
[15] Ibid.
[16] Yar, *Cyber Crime and Society,* 7-8.
[17] Petter Gottschalk. *Policing Cyber Crime* (Hershey: Petter Gottschalk & Ventus Publishing ApS, 2010), 14.

personal or organizational gain, committed by upper class members of society who are educated, wealthy, socially connected and are employed in any legitimate organization. In this case elite class criminal is less likely to be apprehended due to his social status in the society. Consequently, these offenders escape from punishments after committing these offences.

There are many motives for committing these crimes, such as greed, profit, adventure, lust, desire to access forbidden information, disturbed mindset, publicity and revenge. These crimes create serious threat for corporate reputation. Astonishingly, many corporations are involved in white-collar computer crimes to gain profit.

1.4 Cyber Crimes and Conventional Crimes

Crime[18] is as old as the human society. Before the expansion of modern devices, conventional crimes were prevailing in the society. When new developments took place in field of ICT, many new crimes were introduced.

Those crimes which are committed by using computer directly or indirectly are called cyber crimes and those which are committed by using old techniques or methods are called conventional crimes. Currently, the complicated problems faced by the governments are cyber crimes. Though the basis for cyber crimes is conventional crimes but still it is difficult to control this crime.

Apparently, there is no difference between the both. However, a deep examination leads us to its distinction which lies in the involvement of medium used while committing the crime. At any stage where cybernetic intermediate is used then it is called cybercrime or computer crime where technological devices are not used then it is called conventional crimes.

[18] A crime is normally defined as any act or omission which is prohibited by law and in case of breach of it penal consequences are awarded. Mostly, in corporate crimes the act is performed which leads to cyber crime and financial loss to such affected corporations.

1.5 Cyber Crimes

Crime is prevailing everywhere in the world and criminals do not have specific target, they attack developing and developed countries equally.

Developed countries are no exception to these crimes, because they are as victims as developing countries. G8 nations[19] are facing the same problem as third world countries. It cannot be said that they are protected from electronic crimes. However, they are advanced in technology and in better position to tackle this situation. Crime does not have boundary, it is same for developing countries as for developed countries. Developing countries are not much familiar with modern technology, therefore they are easy targets. Many cyber crimes are increasing at rapid pace in developing and developed countries. However, the ratio of these crimes is less in developing countries as compares to developed countries.

1.6 Types of Cyber Crimes

Due to evolution of IT, many new crimes are emerging. It is difficult to cover all of them due to continuous development of such crimes every day. However, few of them which are commonly known are discussed to understand their nature and complication. Financial crimes are discussed below at some length because they are affecting corporations and individuals at large.

The emergence of World Wide Web has enabled unprecedented access to information, and has created unexpected opportunities to attack information assets.[20] Proper understanding of these crimes is important to legislate on these issues, without proper understanding, measures cannot be adopted to prevent them.

---

[19] (G 8 nations are Britain, Canada, France, Germany, Italy, Japan, Russia and the United States).

[20] Michael R Galbreth and Mikhael Shor. "The Impact of Malicious Agents on the Enterprise Software Industry". MIS Quarterly 3 (2010), 595-612.

1.6.1 Advance Fee fraud

Few decades ago, it was difficult to cheat, to get money and deprive someone of his earning. The internet has made it easy for criminals to cheat and deprive innocent people of their earning. One of them is the advance fee fraud which is "intentional misrepresentation for the purpose of gain".[21]

Advance fee fraud[22] is a financial crime that spreads with the introduction of the internet communication, electronic business and electronic commerce,[23] which is carried out by white-collar criminals. These criminals approach the victims without prior information and to obtain email address they use social websites, magazines, journals, newspapers and directories.

Advance fee fraud is actually a kind of lottery scam which begins with an unexpected email notification that says "you have won!", "you have won such and such amount!", "King of this (tribe name), businessman or politician has died and he left his wealth and he advised to distribute among the needy people. Sometimes this type of email comes from a widow on death bed and sometimes it contains name of any famous corporation or company. "Most of these scam emails promise the receiver millions of dollars."[24] The common of all these scams is that some scanned documents are emailed to victims, when receiver of the said email is convinced of the genuineness of the transaction, some fee is requested for bank charge, when fee is received, the receiver disappears. In this way millions of people get defrauded every year through these scams.

[21] Gottschalk. *Policing Cyber Crime*, 21.
[22] Advance fee fraud is also known as lottery scam and email fraud.
[23] Gottschalk. *Policing Cyber Crime*, 21.
[24] Mali, *A Text Book of Cyber crime and Penalties*, 62.

Mostly naïve and greedy people become the victims of such scams and frauds. The recipient of such email is asked to keep the notice secret, not to discuss with anyone else, and to contact a claims agent to receive the said amount. So, the naïve and greedy try to keep it secret and become victim of this scam or fraud.

After contacting the agent, the target of the scam will be asked to pay "processing fees" or "transfer charges" so that the winnings can be distributed, but the target (receiver of scam email) will never receive any payment. People who pay the requested fees, will probably find that they receive unending payment demands to cover "unexpected expenses". The requests for money will go on until the victim realizes what is happening or has no further money to send. After receiving the fee, the scammer disappears from the screen and the victim loses his money. "Many email lottery scams use the names of legitimate lottery organizations or other legitimate corporations or companies, but this does not mean the legitimate organizations are in any way involved with the scams."[25]

1.6.2 Bank Fraud

Bank fraud is an emerging technique of frauds. In bank fraud, an employee of bank sends emails (appear to be from the bank) to their clients for sharing of their personal information such as Credit Cards and Debit Cards information, which he uses for his personal benefit including unauthorized purchases and cause loss to the client for his trust upon the bank employee. Whereas, client considers it, that the employee is seeking information on behalf of bank.

[25]Aaushi Shah and Ravi Srinidhi, *A to Z of Cyber Crime* (Pune: Asian School of Cyber Laws, 2012), 150.

1.6.3 Cyber defamation

Cyber defamation is the same as conventional defamation but in cyber defamation, computer or the internet is used to defame the reputation of a person. There are three ingredients of cyber defamation, if these are found in any published statement then it is considered cyber defamation otherwise this statement will not fall within this category, elements are;

i- the statement must refer to the victim

ii- the statement must be false and defamatory and

iii- the statement must be published by electronic means

If the above mentioned elements are found in any statement, then it is called cyber defamation. If any element is missing then it will not be cyber defamation. The statement published against any organization, financial institution, company or bank defaming their reputation among the competitor of the market and making loss to their credibility and their business is also cyber defamation. Issue arises when someone has published a defamatory statement using public computer or some institution's computer, whether the computer owner is liable or the actual offender? It needs serious consideration.

This is an old phenomenon to destroy the reputation of other competitors while doing same business to control the market. Companies have adopted centuries old techniques to destroy the business of other companies while publishing fake and defamatory comments including the hacking of that company's website to show the negligence of other company for security of clients.

1.6.4 Cyber pornography

Over the last few decades, the "internet has provided an expedient mode of communication and access to a wealth of information."[26] It is a "valuable tool; however, it can also be detrimental to the wellbeing of children due to numerous online hazards."[27] Cyber pornography is assumed to be the largest business on the Internet in present era. Millions of pornographic websites are evidence of this business/industry which is promoting pornographic websites, pornographic online magazines, photos, pictures, books and writings. Though pornography is not illegal in many countries, still child pornography is strictly illegal in most of the countries.[28]

The rapid growth of "electronic and computer based communication and information sharing during the last decade has changed individuals' social interactions, learning strategies and choice of entertainment."[29] The Internet has created a new communication tool, particularly for young people whose use of e-mail, websites, instant messaging, web cams, chat rooms, social networking sites and text messaging is exploding worldwide.[30] There is the "potential for children to be abused via cyberspace through online sexual solicitation and access to pornography."[31] Indeed, the internet is "replete with inappropriate material, including pornography, chatrooms with adult themes and access to instant messaging wherein others could misrepresent themselves."[32] Because children are actively "utilizing the internet where unknown others can have access to them or

---

[26] Stefan C. Dombrowski, Karen L. Gischlar and Theo Durst, "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet." Child Abusive Review 16 (2007): 153-170.

[27] Ibid.

[28] Ibid.

[29] "Prevention and intervention of cyber abuse targeting children and adolescents: A systematic review to evaluate current approaches." is a research report submitted in "University of Toronto" in 2013.

[30] Ibid.

[31] Dombrowski, "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet.": 153-170.

[32] Ibid.

where they can be exposed to inappropriate sexual materials, they require safeguarding and education in safe internet use".[33] The cost to children and society of sexual perpetration is too great to overlook the hazards of online solicitation.[34]

1.6.5 Cyber Stalking

Stalking in not a new phenomenon; from the beginning of the humanity, powerful people started using different tactics to stalk the weaker, since then this method is being used to stalk weaker.

It is defined as" the use of the Internet, e-mail, or other electronic communications devices to stalk another person."[35] In other words we can say that "an element that the person being stalked must reasonably feel harassed, alarmed, or distressed about personal safety or the safety of one or more persons for whom that person is responsible".[36] It refers to the use of "the internet, e-mail, or other electronic communications devices to stalk another person".[37] Same principle is applicable to companies where larger and powerful companies stalk weaker to destroy their business and to control the market.

1.6.6 Cyber Terrorism

The growth and increase in social, political and economic dependence upon the internet affords terrorist organizations a new arena in which to pursue their goals by staging attacks or threats against computer networks and information systems.[38]

---

[33] Ibid.

[34] Stefan C. Dombrowski, John W. LeMasney, and C. Emmanuel Ahia. "Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations." Professional Psychology: Research and Practice 1 (2004): 65-73.

[35] Shah, *A to Z of Cyber Crime*, 42.

[36] *Black's Law Dictionary, v.s. "stalking."*

[37] Mali, *A Text Book of Cybercrime and Penalties*, 35.

[38] Yar, *Cyber Crime and Society*, 50-51.

It is defined as "the premediated use of disruptive activities, or the threat thereof, in cyberspace, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[39]

Many countries have enacted different laws to curb this situation including the UK[40] and US.[41] Many scholars have defined it differently, keeping in view the different prospective of it. Verton has defined it as "the execution of a surprise attack by a subnational foreign terrorist group or individuals with a domestic political agenda using computer technology and the Internet to cripple or disable a nation's electronic and physical infrastructures."[42]

1.6.7 Data Diddling

It is the simplest form of committing computer crime, which is defined "the illegal or unauthorized alteration of the data." It is a common crime which is prevailing all over the world, it occurs during transfer of data. It has affected individuals, financial institutions (banks, changing credit ratings, altering security clearance information credit records etc.), educational institution (for changing the University, College and School transcripts i.e. modifying grades) and all other virtually forms of data processing including inventory records and fixing salaries. Criminals cause billions of dollars' loss to any financial institution or company, because detection of such alteration is not possible to curb this situation within shortest possible time.

---

[39] The above definition was proposed by Rohas Nagpal, President, Asian School of Cyber Laws in the paper titled *Cyber Terrorism in the context of Globalization* presented at World Congress For Informatics And Law II held in Madrid, Spain in 2002.

[40] UK Terrorism Act of 2000.

[41] The USA PATRIOT Act which was passed on 26th October 2001 (an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism).

[42] Yar, *Cyber Crime and Society,* 51.

1.6.8 Denial of Service Attack

Denial of service (DOS) attack (also known as Distributed Denial of Service (DDoS) attack) refers to a cyber-attack which prevents a computer user or owner's access to the services available on his system.[43] This is initiated by "sending excessive demands to the victim's computer, exceeding the limit that the victim's servers can support and make the servers crash"[44] and "results in authorized users being unable to access the service offered by the computer."[45] It is difficult to control such crimes. In DOS attack the hacker closes the access to the website, where the customer cannot get access to the website leaving organization to face the close of business for some time. Earlier, some hackers in past have shut down access to leading e-commerce websites i.e. amazon.com, ebay.com etc., where they faced billions of dollars loss.[46]

1.6.9 Digital Piracy

Digital stealing is about "robbing of people' ideas, inventions, and creative expression everything from trade secrets and proprietary products and parts to movies, music and software."[47] It's a growing threat especially with the rise of digital technologies and Internet file sharing networks.[48]

Digital piracy[49] is the "illegal copying of digital goods (including trademarks), software (including source code), digital documents, digital audio and video for any reason other than to back up without explicit permission from and compensation to the copyright holder.[50] Copyright infringement, trademarks violations, theft of computer and software piracy etc., are the few

---

[43] Ibid., 30.
[44] Mali, *A Text Book of Cyber crime and Penalties*, 46.
[45] Ibid.
[46] Ibid.
[47] Shah, *A to Z of Cyber Crime*, 37.
[48] Ibid.
[49] Digital piracy is also known as copyright infringement and intellectual property crimes.
[50] Gottschalk. *Policing Cyber Crime*, 25.

examples of intellectual property crimes. Copyright protected material's downloading is not only the digital piracy but posting a copyrighted work without the permission of the owner is also copyright infringement.

1.6.10 Email Bombing

Email bombing refers to "sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing".[51] In other words, email bombing is a form of DOS attack that floods an inbox and mail server with messages. If enough messages are sent, the system may be overloaded and will stop working.[52] The DOS attack and email bombing are not similar, as a few people think, both are different. Email bombing plays role to destroy the companies' business by blocking email facility, whereas clients face difficulties to access this facility.

1.6.11 Email/Web Spoofing

Cambridge dictionary has defined spoof as "to try to make someone believe in something that is not true."[53] A spoofed email is one that "appears to originate from one source but actually has been sent from another source."[54] These messages appear to be from a bank, company, or other legitimate institution or organization.

Web and email spoofing occurs when cybercriminals create web sites, web-based traffic, email, or instant messages that appear to be legitimate in every way but are actually fraudulent

[51] Shah, *A to Z of Cyber Crime*, 152.
[52] Mali, *A Text Book of Cyber crime and Penalties*, 41.
[53] Cambridge Advanced Learner's Dictionary, s.v. "spoof"
[54] Shah, *A to Z of Cyber Crime*, 83.

communications designed to socially engineer people into giving up confidential information that can then be used to commit crimes.[55]

Web and email spoofing typically occur together ''as when an attacker sends an e-mail with a link to a spoofed web site.''[56] Furthermore, sometimes criminals send spoof SMS instead of spoof email, both are similar to some extent, however, in SMS spoofing cell phone number is used instead of an email ID.

1.6.12 Fake Social Media Accounts

Fake social media accounts are those which are created by using other persons name instead of own name. Mostly famous persons' names are used to cheat innocent people. Creation and active operation of fake social media accounts is as easy as drinking water. Especially in Pakistan there is no restriction to check fake accounts. This illegal and immoral activity is carried out throughout the world. According to The Cable News Network (CNN) 83 million Facebook accounts are fake and dupe[57] which are malicious in nature and undesirable for society. All social media websites are being used to create fake accounts, cheat innocent people and sell illegal articles.

Previously fake social media accounts were used to be a problem faced by adolescent girls, now everyone is facing the problems caused by fake accounts.

1.6.13 Fake Websites

Fake websites look identical to original ones but it involves manipulating the domain name system to take unsuspecting victims to fake websites.[58] The browser reaches some fake website, rather

---

[55] *Encyclopedia of Cybercrime,* s.v. "fraudulent schemes and theft online" 75.

[56] Ibid.

[57] http://edition.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/ (accessed on 18th February 2015).

[58] Shah, *A to Z of Cyber Crime*, 165.

than original website. This is done to deprive people of their wealth. Many national and international organizations are involved in commission of this fraud.

Many factors are involved to cheat the internet users including design, appearance and lack of awareness among the users, which make it difficult to recognize the original one. These websites have become "increasingly pervasive and trustworthy in their appearance, generating billions of dollars in fraudulent revenue at the expense of unsuspecting internet users."[59]

People may think that it is easy to detect fake websites, nevertheless detecting the fake websites is difficult task due to design and appearance of fake sites which look like original ones. Moreover, fake websites "frequently use images and contents from existing legitimate websites,"[60] which make further difficult for user to understand that which one is genuine and which one is fake. If fake website is designed as an online business company (if someone makes website like ebay or amazon, it will not be possible for an ordinary person to know the actual difference between the existing legal website and fake website), people will not be able to know the fraud which is being committed with them, therefore they will lose their money besides losing trust in the company without knowing the actual situation.

1.6.14 Financial Crimes

Every crime has a hidden motive; in financial crimes the motive is to gain money, same rule is applicable to online financial transactions. Observations show that the motive behind such crimes is money rather than revenge or fun or something else (it is not the general rule sometimes people commit these crimes for the sake of revenge and other purposes also). It includes computer

[59] Gottschalk. *Policing Cyber Crime*, 17.
[60] Ibid.

manipulation, hacking into bank servers, cyber cheating, money laundering, hacking accounting scams, credit card frauds and accounting scams etc.

These are "profit-driven crimes, they should be understood mainly in economic rather than sociological or criminological terms."[61] The theory of these crimes suggests that "financial crimes are opportunity driven, where executive and managers identify opportunities for illegal gain."[62] High up of the organization and outsider are equally involved in these illegal activities. Mali says "with the tremendous increase in the use of the internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated."[63]

1.6.15 Forgery

Computer and IT devices are blessings for the criminals to forge any document, currency notes, academic certificates, medical certificate, electronic records, bank records, financial institution records, company records, institution records, postage and revenue stamps and other government and private records by using computer, scanners and printers.

1.6.16 Identity Theft/Fraud

Identity fraud is the fastest growing while-collar crime in many countries, especially in developed countries.[64] It is a "form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity."[65] This is done to access someone's credit card or other

[61] Gottschalk. *Policing Cyber Crime*, 14.
[62] Ibid.
[63] Mali, *A Text Book of Cybercrime and Penalties*, 6.
[64] Gottschalk. *Policing Cyber Crime*, 23.
[65] Shah, *A to Z of Cyber Crime*, 138.

personal information for financial gain for personal use, leaving the victim upset emotionally and financially.

Identity theft occurs when somebody uses another person's "identifying information, like name, social security number, or credit card number without permission and commits fraud or other crimes."[66] It deprives the real owner of his causing right while loss to his interests.

1.6.17 Internet Time Theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.[67] In the internet time theft unauthorized person, (who is also the in-charge of the computer or network or system), without owner's permission, accesses, transfers data or copy data, introduces virus into any computer, disrupts, denies, provides assistance to anyone to facilitate access to a computer, by tampering with or manipulating any computer, charges the services availed of by a person to the account of another person, destroy or delete and steal the information from any computer commits the Internet time theft. Later this data or information is used to commit other crimes, including financial crimes.

1.6.18 Malicious Agent

A malicious agent (is also known as malicious software) is "a computer program that operates on behalf of a potential intruder to aid in attacking a system or network." [68] Though "a computer virus traditionally was the most prominent representative of the malicious agent species, spying agents have become more common, which transmit sensitive information from the organization to the

---

[66] Ibid.
[67] Mali, *A Text Book of Cyber crime and Penalties*, 56.
[68] Gottschalk. *Policing Cyber Crime*, 22.

author of the agent. Another kind of agent is the remotely controlled agent, which provides the attacker with complete control of the victim's machine."[69]

Malicious software is also used for this purpose, which is classified as 'malicious software based on the perceived intent of the creator rather than any particular features."[70] This includes "spy ware, botnets, keystroke loggers, and dialers. In a botnet, the malware logs in to a chat system while a key logger intercepts the user's keystrokes when entering a password, credit card number, or other information that may be exploited."[71] This software automates a "variety of attacks for criminals and is partially responsible for the global increase in cybercrimes."[72]

1.6.19 Online/Internet Gambling

Many websites exist which offer online/internet based gambling. In some countries it is permissible while in other countries it is prohibited. The issues arises when a person residing in a country, where gambling is illegal and gambles on such website. Then what will be the punishment for the gambler in case of his involvement in gambling or loss of his money in gambling? (This is a jurisdiction issue, which will be discussed at the end of this chapter).

It is a global issue that has an effect upon all countries independent of their local laws prohibiting or allowing gambling to take place.[73] Fidelie asks the question whether Internet gambling is an innocent activity or cyber crime?.[74] She found a very unclear legal status of the Internet gambling. [75] Gambling is an industry that has undergone many changes throughout its existence. Gambling

[69] Ibid.
[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Gottschalk. *Policing Cyber Crime*, 27.
[74] Internet Gambling: Innocent Activity or Cyber crime? is the Article of Laura Woods Fidelie published in International Journal of Cyber Criminology 1 (2009): 476-491
[75] Gottschalk. *Policing Cyber Crime*, 27.

is generally controlled by state governments in an exercise of their police powers.[76] However, the Internet gambling's interstate and international scope necessitates its governance by international law.[77]

The great difficulty in banning the Internet gambling, Fidelie recommends that governments all over the world should regulate and tax online business ventures.[78] She suggests that because of the unclear legal status of the Internet gambling, there must be a legislation explicitly defining what is and is not permissible activity, as well as an emphasis on regulation by world governments and self-regulation by the Internet gambling business.[79]

1.6.20 Salami Attacks

The attack is called salami attack as it is "analogous to slicing the data thinly, like a salami."[80] According to Encyclopedia of White-collar & Corporate crime, Salami is "in banking, a fraud that involves taking all of the round-down fractional cents from periodic interest payments and crediting them to a single account. Thus each transaction has only a thin slice removed."[81]

Salami attacks are used for committing financial crimes, where the employee makes the alteration so insignificant that in a single case it would go completely unnoticed.[82] For example, a bank employee inserts a program, into bank's servers, that deducts a small amount of money from every customer's account. Due to small amount of deduction from the account, no account holder will

[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.
[80] Mali, *A Text Book of Cyber crime and Penalties*, 45.
[81] Encyclopedia of White-collar & Corporate crime, v.s. "Salami"
[82] Mali, *A Text Book of Cyber crime and Penalties*, 45.

notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.[83]

1.6.21 Sale of Illegal Articles

Few decades ago sale of illegal articles was difficult task; through the Internet it is common to find illegal articles on just a click, i.e. narcotics drugs, weapons and other article's information is posted on websites, from where people get information and buy illegal products.

It is practically "impossible to control or prevent a criminal from setting up a website to transact in illegal articles"[84] due to "several online payment gateways that can transfer money around the world at the click of a button".[85] Furthermore, it has created a "marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims"[86] which pose a "serious potential threat to the health and safety of patients."[87]

1.6.22 Stock Robot Manipulation

Stock Robot Manipulation is a computer program which is able to manipulate stock-trading. This program generates "fake buying and selling orders that terminate each other, while at the same time influencing stock prices. Then the program performs real buying and selling orders where stocks are bought at low prices and sold at high prices."[88] This type of manipulation is illegal,

[83] Ibid.
[84] Shah, *A to Z of Cyber Crime*, 193.
[85] Mali, *A Text Book of Cyber crime and Penalties*, 19.
[86] Ibid.
[87] Shah, *A to Z of Cyber Crime*, 193.
[88] Gottschalk. *Policing Cyber Crime*, 23.

which cannot be permitted in any case, because if someone uses this program he can easily crash the whole stock market, and investor will lose their legitimate business.

1.6.23 Trojans and Key-loggers

A Trojan is "an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing."[89] Common types of Trojans are; Remote Administration Trojans (RATs), Password Trojans; Privileges-Elevating Trojan, and Destructive Trojans. There are many other Trojans which affect the normal functions of any computer, from deleting any file to uploading any virus in the victim's computer. Further, many hackers use it as a tool to get the password and personal information of the victim.

Key-loggers: Key-loggers (also known as Keystroke loggin) is the "action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that his actions are being monitored."[90] There are numerous "keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis."[91]

A key logger is a "hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a key-logger is a small battery sized plug that serves as a connector between the user's keyboard and computer."[92] As this device resembles an ordinary keyboard plug, it is relatively easy for someone who wants to monitor a user's behavior to physically hide such a device "in plain sight."[93] As the user types, 'the device collects each

[89] Mali, *A Text Book of Cyber crime and Penalties*, 52.
[90] Shah, *A to Z of Cyber Crime*, 145.
[91] Ibid.
[92] Ibid.
[93] Ibid.

keystroke and saves it as text in its own miniature hard drive, later the person who installed the key-logger must return and physically remove the device in order to access the information the device has gathered".[94] This does not require physical access to the user's computer. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or it can be downloaded unwittingly as spyware.[95]

Key-loggers are used to log all the strokes on a victim's keyboard.[96] This assumes sinister proportions, if a key logger is installed on a computer which is regularly used for online banking and other financial transactions. It will create many problems for the owner of this keyboard or system. These are most commonly found in cyber cafes and hotels' computers.[97] While "unsuspecting victims also end up downloading spyware when they click on friendly offers for free software".[98]

1.6.24 Use of Encryption by Terrorists

Encryption (derived from the term cryptography, meaning 'hidden writing') is a "technique which enables communications to be encoded prior to transmission, so that they are unreadable if intercepted; only the intended recipient has a key which enables the message to be decoded and restored to its original legible form."[99] In other words, it is the process of transforming or changing plain text or data into a form or cipher that cannot be read by anybody other than the sender and by the intended receiver.

---

[94] Ibid, 145-6.
[95] Ibid, 146.
[96] Mali, *A Text Book of Cybercrime and Penalties*, 54.
[97] Ibid.
[98] Ibid.
[99] Yar, *Cyber Crime and Society,* 58.

"Threat of cyber terrorist attack on critical infrastructures is more a case of strategically useful fancy than hard fact. However, this does not necessarily mean that there are no significant convergences between terrorist activities and the Internet."[100] In contrast to the other computer-focused crimes, it has been argued that the Internet plays a significant and growing role in computer-assisted terrorist offences.[101]

Many criminals are using this technology to protect information stored on their hard disks, which creates many problems for law-enforcement agencies to detect and understand the exact nature message. In other words, terrorist groups make use of the Internet in support of their conventional, terrestrially based activities to finance their illegal activities.[102]

1.6.25Virus / Worm Attacks

Computer viruses are 'small software programs that are designed to spread from one computer to another and to interfere with computer operations."[103] It "might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk."[104] These are mostly spread by "attachments in e-mail messages, instant messaging messages, attachments of funny images, greeting cards, and audio and video files."[105] These can also spread through downloads on the Internet, where they are hidden in illicit software or other files or programs.[106]

---

[100] Ibid.
[101] Ibid.
[102] Ibid.
[103] Mali, *A Text Book of Cyber crime and Penalties*, 49.
[104] Ibid.
[105] Ibid.
[106] Ibid.

Worms, unlike viruses do not need the host to attach themselves to, they merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.[107]

1.6.26 Web Defacement

Website defacement is usually the "substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker."[108] Governments and religious sites are mostly targeted by the hackers to display their political and religious beliefs respectively, in addition to disturbing images and offensive phrases. Moreover the financial websites are also hacked to gain financial benefits and to hack the personal data of clients/consumers. Sometimes the hacker hacks websites just for fun.

Corporations are also "targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general".[109] If website of any organization or corporation is hacked, visitors may lose faith in such site that can not promise security and will become wary of performing online transactions. Furthermore after defacement "sites have to be shut down for repairs, (sometimes for an extended period of time), causing expenses and loss of profit."[110]

---

[107] Ibid.
[108] Shah, *A to Z of Cyber Crime*, 231.
[109] Ibid.
[110] Ibid, 232

1.6.27Web Jacking

The web jacking is done through force to get ransom, where the perpetrators have "either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom."[111]

This happens when somebody forcefully takes control of a website (by cracking the password and later changing it), where "the actual owner of the website does not have any control over what appears on that website".[112] Even the Supreme Court of Pakistan's website was hacked by hackers[113] in 2010 to put pressure on Pakistani government for release of Dr. Afia., and they also posted some objectionable material on it.[114] Again in 2011, the apex court's website was "defaced by a hacker who asked the Chief Justice to ban all pornographic websites and do more to help the poor."[115]

1.7 Targets of Cyber Crimes

Underworld criminal does not have any specific target however the main target of these criminal is the databases and archives of governments and national security infrastructures are prime targets for cyber exploitation by the criminal underworld, because they house masses of confidential, top

---

[111] Mali, *A Text Book of Cyber crime and Penalties*, 59.

[112] Ibid.

[113] Two hackers were involved in hacking the Supreme Court website, one was Pakistani national and other was Indian national.

[114] www.ndtv.com/world-news/pakistan-supreme-courts-website-hacked-433856 (accessed on 13th February 2015)

[115] http://timesofindia.indiatimes.com/world/pakistan/Pakistan-Supreme-Courts-website-hacked/articleshow/10136938.cms (accessed on 13th February 2015)

secret social, economic and military information. Besides, the databases of banks and private organization are also the target of these criminals.

1.8 Territorial Jurisdiction and Cyber Crimes

The most important issue in any matter is the jurisdiction of the courts. Whether they have jurisdiction on such issue or not? Cyber crimes are emerging therefore they are creating confusion for the legal professionals. If someone is committing digital crime within the territorial jurisdiction of a country, he can be dealt according to that country's law. For instance, in case the offender lives in Asia and the victim is in Europe, how law enforcement agencies will deal with this offender. Whether there is any specific legislation on this? Or which law will be applicable to this issue? To solve this issue, it is important to take help from International Law because its solution has been provided in this law.

Jurisdiction concerns the "power of the state under international law to regulate or otherwise impact upon people, property and circumstances and reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs".[116] It has large number of different meanings, but most often 'jurisdiction' refers to powers exercised by a state over persons, property, or events (the powers of physical interference exercised by the executive, such as the arrest of persons, seizure of property, and so).[117]

Jurisdiction is a "vital and indeed central feature of state sovereignty, for it is an exercise of authority which may alter or create or terminate legal relationships and obligations. It can be achieved by means of legislative, executive or judicial action".[118] While jurisdiction can be on

[116] Malcolm. N. Shaw, International Law, 6th ed. (New York: Cambridge University Press, 2008) 645.
[117] Akehurst, Modern Introduction to International Law, 109.
[118] Shaw, *International Law,* 645.

many grounds and enforcement is restricted by territorial factors only. For example, if a man commits financial crime in Pakistan and then manages to reach China, the Pakistani courts have jurisdiction to try him, but they cannot enforce it by sending officers of law enforcement agencies to China to apprehend him. They must request the Chinese authorities for his arrest and dispatch to Pakistan for trial. It may take long time to arrest him and punish him according to Pakistani law, because no state has the authority to infringe the territorial integrity of another state in order to apprehend an alleged criminal, even if the suspect is charged with an international crime.[119]

If he remains in Pakistani territory, he can be tried and convicted here, even if it becomes apparent that he is not Pakistani national. However, if some circumstances exist that the Pakistani courts do not have jurisdiction to try the criminal, even he arrested here.[120] For example, hacker has hacked a website of USA in China, and the criminal is caught in Pakistan, both countries can demand his custody through extradition[121], but he cannot be tried in Pakistan for lack of jurisdiction.

As civil cases are concerned international law does not seem to impose any restrictions on the jurisdiction of courts, however in criminal trials states most frequently invoke few principles to bring in her domain, which are discussed below;

a. Territorial principle
b. Nationality principle
c. Passive personality principle
d. Protective principle

[119] Akehurst, *Modern Introduction to International Law*, 110

[120] Punishment of this is discussed in the last chapter of this research.

[121] To hand over criminals to other countries, it is very much relevant to look into agreements with other countries. Whether we have agreement with that country or not? If Pakistan does not have any explicit or implied agreement with other country the accused can not be handed over to that country.

e. Universality principle

To understand the actual concept of these principles, it will not be easy to understand jurisdiction without these principles, therefore these principles need to be discussed at length.

a. Territorial principle

The territorial basis for the exercise of jurisdiction "reflects one aspect of the sovereignty exercisable by a state in its territorial home, and is the indispensable foundation for the application of the series of legal rights that a state possesses".[122] The countries are bound to legislate and prosecute offenders within their territorial boundaries, and as a general principle courts can not exercise their jurisdiction beyond territorial jurisdiction.

Every state claims jurisdiction over crimes committed in its own territory, even by foreigners.[123] Same view is adopted in Pakistan Penal Code 1860 (PPC) regarding the criminals who commit crimes within Pakistan or beyond Pakistan, including the crimes committed aboard ship or aircraft.[124] The same principle is provided in U.S. Code in section 1030 which allows the U.S. government to exercise jurisdiction over criminal activity that "affects the communication of the United States.[125]

Sometimes a criminal act may begin in one state and is completed in another: for instance, a man may shoot across a frontier and kill someone on the other side.[126] The same principle of international law is applicable to cyber criminals because while living in one state they find target in other states as well, where the victims face many consequences in other states. In such

[122] Ibid, 652-653.
[123] Akehurst, *Modern Introduction to International Law*, 110.
[124] The Pakistan Penal Code, 1860(XLV of 1860), S 4
[125] 18 U.S.C, 1030 (e) (2) (B).
[126] Akehurst, *Modern Introduction to International Law,* 110.

circumstances both states have jurisdiction, "the state where the act commenced (has jurisdiction under the subjective territorial principle), and the state where the act is completed (has jurisdiction under the objective territorial principle).[127]

b. Nationality Principle

Whether a person has the nationality of a particular state is "determined by the municipal law of that state, international law only lays down certain limits for states to prescribe which criteria are relevant for nationality".[128] A state may prosecute its nationals for crimes committed anywhere in the world (active nationality principle),[129] this rule is universally accepted, and continental countries make extensive use of it to prosecute their nationals for unlawful acts and activities.[130]

c. Passive personality principle

Under this principle, "a state may claim jurisdiction to try an individual for offences committed abroad which have affected or will affect nationals of the state".[131]

d. **Protective principle**

This principle provides that states may "exercise jurisdiction over aliens who have committed an act abroad which is deemed prejudicial to the security of the particular state concerned. It is a well-established concept, although there are uncertainties as to how far it extends in practice and particularly which acts are included within its net".[132] This allows a state to punish acts prejudicial to its security, even when they are committed by foreigners abroad-for example, plots to overthrow

---

[127] Ibid, 110-111. (Also sometimes called the 'effects doctrine', based on the fact that the injurious effect, although not the act or omission itself, occurred on the territory of the state).

[128] Ibid, 111.

[129] Ibid.

[130] In Pakistan Sections 3 and 4 of Pakistan Penal Code, 1860 are relevant.

[131] Shaw, *International Law,* 664.

[132] Ibid, 667.

its government, espionage, forging its currency and plots to break its immigration regulations.[133] Though, this is the recognized international principle for prosecution, if this is allowed unchecked, it will bring many difficulties for other countries, because every country under this principle will demand that he wants to punish the criminal according to its own law. Hence, it will not be easy to allow this concept widely.

The protective principle of jurisdiction must not be confused with 'diplomatic protection', which refers to the right of a state to intervene diplomatically or to raise an international "claim on behalf of its nationals against another state".[134]

e. Universality principle

Under this principle "each and every state has jurisdiction to try particular offences. The basis for this is that the crimes involved are regarded as particularly offensive to the international community as a whole."[135] Some states claim jurisdiction over all crimes, including crimes committed by foreigners abroad.[136] This principle is criticized internationally because this principle "can obviously lead to unjust results when an individual is punished elsewhere for an act which was lawful under the law of the place where it was committed".[137]

Universality principle is normally considered to be contrary to international law which "allows states to exercise universal jurisdiction over certain acts which threaten the international

[133] Akehurst, *Modern Introduction to International Law,* 111-112.
[134] Ibid, 112.
[135] Shaw, *International Law*, 668.
[136] Akehurst, *Modern Introduction to International Law*, 112.
[137] Ibid.

community as a whole and which are criminal in all countries, such as piracy, and various forms of international terrorism."[138]

The concept of universal jurisdiction, in its broad sense of the power of a state to "punish certain crimes, wherever and by whomsoever they have been committed, without any required connection to territory, nationality or special state interest," however, raises a number of problems.[139] (These problems are not part of my research. These issues can be found in international law books). Above mentioned principles can also be used to prosecute the offender. Many countries may not agree to one or the other principle. Therefore, internationally one solution should be adopted as the Council of Europe has worked on a mechanism to provide proper guidelines for European Union states. Other countries should also adopt this Council of Europe's Convention adding other issues including the jurisdiction issues to resolve this problem permanently.

1.9 Conclusion

There are many challenges to overcome cyber crimes successfully, to prevent such crimes education and public awareness is necessary. Due to lack of awareness of existing cyber crimes in Pakistani society, the general public is facing many problems. Even the law enforcement agencies are unware of these crimes due to complex nature of these crimes. Therefore, the proper understanding of such crimes is necessary to control them. Without knowing them, we can not make laws to punish the criminals.

[138] Ibid.
[139] Ibid, 113

Chapter 2:

Cyber Crimes in Pakistan and Computer Forensic

Most of the countries around the globe are facing serious threats due to increasing trend of cyber crimes and Pakistan is no exception. There is an immense need to investigate the role of Pakistan in this regard which will help in understanding the complexity. Pakistan being new in this race is facing an intensified threat due to lack of awareness. People are facing problems including leakage of personal information to fraud of online shopping every day and therefore, understanding this particular subject is very important for Pakistan.

Increased access to computer and IT is a mixed blessing, which contributes to the productivity and help facilitate communications and file transfers worldwide over the Internet.[140]

> However, they also provide opportunities for abuse of corporate policies and the commission of computer-related crimes. Internet viewing of pornography has become a serious problem for corporations and government agencies. Embezzlements using computers have become commonplace in small- and medium-sized businesses.[141]

Computer forensic is also discussed in this chapter to raise awareness and accord with internationally best accepted practices. Chances for fraud vulnerability increase with reduced awareness to avoid leakage and unwanted access to personal data. Lack of awareness creates to obstacles for law enforcement agencies towards investigation, data and forensic evidence collection, and producing as evidence in the Court for the enforcement of law and the protection of victims.

---

[140]John R. Vacca. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. (Massachusetts: Charles River Media, Inc. Boston, 2005), 241.

[141] Ibid.

2.1 Pakistan and the Cyber World

Without determining the exact role of any entity, it is not possible to find the accurate solution for that. Pakistan is newly introduced in the cyber world therefore, it has a lot of significance to understand its contribution at what stage Pakistan is, in case of cyber world.

Three decades ago commission of cyber crimes was not considerable. Pakistan is newly introduced in cyber world and most of people are unaware of cyber crimes but still country has no sufficient laws to prevent cyber crimes. Internet aids the world with numerous benefits to society and business; besides these blessings it opens doors for criminal activities too. This jeopardy has failed to become the part of Pakistan's legal system, because the world is making sufficient laws for emerging cyber crimes, and still Pakistan is not bothering to make any law to control this issue.

The Pakistan internet market has grown manifolds with the majority of the internet users in big cities, in addition to small number of users in other cities and rural areas. These cities provide majority of the "customer base and expansion in activity is also likely to remain primarily confined to these cities because of the concentration of economic activity in these cities".[142] Pakistan is not free from cyber space dilemma. The availability of computers and the internet connections, provide "unprecedented opportunities to communicate and learn in Pakistan. However, certain individuals (and corporations) do exploit the power of the Internet for criminal purposes."[143]

First ever legislation Pakistan has in field is "Electronic Transactions Ordinance, 2002,"[144] which address cyber crimes issues. This Ordinance was promulgated by the President of the Pakistan with the objective "to recognize and facilitate documents, records, information, communications

[142] Zibber Mohiuddin, "A paper presented on: Cyber Laws in Pakistan; A situational Analysis and way forward", (International Judicial Conference on June 24, 2006 Supreme Court of Pakistan Islamabad), 17.

[143] Ibid.

[144] Electronic Transactions Ordinance, 2002 (LI of 2002).

and transactions in electronic form, and to provide for the accreditation of certification service providers."[145] However, this does not discuss the whole scenario of computer crimes. Few things are covered under this law.

There is another considerable legislations in Pakistan's legal system. The Prevention of Electronic Crimes Ordinance 2007 was promulgated to give awareness of electronic crimes. Consequently the Ordinance was again promulgated in May 2008 and later on in February 2009. Last promulgation of Prevention of Electronic Crimes Ordinance took place on 4th July 2009. This proposed law was not tabled in parliament and it was only implemented as a presidential Ordinance which lapsed.

In Pakistan Presidential Ordinance is applicable for one hundred and twenty days[146] from the date of its promulgation. Therefore, there is no particular cyber prevention law in Pakistan.[147] Masses are looking forward for significant steps to protect them from cyber crimes where in most cases it is not possible to catch the criminals who are either not within national borders or because they are working secretly.

It is not possible to eliminate cyber crime from the cyber space in its entirety from Pakistan or from the globe. However, it is quite possible to check it and take initiatives to reduce it by creating awareness among the users of the internet. The primary step is to make people aware of their rights and duties and further making the application of the laws more stringent to check crime.[148]

---

[145] Ibid. Preamble.

[146] Pak. Const. art. 89, cl. (2) (a) (i)

[147] http://propakistani.pk/2011/01/10/a-country-without-cyber-law-pakistan/ (accessed on 10th August 2014)

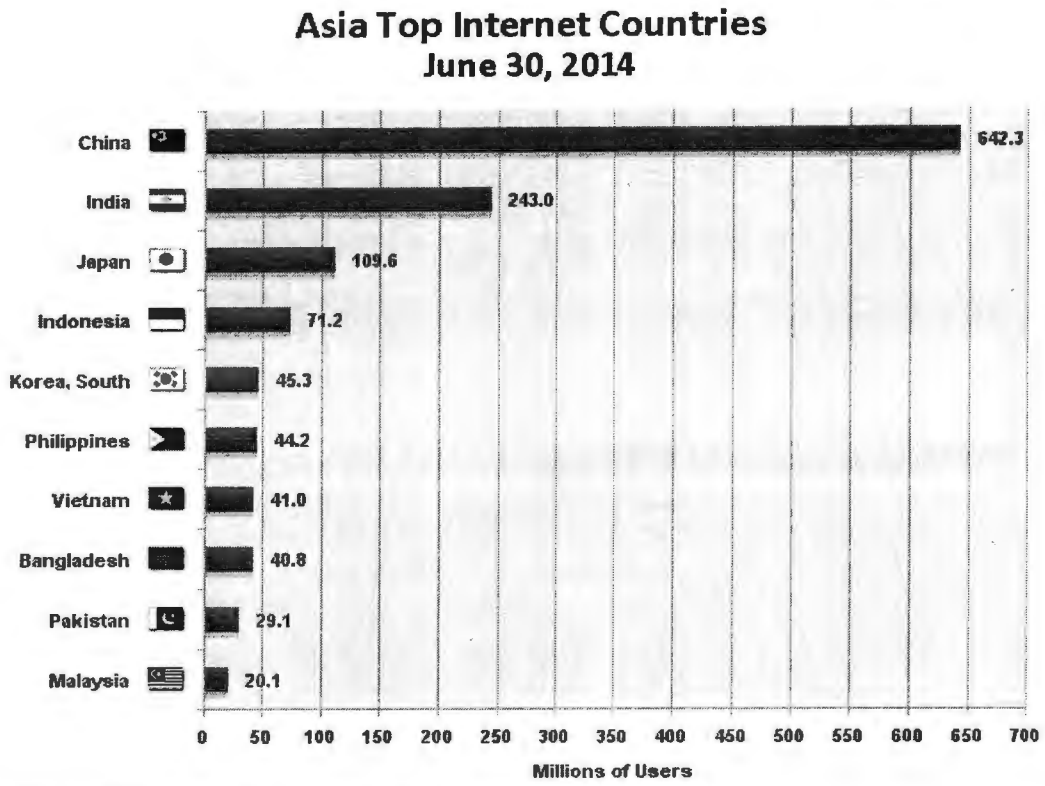
[148] Mohiuddin, "Cyber Laws in Pakistan, 19.; http://supremecourt.gov.pk/ijc/articles/10/5.pdf (accessed on 5th March 2015)

2.2 The Internet use in Pakistan

The Internet access has been available in Pakistan since the mid-90s and in 1995 the Pakistan Telecommunication Company Limited (PTCL) started offering access via the nationwide local call network[149] since then the cybercrimes started emerging in Pakistan.

Since the internet age is less than two decades ago in Pakistan but the ratio of the internet is rising gradually. Pakistan is among the top Asian net users countries, which is placed at no. 9 [150] in these countries (which is shown in chart below), and total internet user are 29,128,970 as of Dec.31, 2013.[151] This ratio is increasing on daily basis as the government has provided laptops and the internet facility to the talented students besides reducing the prices of the accessories and the internet. Further, the 3G and 4G technology has brought revolution in the field of IT.

[149] http://www.internetworldstats.com/asia/pk.htm (last accessed on 3rd March 2015).
[150] Ibid.
[151] Ibid.



This ratio is increasing day by day, the manual business is shifting on the internet, which has reduced the paper work while replacing the manual system with computer technology. Although, it is blessing for the human beings to save their precious time and utilize in any other useful purpose, but fraud, cheating and many other illegal activities are being done by using the internet and computer. Resultantly, effecting the large population of this country, which cannot be ignored in any manner. If law is suitable and meets the demands of society and law enforcement agencies are capable and have expertise in their respective fields, then it will reduce the risk of destruction. It is always considered better to think before the commission of any offence and adopt the relevant measures to protect the people from any loss.

2.3 Complexity of Cyber Crimes

The problems is not with the problems, it lies somewhere inside the system or the investigator. In Pakistan, the problem is that many investigators have neither the expertise nor the experience to deal with investigation, evidence collection, evidence preservation and presentation to the court. Consequently, the offender escapes from punishment.

The investigation of conventional crimes is easy but the investigation of cyber crimes is very complicated. If latest techniques are adopted and applied the complexity of the digital crime can be reduced. (Detail of evidence collection, evidence preservation and related matters have been discussed in later part of this chapter). Further, the technology is "constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously."[152]

2.4 National Response Centre for Cyber Crimes

The Government of Pakistan has established a department "National Response Centre for Cyber crime" (NR3C) under the control of Federal Investigation Agency (FIA), which is responsible for all matters concerning cyber crimes, to investigate, trace the criminals and stop misuse of the internet.

NR3C has expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and training in said fields.[153] Since its inception it has been involved in capacity building of Investigators, Police officers, Intelligence agencies, Judiciary, Prosecutors and other Govt. organizations. It has also conducted a large number of seminars, workshops and training programs to create awareness among the academia, print media, electronic media and

[152] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 219.
[153] http://www.nr3c.gov.pk/about_us.html (accessed on 3rd March 2015).

lawyers. NR3C has also arrested and prosecuted many criminals including two boys for hacking of Supreme Court website.[154]

NR3C is a law enforcement agency dedicated to fight cyber crime. Inception of this Hi-Tech crime fighting unit established in 2007 to identify and curb the phenomenon of technological abuse in society.[155] NR3C's primary function is to deal with technology based crimes in Pakistan. This is the only unit which directly receives complaints and assists other law enforcement agencies in cyber cases.[156]

2.5 Computer Forensic Evidence

When any crime is committed, the investigator starts his work to investigate the matter to trace the offender and bring him before the concerned authorities to prosecute him. The most important thing in investigation is 'preservation of data', which is recovered from the crime scene or the tool which is used for committing the crime. In many cases the criminal may destroy the evidence, therefore it is necessary to know how to recover the destroyed data and preserve the same for further process, when the investigator is unable to recover the destroyed data or files, he may not be able to proceed with the investigation, and the criminal will be acquitted from the charge for lack of evidence. Hence, the investigator tries to recover data or files as much as possible for the investigation purposes. The process of "acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal, with the continuous evolution of technology, it is difficult for law enforcement and computer professionals to stay one step ahead of technologically savvy criminals."[157]

---

[154] http://propakistani.pk/2010/10/27/nr3c-arrests-two-boys-for-hacking-sc-website/ (accessed on 3rd March 2015)

[155] http://www.nr3c.gov.pk/about_us.html (accessed on 3rd March 2015).

[156] Ibid.

[157] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 4.

Computer forensics[158] is the "process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence."[159] In other words, it is the process of collection, preservation, analysis and presentation of computer evidence for criminal and civil proceedings. Information is retained on a computer and it's difficult to completely remove it as generally people think that after deleting the information it can not be recovered. *Inter alia*, computer forensics can "often find evidence of, or even completely recover, lost or deleted information, even if the information was intentionally deleted."[160] In computer forensics, the goal is to recover the data and interpret as much information about it as possible [161] as compares to data recovery, the goal is to retrieve the lost data

2.6 Data Recovery

Every criminal while committing and after the commission of crime attempts to abolish the evidence for apprehension of arrest, mostly in cyber crimes, it has been observed that criminals destroy the computer and its related devices to remove the evidence. If there is a "computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer."[162] Concerned computer will be examined by the forensic expert to ascertain whether the data has been destroyed or not? If that has been destroyed then it will be recovered for the investigation.

In data recovery, the goal is "to retrieve the lost data."[163] Where data has been destroyed then in all such cases, data recovery has a lot of significance for investigator and the corporations. Recent

[158] It also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination.

[159] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 4.

[160] Ibid.

[161] Ibid.

[162] Ibid, 8.

[163] Ibid, 4.

analysis of security implications of "alternative data streams" on Windows NT has shown that Windows NTFS file system allows data hiding in alternative data streams connected to files. These data streams are not destroyed by many file wiping utilities that promise irrecoverable removal of information.[164] Furthermore, "data can be hidden in slack space to store secrets, plant evidence", and maybe hide tools from integrity checkers, merely the forensics software will find it.[165] Therefore, it can be retrieved for the investigation purposes as well as for corporations.

There are many reasons for which we need to recover data, these are systems crash, accidentally overwritten, accidentally deletion of files, accidentally formation of hard drives/disks, viruses and sometimes employees can damage the data. These types are not relevant to be discussed in detail, though the data is also recovered in such situations. In those cases, where the data has been damaged while committing crimes, are relevant to this research. Sometimes, a virus attack has attacked the system, suffered damage from burn or fire, or computer hard drive is immersed in water, mainframe software has malfunctioned and file allocation tables are damaged, same can be recovered by experts to restore to its original shape. Hence, data recovery is not simply to investigate crimes, this technique can be also be used for the welfare of any organization.

Data can be recovered by using multiple functions and tools. It can be recovered by using the limited software tools (which are normally available to the general public and can be found on the internet easily) but to recover the whole data the advanced tools (normally these tools are not easily available to the general public and only can be used by the law enforcement agencies to investigate crimes) are used to recover files and restore them for investigation purposes. The forensics expert can recover the smallest files. Sometimes this tool is also used to investigate the intellectual property rights' claims.

---

[164] Ibid, 206-7.
[165] Ibid, 208.

Data recovery is not important in crimes only, it is also very helpful to recover the corporations' data, in case data has been damaged due to any reason. Subsequently many computers are "used in more important transactions and storage functions, and more important data is stored on them."[166]

Companies are using specialized hardware and software tools for centralized backup and recovery of business data. "Companies that can provide reliable and rapid access to their information are now the fastest growing organizations in the world. To remain competitive and succeed, they must protect their most valuable asset i.e. data."[167] Where data is not protected clients will lose confidence on company and company will bear loss. Whatever the case, companies are more concerned with their data safety, but in case crime has been committed or company is involved in money laundering or financial crimes then the criminal will destroy the computer system to remove the evidence. Here, the investigator will be so competent to get out the original data to investigate these crimes. Contrary to the popular belief that "it's hard to recover information, it's actually starting to appear that it's very hard to remove something even if you want to." [168]

2.7 Evidence Collection and Data Seizure

Evidence in "its purest form is information presented in testimony or in documents that is used to persuade the fact finder to decide the case for one side or the other."[169] Whereas the electronic evidence is "information and data of investigative value that is stored on or transmitted by an

[166] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 192.
[167] Ibid, 192.
[168] Ibid, 213.
[169] Albert J. Marcella and Doug Menendez. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. 2nd ed.* (New York: Auerbach Publications, 2008), 11.

electronic device."[170] Such evidence is "acquired when data or physical items are collected and stored for examination purposes."[171]

The most important thing in investigation of any crime is collection of evidence and preservation of it. Evidence is difficult to "collect at the best of times, but when that evidence is electronic, an investigator faces some extra complexities, as it has none of the permanence that conventional evidence has."[172] Inter alia, the collection of electronic evidence is "very expensive to collect, the processes are strict and exhaustive, the systems affected may be unavailable for regular use for a long period of time, and analysis of the data collected must be performed."[173] In many cases, the victim is unware of fraud, and sometime the law enforcement agencies are informed too late. Resultantly, it creates many hurdles for the investigator to investigate and prosecute the offender and bring him before the court for justice.

It is also important for the investigator to know the latest techniques for evidence collection besides knowing the different types of evidence categories. Without knowing and considering cyber techniques and technology, it will be a fatal exercise to find the evidence due to usefulness of it for the prosecution purposes.

Electronic crime is difficult to "investigate and prosecute, Investigators have to build their case purely on any records left after the transactions have been completed."[174] In addition to this, the electronic records are extremely malleable and electronic transactions currently have fewer limitations, which make it further difficult to investigate properly as computer records can be straightforwardly modified or destroyed. Moreover, computer transactions are "fast, they can be

---

[170] Ibid.
[171] Ibid.
[172] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 217.
[173] Ibid.
[174] Ibid, 218.

conducted from anywhere, can be encrypted or anonymous, and have no intrinsic identifying features such as handwriting and signatures to identify those responsible."[175]

Many problems (as discussed above) which are faced by the investigator and law enforcement agencies, even if the details of the "transactions can be restored through analysis, it is very difficult to tie the transaction to a person."[176] Such information merely shows that "whoever did it either knew or could get past those identifiers, as the identifying information (such as passwords or PIN numbers or any other electronic identifier) does not prove who was responsible for the transaction."[177] "Even though technology is constantly evolving, investigating electronic crimes will always be difficult because of the ease of altering the data and the fact that transactions may be done anonymously."[178] The best way the investigator can adopt is to follow the rules of evidence collection and be as diligent as possible.

There are five rules for collection of evidence, same are applicable to cyber crimes. These relate to "five properties that evidence must have to be useful."[179] If any rule is missing from the evidence, that will make the prosecution case weak. These rules are given below:

1. Evidence must be admissible in law;
2. It must be authentic;
3. It must be complete;
4. It must be reliable; and
5. It must be believable.

These rules are explained briefly

[175] Ibid., 219.
[176] Ibid.
[177] Ibid.
[178] Ibid.
[179] Ibid, 220.

1. **Admissible:** Admissible[180] is the fundamental rule for collecting evidence, if it is not admissible in the court of law according to law, then this evidence will not be collected.
2. **Authentic:** The investigator must be able to show that the evidence relates to the incident in a relevant way. If investigator can't tie the evidence positively to the incident, then he can't use it to prove anything.[181]
3. **Complete:** While collecting the evidence, the investigator should collect complete evidence. If half evidence is collected or some part of it is missing, it will lead to the acquittal of the criminal. It's not enough to "collect evidence that just shows one perspective of the incident,"[182] it should also be collected which links the criminal to that act.
4. **Reliable:** The evidence collected must be reliable. Its "collection and analysis procedures must not cast doubt on the evidence's authenticity and veracity."[183]
5. **Believable:** The evidence presented should be clearly understandable and believable to a judge or presiding officer of the court. It also shows the relationship between the occurrence and the accused.

If these five principles are met in letter and spirit, then the accused will be punished according to law, otherwise chances will increase for acquittal. On the basis of above mentioned rules, few things are established which must be kept in mind while collecting the cyber evidence, and things which must not be done while collecting the digital evidence, these are as:[184]

a- Minimize handling and corruption of original data.

---

[180] Which things are considered admissible and what are not inadmissible. Detail of this can be found in Law of Evidence, in Pakistan the law of evidence is "Qanun-e-Shahadat Order 1984 (P.O. no X of 1984).

[181] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 220.

[182] Ibid.

[183] Ibid.

[184] Ibid, 221. Below mentioned points in main text are taken from the above mentioned book "*Computer Forensics: Computer Crime Scene Investigation.*"

b- Account for any changes and keep detailed logs of actions.

c- Comply with the five rules of evidence.

d- Do not exceed knowledge.

e- Follow local security policy.

f- Capture as accurate an image of the system as possible.

g- Be prepared to testify.

h- Work fast. (work fast does not mean to work in hurry, it means when it comes to the knowledge of the investigator, he must immediately go to the place of occurrence without wasting any further time, otherwise data can be changed)

i- Proceed from volatile to persistent evidence.

j- Don't shutdown before collecting evidence.

k- Don't run any programs on the affected system.

In addition to collecting volatile evidence, the investigator must not waste time on unimportant things, he must draw a list of volatility, otherwise he will not be able to collect the important data rather he will collect less important information. Volatility list would be:

a- Registers and cache

b- Routing tables

c- Arp cache

d- Process table

e- Kernel statistics and modules

f- Main memory

g- Temporary file systems

h- Secondary memory

i- Router configuration

j- Network topology

When the investigator has gone through the whole procedure, and collected the data than he will proceed with identification, preservation, analysis and presentation to the court for prosecution.

There are two methods for data collection: freezing the scene and honey-potting. Two functions can be performed at same time while collecting the data, "freezing the scene involves taking a snapshot of the system in its compromised state,"[185] and all data collected should "have a cryptographic message digest created, and those digests should be compared to the originals for verification."[186] Honey-potting is the process of "creating a replica system and luring the attacker into it for further monitoring."[187] A related method sandboxing "involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage."[188] Honey-potting and sandboxing are "extremely resource intensive, so they may be infeasible to perform."[189] Therefore, this responsibility should be assigned to the forensic expert, who is also expert in law or the lawyer should be consulted for this particular purpose.

The most important thing in data collection is the careful collection of the artifacts,[190] which can help the investigator to trace the suspect, as in hurry the criminal can leave many artifacts. These are difficult to find, if found, then they are very useful to analyze the similar attack committed by the attacker.

Following steps should be performed while collecting the data or information;[191]

---

[185] Ibid., 225.
[186] Ibid, 226.
[187] Ibid.
[188] Ibid.
[189] Ibid.
[190] These are code fragments, trojaned programs, running processes, or sniffer log files etc.
[191] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 227.

a- Find the evidence.

b- Find the relevant data.

c- Create an order of volatility.

d- Remove external avenues of change.

e- Collect the evidence.

f- Document everything.

Evidence is called "separating the Wheat from the Chaff" however the case is opposite in Pakistan, where a lot of material is collected considered to be relevant and important for investigation purposes, rather it's a bulk of documents, which are of no use. In many cases in Pakistan, the investigator is not expert, even he is unaware what data is relevant and what not? Unluckily, the investigators are not aware of the data collection, mostly they collect is useless data. Resultantly, they favor the offender and waste the precious time of the courts in useless things.

When the data has been collected, its preservation starts, if it is not kept according to standard procedure, it will not be helpful for the prosecution to establish his case beyond any reasonable doubt. Resultantly, the offender will get the benefit of it and consequently he will be acquitted. If due attention is not paid to lay down procedure of data preservation, the victim will not be able to get justice due to negligence of the evidence colleting officer. Keeping in view the interests of victims and the safety of the other people, the responsibility of evidence collection and investigation of the crime should be handed over to expert investigator.

Once the data has been collected, it must be protected from contamination. Originals should never be used in forensic examination; verified duplicates should be used. This not only ensures that the original data remains clean, but also enables examiners to try more *dangerous*, potentially data-corrupting tests. Of course, any tests done should be done on

a clean, isolated host machine. You don't want to make the problem worse by letting the attacker's programs get access to a network.[192]

It has been observed, in many cases when the data has been preserved according to the standard procedure, than it is destroyed in experiments. It can be secured by following above discussed principles.

A good way of ensuring that "data remains uncorrupted is to keep a chain of custody." [193] The chain of custody is the proper documentation of data collected.[194] While digital evidence collection is difficult and complex, therefore the documentation may end up greater than the data collected, however it's indispensable to prove the case. Inter alia, the most common reasons for improper evidence collection are "poorly written policies, lack of an established incident response plan, lack of incident response training, and a broken chain of custody."[195] For not maintaining the proper documentation of data, it may challenge its authenticity and veracity as defense counsel may ask questions regarding proper procedure performed/adopted for data collection and preservation, and the investigator will not be able to reply correctly.

2.8 Investigating the Computer/Internet Crime

The main purpose of investigating the internet crime is to trace the accused and prosecute him, while providing the opportunity to recover the victim's assets, if possible.

Cyber crime investigation has both similarities and difference when compared to traditional crime. Traditional crimes generally concern "personal or property offences that law enforcement has continued to combat for

[192] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 228.

[193] Ibid.

[194] Everything related to data is important; who had access to it, who found it, when and where it was transported and how, and what they did with it are important for investigation.

[195] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 247.

centuries".[196] Cybercrime is characterized by being "technologically advanced, it can occur almost instantaneously, and it is extremely difficult to observe, detect, or track".[197] Although, the investigators are expert to track these crime, but still it is not an easy task to investigate properly due to lack of knowledge and experience besides changing trend of cyber crimes.

Within cyber crime investigations, IT forensics and cyber crime investigations are an extremely complicated field [198] due to complexity of the computer system and the internet, where computer evidence is "fragile by its very nature, and the problem is compounded by the potential of destructive programs and hidden data. Even the normal operation of the computer can destroy computer evidence that might be lurking in unallocated space, file slack, or in the Windows swap file."[199] There are no strict rules to be followed vis-à-vis the processing of computer evidence. Every case is different, and has different merits; flexibility on the part of the cyber investigator is important to reach at required solution.

While investigation the computer crimes, "Evidence is easily found in typical storage areas (spreadsheet, database, and word processing files). Unfortunately potential evidence can also reside in file slack, erased files, and the Windows swap file. Such evidence is usually in the form of data fragments and can be easily overwritten by something as simple as the booting of the computer or the running of Microsoft Windows (when windows starts, it potentially creates new files and opens existing ones as a normal process). This situation can cause erased files to be overwritten, and data previously stored in the Windows swap file can be altered or destroyed",[200] creating many difficulties for the investigator.

---

[196] Gottschalk. *Policing Cyber Crime*, 110.
[197] Ibid.
[198] Ibid.
[199] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 240.
[200] Ibid, 238.

Few thoughtful guidelines have been provided for the investigator to investigate the case, if these are fully met, the case scenario will be changed; the investigator must observe following guidelines;[201]

a- Shut down the computer.

b- Document the hardware configuration of the system.

c- Transport the computer system to a secure location.

d- Make bit stream backups of hard disks and floppy disks.

e- Mathematically authenticate data on all storage devices.

f- Document the system date and time.

g- Make a list of key search words

h- Evaluate the Windows swap file.

i- Evaluate file slack.

j- Evaluate unallocated space (erased files).

k- Search files, file slack, and unallocated space for keywords.

l- Document file names, dates, and times.

m- Identify file, program, and storage anomalies.

n- Evaluate program functionality.

o- Document findings.

p- Retain copies of software used.

Internet forensics is the application of scientific and legally sound methods for the investigation of Internet crimes, whose focus ranges from an individual system to the Internet at large. The computer forensics expert works on a different level than the person he is investigating. As all

[201] Ibid, 240. Below mentioned points in main text are taken from above mentioned book in the refrence.

electronic crimes are committed over the computer or the internet, and whatsoever the reason of committing the crime, the investigator is legally bound to properly investigate the crime.

2.9 Investigating Corporate Espionage

Corporations are "dependent on the infrastructures that form the basis for modern economy."[202] Commercial, business, financial transactions, informational activities, infrastructural activities and government activities take place on computer networks. This information is vulnerable to intentional and unintentional attackers.[203] Threats to the security of "business information are numerous and they come from all directions, including organized crime syndicates, terrorists, and government sponsored espionage, and most global high technology companies have little idea of the array of hostile forces targeted against them."[204] Some of the threats "might be obvious, as well as the strategies that companies can mount against them, but others might not be so cut and dried because the nature of such threats and how to protect against them is not taught in business schools."[205]

Nowadays, many intelligence services around the world are "shifting their emphasis and targets to business and government intelligence services want technological production and marketing information, and they usually share what they get with their country's companies.[206] Government-sponsored intelligence operations against companies seek "information about bids on contracts, information that affects the price of commodities, financial data, and banking information."[207] To get this sensitive information, government intelligence services use many of the techniques

[202] Ibid, 469.
[203] Ibid, 470.
[204] Ibid, 474.
[205] Ibid.
[206] Ibid.
[207] Ibid.

developed[208] during the Cold War era.[209] This sort of surveillance can not be acceptable for democratic governments because it's against the fundamental rights, violation of these rights can not be permitted at any cost. However, investigating the money laundering charges and financial crimes, there is a need to proper legislate on this particular topic.

Business community needs to "understand that the criminal and terrorist threat worldwide is changing and is now both more sophisticated and more dangerous than anyone would have thought."[210] These threats include "terrorism, organized crime, and inside operations carried out by disgruntled employees and hackers."[211]

Companies should provide "substantial information, security protection for relatively low cost."[212] They "should review security measures in sensitive areas of their operations such as research and development, talk to traveling executives who carry company laptops about using precautions to prevent theft, and examine communications with overseas facilities with an eye toward installing commercially available encryption that is all but impossible to crack."[213]

"Espionage is the use of spies to gather information about the activities of an organization. Information gathered through espionage is generally confidential information that the source does not want to divulge or make public."[214]

---

[208] That includes bugging telephones and rifling through papers left in hotel rooms by visiting businessmen and businesswomen. In addition, government intelligence services are known to plant moles in companies and steal or surreptitiously download files from unsecured computers. Several also have highly sophisticated signal intelligence capabilities to intercept even encrypted company communications. Messages that are not encrypted with the latest technology are especially vulnerable. These include telecom and computer communications, including email.

[209] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 474.

[210] Ibid, 475.

[211] Ibid.

[212] Ibid.

[213] Ibid.

[214] *Investigating Network Intrusions and Cyber crime*: (New York: EC-Council, 2010), 265.

security of the United States, enacted the Economic Espionage Act of 1996, to address the growing problem of theft of trade secrets."[220]

Corporations use certain measures to stop the espionage and always take some steps for the prevention of the same. Steps to prevent corporate espionage are understanding and prioritizing critical assets, defining acceptable level of loss, controlling access, baiting, detecting moles, profiling, monitoring, and analyzing signatures.[221]

The following are some of the types of information that corporate spies seek:[222]

a- Marketing and new product plans

b- Source code of software applications: It can be used to develop a similar application by a competitor or to design a software attack to bring down the original application, thus causing financial losses to the original developer.

c- Corporate strategies

d- Target markets and prospect information

e- Business methods

f- Product designs, research, and costs: Huge investments will be in vain if the product design and related research is stolen, because the competitor can also develop the same product and offer it for less.

g- Alliance and contract arrangements: delivery, pricing, and terms

h- Customer and supplier information

i- Staffing, operations, and wages or salaries

j- Credit records or credit union account information

---

[220] Marcella. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 19.

[221] *Investigating Network Intrusions and Cyber crime*, 284.

[222] Ibid, 267.

Economic and industrial espionage is a "global industry with a growing workforce."[223] While investigating the corporate espionage, the investigator must be aware that from where this sensitive information has been leaked either inside or outside the company. Mostly, the employees[224] of the organization are involved in espionage.

The major techniques used for corporate spying are hacking, social engineering, dumpster diving, and phone eavesdropping.[225] The investigator must also be aware of the latest techniques which are being used by the criminal if he is not aware of such techniques, it will be difficult for him to properly investigate the matter. The following are some common spying techniques;[226]

a- Hacking computers and networks[227]

b- Social engineering[228]

c- Dumpster diving[229]

d- Trash bins

e- Printer trash bins

f- User desks

---

[223] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 469.

[224] There can be many reasons for the involvement of the employee in the espionage, most famous reasons are

a- Lack of loyalty
b- Job dissatisfaction
c- Boredom
d- Mischief
e- money

[225] *Investigating Network Intrusions and Cyber crime*, 284.

[226] Ibid, 267.

[227] This is an illegal technique for obtaining trade secrets and information. Hacking involves gaining unauthorized access to computers and networks.

[228] Social engineering is the use of influence and the art of manipulation to gain credentials. Individuals at any level of business or communicative interaction can make use of this method. All the security measures that organizations adopt are in vain when employees get socially engineered by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam e-mail, and bragging to coworkers.

[229] Dumpster diving is searching for sensitive information in the following places at a target organization.

g- Whacking[230]

h- Phone eavesdropping[231]

i- Network leakage[232]

j- Cryptography[233]

k- Steganography[234]

After going through the motives and kind of corporate espionage, the investigator will be able to investigate the matter. The following are some steps an investigator should take when investigating corporate espionage cases:[235]

a- **Check the possible points of physical intrusion:** Before starting an investigation into a corporate espionage case, an investigator should scan all possible points of physical intrusion carefully. These points may provide clues about how the information might have

---

[230] Whacking is wireless hacking that is used to capture information passing through a wireless network.

[231] Phone eavesdroppsing is overhearing phone conversations while being physically present.

[232] Most organizations set up their network to block or limit inbound and outbound connections. Even organizations that are starting to filter outbound traffic still allow certain traffic out. Two types of traffic that are always allowed out of an organization are Web and e-mail traffic.

[233] Cryptography is a technique to garble a message in such a way that the meaning of the message is changed. Cryptography starts with a plaintext message, which is a message in its original form. An encryption algorithm garbles a message, which creates ciphertext. A decryption algorithm can later take the ciphertext and convert it back to a plaintext message. During the encryption and decryption process, what protects the ciphertext and stops someone from inadvertently decrypting it back to the plaintext message is the key. Therefore, the secrecy of the ciphertext is based on the secrecy of the key and not the secrecy of the algorithm. Thus, to use an encryption program, a user has to generate a key. The key is often tied to a username and e-mail address. No validation is performed, so an attacker can put in bogus information that could be used later to launch a man-in-the-middle attack where the attacker can trick someone into using a false key. If someone knows the public key for a user, he or she can encrypt a message; but he or she can only decrypt the message if he or she knows the user's private key. The public key can be distributed via a trusted channel, but a user's private key should never be given out. If someone can get access to a user's private key, he or she can decrypt and read all that user's messages.

[234] Steganography is data hiding and is meant to conceal the true meaning of a message. With steganography, a user has no idea that someone is even sending a sensitive message because he or she is sending an overt message that completely conceals and hides the original covert message. Therefore, cryptography is often referred to as secret communication and steganography is referred to as covert communication. Insiders often use steganography to transmit credentials to other organizations.

[235] *Investigating Network Intrusions and Cyber crime*, 271. In main text below are the points taken from this book.

leaked and can also provide fingerprints if anybody passed through. This information may be helpful when presenting the case before a court of law.

b- **Check the CCTV records:** An investigator should check all CCTV records for any unusual activity. This often leads to the real culprit.

c- **Check e-mails and attachments:** An investigator should check all official e-mails and other e-mails with attachments used at the workplace. In many cases, the information is passed outside using e-mails. An investigator should thoroughly scan any suspicious e-mail and try to find out its destination.

d- **Check systems for backdoors and Trojans:** Disgruntled employees install backdoors and Trojans in their systems using their privileges as employees before quitting their jobs. So an investigator should scan all the systems and check for backdoors and Trojans. If any backdoor or Trojan is discovered, an investigator should trace its connections.

e- **Check system, firewall, switch, and router logs:** Logs show each and every event taking place in a network. An investigator should examine the logs of all network devices to detect suspicious activities, such as when and which data passed through the network and which kind of services and protocols were used.

f- **Screen the logs of network and employee monitoring tools, if any:** If an administrator has installed any kind of employee monitoring tools on the organization's systems, an investigator should analyze their reports. But before using any such monitoring tools, the investigator must take care of any legal aspects.

g- **Seek the help of law enforcement agencies, if required:** The investigator should enlist the help of law enforcement agencies if it is necessary to track the culprit and bring him or her to trial.

2.10 Conclusion

In any case, the evidence is integral part for successful prosecution. Cyber evidence is not easy to collect, preserve and present in the competent court, due to its complexity. Therefore, it is necessary to provide legal cover to all matters which are related to digital evidence. So, in this way, the prosecution can strengthen her case to prosecute the criminal.

Chapter 3:

Cyber Laws in Pakistan & other Jurisdictions

Countries having strong and ample legislation can step with increasing trends of digital crimes. Unfortunately, Pakistan does not have sufficient laws to deal with this situation. For comparison, understanding of other countries' legislation on same subject has lot of importance which plays an important role. Firstly, the International aspects of cyber laws; secondly, the EU laws, the UN and allied departments and ITU' efforts to combat cyber crimes and lastly the Pakistani laws will be compared with the US cyber laws, and at the end some recommendations will be given for Pakistani legislature to take necessary steps.

3.1 International Aspects of Cyber Laws

Only Pakistan is not the target of these crimes, international community is also facing many problems as "information and communications flow more easily around the world. Borders are no longer boundaries to this flow. This causes difficulty, as the internet-based society has no physical boundaries and thus much traffic escapes national control. Criminals are increasingly located in places other than where their acts produce their effects."[236] Many investigators have neither the expertise nor the experience to deal with evidence collection, hence the offender escapes from punishment.

Over the last many years "developed nations' are shifting from the industrial era to the new information age and has enabled them to develop the nascent technology and produce ever greater quality in standards and value".[237] As internet users are increasing day by day, therefore they have

[236] Mohiuddin, "Cyber Laws in Pakistan, 19.; http://supremecourt.gov.pk/ijc/articles/10/5.pdf (accessed on 5th March 2015)

[237] Ibid.

adopted many security measures to protect their personal information and databases and have secured this information from the attacker/hacker.

Since the internet users are increasing day by day, similarly the governments and law enforcement agencies are also facing many difficulties to bring the criminal before the court and prosecute them. In addition to existing cyber crimes, many new crimes are emerging, resultantly it becomes very difficult to trace and understand the new techniques to overcome these problems. Moreover, criminals don't have any specific area or jurisdiction or range to target, wherever they find the target easily, they hit the target.

Below given chart shows the statistics of the internet users worldly, which shows that most of the people are using the internet for different purposes including the online business transactions.

WORLD INTERNET USAGE AND POPULATION STATISTICS[238] JUNE 30, 2014 - Mid-Year Update						
World Regions	**Population (2014 Est.)**	**Internet Users Dec. 31, 2000**	**Internet Users Latest Data**	**Penetration (% Population)**	**Growth 2000-2014**	**Users % of Table**
Africa	1,125,721,038	4,514,400	**297,885,898**	26.5 %	6,498.6 %	9.8 %
Asia	3,996,408,007	114,304,000	**1,386,188,112**	34.7 %	1,112.7 %	45.7 %

[238] http://www.internetworldstats.com/stats.htm (accessed on 3rd March 2015)

Europe	825,824,883	105,096,093	**582,441,059**	70.5 %	454.2 %	19.2 %
Middle East	231,588,580	3,284,800	**111,809,510**	48.3 %	3,303.8 %	3.7 %
North America	353,860,227	108,096,800	**310,322,257**	87.7 %	187.1 %	10.2 %
Latin America / Caribbean	612,279,181	18,068,919	**320,312,562**	52.3 %	1,672.7 %	10.5 %
Oceania / Australia	36,724,649	7,620,480	**26,789,942**	72.9 %	251.6 %	0.9 %
WORLD TOTAL	**7,182,406,565**	**360,985,492**	**3,035,749,340**	**42.3 %**	**741.0 %**	**100.0 %**

The developing countries are not only facing cyber-attacks alone but the developed countries are also facing the same issues. However, they have strong legislation and expertize to trace the offender and prosecute them, whereas the developing countries are lacking in investigating the cyber crimes. Hence, developing countries are the target for such attacks because they do not now the nature of these attacks.

To help the developing countries to legislate, create awareness and facilitate in investigation, the International Telecommunication Union (ITU) has facilitated these countries to take security measures to protect online business transactions and safeguard people from all kinds of frauds. ITU has also produced many books to help them to understand the exact nature of these crimes. "Understanding Cyber crime: Phenomena,

Challenges and Legal Response"[239] is the ITU publication which has been prepared by Prof. Dr. Marco Gercke for the developing countries.

Understanding the sensitivity of the matter, United Nations Office on Drugs and crime (UNODC) has also prepared many books and reports to assist the world to carry out work on cyber laws to tackle the emerging situations, "The Use of the Internet for the Terrorist Purpose" and "Comprehensive Study on Cyber crime"[240] latter is the draft document prepared by the (UNODC) for the international community for understanding of cyber crime.

Even the United Nations General Assembly (UN General Assembly) has adopted many resolutions to get-rid of these crimes from the globe. In Resolutions 55/63[241] and 56/121[242] respectively, the UN General Assembly requested the states to eliminate the safe havens for those who misuse information technology criminally. In Resolutions 57/239[243] and 58/199[244], UN General Assembly encouraged the "Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure."

In Resolution 65/230,[245] the UN General Assembly requested the Commission[246] "to conduct a comprehensive study of the problem of cyber crime and responses to it by Member States, the international community and the private sector, including the exchange of information on national

---

[239] Marco Gercke. *Understanding Cyber crime: Phenomena, Challenges and Legal Response*. Geneva: International
Telecommunication Unit, 2012. a new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries published by ITU in April 2009.

[240] This was prepared for the open-ended intergovernmental expert group on cyber crime, UNODC. However, this has not been formally edited and remains subject to editorial changes.

[241] A/RES/*55/63*. A resolution of the United Nations General Assembly. The 63rd resolution of the General Assembly in Session 55.

[242] A/RES/*56/121*.

[243] A/RES/*57/239*.

[244] A/RES/*58/199*.

[245] A/RES/65/230.

[246] UNODC Commission on Crime Prevention and Criminal Justice to establish, an open-ended intergovernmental
expert group.

legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cyber crime."

Later, in its resolution no. 67/189[247] UN General Assembly appreciated the work of "open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cyber crime and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course".

The Council of Europe's (CE) Convention on Cyber Crime was the first international initiative on computer crimes which was adopted in 2001, to foster international cooperation by criminalizing the basic cyber crimes.

As, US has knowledge and experience in the field of cyber security, with significant influence in the area,[248] besides it has an excellent structure for the investigation of these crimes. Many law enforcement agencies[249] are involved to investigate these matters including Federal Bureau of Investigation (FBI), which is also responsible to investigate cyber crimes. That's why US is protected from many crimes which are easily committed in developing countries or rest of the world. Therefore, US is only the country which is mostly protected from emerging crimes due to strong legislation on cyber issues. If these legislative guidelines are adopted in Pakistan then the ratio of cyber crimes can easily be tackled. The US Department of Justice is working with foreign governments through many channels to address global threats related to computer crimes.[250]

---

[247] A/RES/67/189.

[248] Mohiuddin, "Cyber Laws in Pakistan, 11.

[249] Federal Bureau of Investigation (FBI), the United States Secret Service (US Secret Service), the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, Internet Fraud Complaint Center, the Internet Crime Complaint Centre (IC3), the National White- Collar Crime Center (NW3C) and the Bureau of Alcohol, Tobacco and Firearms (ATF) are the agencies which investigate cyber crimes and related crimes in US.

[250] Mohiuddin, "Cyber Laws in Pakistan, 16.

Keeping in view the requirement of the Pakistani society, government of Pakistan should cooperate with the US Department of Justice to learn their techniques in this field.

3.2 European Union Laws

The European Union acknowledging the importance of digital technology and recognizing the consequences caused by it, agreed on a convention which was adopted in 2001 to curb these crimes. The convention is called "Council of Europe's Convention on cybercrime", which was opened for signature on 23rd November 2001, and entered into force on 1st July 2004, so far 45 countries have ratified this convention and eight countries have signed this but not ratified yet.[251] The Council[252] of Europe's Convention on Cybercrime[253] is the first international treaty designed to address several categories of crimes "committed via the Internet and other computer networks, by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations".[254] Likewise, it provides safeguards to detect hacking, computer-facilitated fraud, illegal access and interception of computer data, data interference, system interference, misuse of devices, computer-related fraud and forgery, child pornography, and copyright infringement/violations and other crimes committed through digital means. Although, it is a comprehensive document on computer crimes, but a number of cyber crimes are not included in the convention i.e. identity theft, cyber terrorism and spam. Thus, it is useful as guidelines for the legislature, but it is not satisfactory to meet the demands of contemporary world. In addition,

---

[251] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (accessed on 15th March 2015).

[252] The Council of Europe has 46 members, including all 25 members of the European Union.

[253] The Council of Europe's Convention on Cybercrime is also known as the Budapest Convention on Cybercrime or the Budapest Convention.

[254] http://www.iol.co.za/news/world/us-ratifies-treaty-on-cybercrime-1.288245#.VQU1q-F8t5Q (accessed on 15th March 2015).

convention on cyber crimes has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence.

The U.S. Congress have ratified this convention despite the praise and criticism from the public.[255] Though, the U.S has not ratified the additional protocol to this convention. Before the adoption of CE convention it was difficult to get information from other countries and investigate electronic crimes, nevertheless, it made easy for signatories to obtain cyber information and investigate digital crimes.

The Convention's main objective is to establish a "common criminal policy to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. To these ends, the Convention requires signatories to, define criminal offenses and sanctions under their domestic laws"[256], "establish domestic procedures for detecting, investigating, and prosecuting computer crimes, and collecting electronic evidence of any criminal offense," and establish a "rapid and effective system for international cooperation." If these measures are adopted and applied successfully, then these crimes can be mitigated.

This Convention represents a significant step forward in tackling cyber crimes because it binds signatories to prosecute computer-related crimes strongly which many countries were unable to do before the adoption of this Convention. Furthermore, due to transnational jurisdiction provision, the Convention has improved deterrence and reduced the number of countries in which criminals can evade prosecution. Similarly, the Convention's procedures for collecting evidence and assist

[255] http://news.cnet.com/2100-7348_3-6102354.html (accessed on 15th March 2015).

[256] This convention also provides that Signatories must also enact laws establishing jurisdiction over such offenses committed on their territories, registered ships or aircraft, or by their nationals abroad. Therefore, covering all the related subjects of that state whether the crime is committed on land or sea.

law enforcement authorities to fight terrorism. The Convention had not protected the privacy that "undermines individual privacy rights and expands surveillance powers too far".

Among the targets of these participating in the convention are "hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material and terrorists attempting to attack infrastructure facilities or financial institutions."[257]

3.3 Cyber laws, U.N. and its Agencies

The United Nations (UN) is an intergovernmental organization established on 24th October 1945 to promote international co-operation among member states. The UN Charter stipulates that each primary organ of the UN can establish various specialized agencies[258] to fulfill its obligations and to perform duties. It has established various departments and specialized agencies to tackle different issues. Moreover, in 2002 it established the United Nations Office on Drugs and Crime (UNODC)[259] to assist the U.N in better "addressing a coordinated, comprehensive response to the interrelated issues of illicit trafficking in and abuse of drugs, crime prevention and criminal justice, international terrorism, and political corruption."[260] Since then the UNODC has worked on cyber crimes to provide guidelines and suggested preventive measures. These goals are pursued "through different functions such as research, guidance and support to governments in the adoption and implementation of various conventions, treaties and protocols, as well as technical/financial

[257] http://www.iol.co.za/news/world/us-ratifies-treaty-on-cybercrime-1.288245#.VQU1q-F8t5Q (accessed on 15th March 2015).

[258] U.N. CHARTER, art. 59.

[259] The U.N's Office for Drug Control and Crime Prevention was established in 1997 and was renamed The United Nations Office on Drugs and Crime (UNODC) in 2002.

[260] http://en.wikipedia.org/wiki/United_Nations_Office_on_Drugs_and_Crime (accessed on 17th March 2015).

assistance to said governments to face their respective situations and challenges in these fields."[261] Cybercrime is one of the crime which is spreading rapidly all over the globe therefore the UNODC is also responsible to deal with these crimes. (UNODC's role will be discussed separately after the role of UN).

3.4 United Nations' work on Computer related Crimes

Some people may think that the UN is not considered as a jurisdiction, than why U.N's law is being discussed in present study? Keeping in view the demands of present era, the U.N has adopted many resolutions to provide proper guidelines to highlight these issues as well as to assist the member countries to eradicate the safe sanctuaries of digital offenders.

The U. N adopted a resolution 53/70 on 4th January 1999, titled "Developments in the Field of Information and Telecommunications in the Context of International Security"[262] to discuss the IT and its impact on the U.N member states and provided proper guidelines to avoid these threats.

The UN's General Assembly in its resolution 65/230,[263] requested the Commission on Crime Prevention and Criminal Justice to "establish an open-ended intergovernmental expert group[264]

> to conduct a comprehensive study on the problem of cybercrime, by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with

[261] Ibid.
[262] A/RES/53/70.
[263] A/RES/65/230. The General Assembly in 2010 has adopted the Resolution 65/230 based initially on the Salvador Declaration Article 42.
[264] This group is organized by UNODC which is situated at Vienna.

a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.[265]

Later, in its resolution 67/189[266] The UN General Assembly appreciated the work of the open-ended intergovernmental expert group. Many other U.N resolutions have discussed these issues at length. In resolution 55/63[267] and 56/121[268] respectively, the UN General Assembly requested the states to "eliminate safe havens for those who criminally misusing information technology, and legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized."[269] In resolution 57/239[270] and 58/199,[271] the UN General Assembly encouraged for the Creation of a Global Culture of Security and the Protection of Criminal Information Infrastructure.

Resolution 52/85 of 12 December 1997, 53/111 of 9 December 1998, and 54/126 of 17 December 1999 respectively, all these resolution are based for "Convention against Transnational Organized Crime." After many years struggle by the U.N member states, this resolution was brought before the members states to sign. U.N has prepared a detailed report on the use of the internet being used for terrorist activities, this report is titled as "Countering the Use of the Internet for Terrorist Purposes -Legal and Technical Aspects."[272] Many terrorist groups are involved in cyber crimes, subsequently this is useful for legislation and investigation purposes, besides taking many practical

---

[265] Article 15 of "Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World".

[266] A/RES/67/189.

[267] A/RES/*55/63*.

[268] A/RES/*56/121*. This resolution was adopted on December 19, 2001, including recommendations on the prevention and combat criminal misuse of information technologies.

[269] A/RES/*55/63*.

[270] A/RES/*57/239*.

[271] A/RES/*58/199*.

[272] This report can be found at www.un.org/terrorism/internet.

measures to eradicate terrorism; the United Nations Counter-Terrorism Implementation Task Force[273] (CTITF)[274] was established by the Secretary-General in 2005 for this purpose.

The U.N adopted resolution on "Global Counter-Terrorism Strategy" on 20th September 2006 that provides strategies for control of these crimes, another resolution provides as follows; "Special measures to be adopted to fight the menace of international terrorism"[275] was adopted by the General Assembly,[276] in which it was emphasized to make legislation on cyber terrorism and to provide effective measures against cybercrimes by "creating a system against cyber-attacks that is able to react swiftly upon any sign of cyber terrorist activities";[277] "developing safer software and making customers more aware of the need for safer Internet use";[278] "supporting the creation of a (an) international Office of Cyber Security with trained personnel";[279] "defining in their legislation a number of offences, including crimes against privacy, honesty and availability of computer systems and data stored therein";[280] "imposing adequate punishments such as fines or prison",[281] and ratifying 2001 Council of Europe Cybercrime Convention.[282]

United Nations Convention against Transnational Organized Crime's (CTOC) main purpose is to promote cooperation to prevent and combat transnational organized crime more effectively.[283] Cyber crimes are not exception to this, because criminals do not have any border. If enemies of progress and development are crossing borders for opportunities, then law enforcement agencies

---

[273] More detail of CTITF can be found at www.un.org/terrorism/cttaskforce.

[274] CTITF is chaired by a senior U.N official appointed by the Secretary-General and consists of 30 U.N system entities and INTERPOL which are also responsible to work on cyber terrorism.

[275] A/RES/4/3

[276] The General Assembly adopted this resolution, on its 2nd meeting, held on 23 March 2010,

[277] Special measures to be adopted to fight the menace of international terrorism, Article 5 (b) (i).

[278] Ibid (5) (b) (ii).

[279] Ibid (5) (b) (iii).

[280] Ibid (5) (b) (iv).

[281] Ibid (5) (b) (v).

[282] Ibid (5) (b) (vi).

[283] Article 1 of the United Nations Convention against Transnational Organized Crime.

must also cross the border to hook them; without any specific agreement it is not possible to enter into any county's territory. This convention made it possible for U.N member states to catch the criminal from other states as well.

One may think that CTOC is only applicable to the conventional crimes, not to cybercrimes only; that answer is simple which has been given in Article 3(2), which says that if crimes has been "committed in more than one state" or "committed in one State but a substantial part of its preparation, planning, direction or control takes place in another states," "committed in one State but involves an organized criminal group that engages in criminal activists in more than one State"[284] such as terrorist groups those who are involved in heinous crimes and is "committed in one State but has substantial effects in another State."[285] Criminals have no borders, wherever they find any target they attack it without any restriction or problem. Money laundering[286] is also discussed in CTOC which falls under the domain of financial crimes, where these crimes are committed and are affecting the other countries as well. Further, criminals may plan in one state and execute in other state. Therefore, these crimes are covered under this convention.

When someone is caught red-hand, while committing crime or is traced by the Investigation agencies of respective countries, then the jurisdiction[287] comes into operation whether this country has jurisdiction on not? If there is any dispute related to the jurisdiction, again CTOC plays an important role of cooperation that countries shall provide "international cooperation in all matters which are committed beyond his territorial jurisdictions."[288] Then extradition[289] treaties comes to help the agencies for bringing back the accused. If countries does not have any bilateral or

[284] Ibid, 3(2) (c).
[285] Ibid., Article 3(2) (a), (b), (c) and (d).
[286] Ibid 7.
[287] Ibid 15.
[288] Ibid 13.
[289] Ibid 16.

multilateral agreements than it encourages countries to enter into "bilateral or multilateral agreements (or arrangements) on the transfer to their territory of persons sentenced".[290] This can also be used in digital crimes.

Lack of resources and man power creates many problems for one country to fight criminals. Keeping in view this situation, particularly the situation of third world and developing countries, this convention encourages the States to "afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention."[291] What type of mutual legal assistance to be afforded by the states and what type of assistance can be requested from other states is discussed in Article 18(3) of CTOC. Following are the purposes for which assistance can be sought and provided to member states, namely "taking evidence or statements from persons" "effecting service of judicial documents"; "executing searches and seizures, and freezing"; "examining objects and sites; providing information, evidentiary items and expert evaluations"; "providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records"; "identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes"; "facilitating the voluntary appearance of persons in the requesting State Party"; "any other type of assistance that is not contrary to the domestic law of the requested State Party."[292] Moreover, if states are willing to investigate jointly then it encourages States to conclude bilateral or multilateral agreements or arrangements for investigations, prosecutions or judicial proceedings.[293] Likewise, it provides guidelines for law

[290] Ibid 17.
[291] Ibid 18 (1).
[292] Ibid 18(3).
[293] Ibid 19.

enforcement cooperation;[294] measures to enhance cooperation with law enforcement authorities;[295] training and technical assistance;[296] collection, exchange and analysis of information on the nature of organized crime;[297] and to take measures for the prevention of transnational organized crimes.[298]

3.5 UNODC work on Cyber Crimes

The United Nations Office on Drugs and Crime (UNODC) is U.N's specialized agency which is responsible to combat drugs and crimes. Frequently cyber crimes are discussed on UNODC forum because of its expertise in relevant fields as discussed in Article 8 of the Salvador Declaration.[299] This is only one organization under U.N umbrella, which provides expertise to states to investigate electronic crimes in their jurisdictions. In Salvador Declaration, it is further encouraged for the "member States to cooperate, including through information-sharing, in an effort to address evolving transnational criminal threats."[300] The cyber crimes are transnationals affecting the international community at large, according to this declaration states must adopt measures to share information with other countries to reduce the cyber crime among the member states. It also provides for States "to take appropriate legal measures to prevent, prosecute and punish economic fraud and identity-related crime,"[301] all these crimes come under the domain of computer related crimes which are disturbing the corporations at large causing billions of dollars loss to the governments and private organizations. Furthermore, it is recognized in Salvador Declaration "that the development of information and communications technologies and the increasing use of the

[294] Ibid 27.
[295] Ibid 26.
[296] Ibid 29.
[297] Ibid 28.
[298] Ibid 31.
[299] Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World.
[300] Article 13 of "Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World".
[301] Article 15, ibid.

Internet create new opportunities for offenders and facilitate the growth of crime."[302] Hence, states are bound to enact strict legislation to fulfill international obligations.

Salvador Declaration is not meant for conventional crimes only, the internet related crimes are also discussed in it; for criminals youth is easy target for them, keeping in view the importance of youth, it provides that "we (the member states of UNODC) realize the vulnerability of children, and we call upon the private sector to promote and support efforts to prevent child sexual abuse and exploitation through the Internet."[303] Besides UNODC also provides technical assistance and training to U.N member states for prevention, detection and investigation of digital crimes; Article 41 of this declaration offer that;

> UNODC upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.[304]

Further expanding the scope of UNODC, this declaration assigned a greater role to this organization to conduct a comprehensive study of the problems of cyber world and provide assistance in national legislation as well.

> "We (member states of UNODC) invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange

[302] Article 39, ibid.
[303] Article 40, ibid.
[304] Article 41, ibid.

of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cyber crime.[305]

After getting the mandate, UNODC prepared a detailed report titled "Comprehensive Study on Cyber crime"[306] to help the member states to formulate their legislations. This report consists of eight chapters which cover the following topics;

i. Connectivity and cybercrime;
ii. The global picture;
iii. Legislation and frameworks;
iv. Criminalization;
v. Law enforcement and investigations;
vi. Electronic evidence and criminal justice;
vii. International cooperation; and
viii. Prevention.

Though, this is comprehensive study on cyber crimes but all topics are not relevant for this research, chapter three is important which "examines the role of national, international and regional legislation and frameworks in the prevention and combating of cybercrimes."[307] While the legislation in Pakistan is not up to the prescribed international standards, in other words it is justified to say that Pakistan does not have any legislation pertaining to cybercrime. The ETO is

[305] Article 42, ibid.

[306] This report was prepared for the open-ended intergovernmental expert group on cybercrime by Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, UNODC. However, this report has not been formally edited and remains subject to editorial changes. This report can be accessed on UNODC website.

[307] *Comprehensive Study on Cybercrime* (New York: United Nations, 2013), 51.

not sufficient to deal with digital crimes, as it contain only few sections which are relevant to computer crimes.

UNODC discovers that legislation is required in all areas, "including criminalization, procedural powers, jurisdiction, and international cooperation and internet service provider responsibility and liability."[308]

Evidence is the most important fact relevant to the guilt or innocence of any person at trial and in awarding punishment to the criminals, if evidence is not available or the evidence is weak; the chances of awarding punishment will be lesser and it will be a fatal exercise. In cyber crimes, evidence exists in electronic or digital form. Chapter six of this study (UNODC study) highlight the importance of digital evidence in cyber crimes, "starting from the need to identify, collect and analyse electronic evidence through digital forensics."[309] This chapter also examines the "admissibility and use of electronic evidence in criminal trials, and demonstrates how a range of prosecutorial challenges can impact on criminal justice system performance."[310] Other useful booklet published by UNODC is "Crime scene and physical evidence awareness for non-forensic personnel"[311] which has lot of significance for investigators.

Understanding the sensitivity of the cyber crime, UNODC has prepared a lot of books and reports to assist the world to carry out work on cyber laws to tackle the emerging situations, *inter alia* are the "The Use of the Internet for the Terrorist Purposes"[312] is the draft document prepared by the UNODC for international community for understanding of cyber crimes and measures which are necessary for prevention of these crimes.

---

[308] Ibid.

[309] Ibid, 157.

[310] *Comprehensive Study on Cybercrime*, 157.

[311] *Crime scene and physical evidence awareness for non-forensic personnel* (New York: United Nations, 2009).

[312] *The Use of the Internet for the Terrorist Purpose* (Vienna: United Nations, 2012).

Terrorist are expanding their activities from the conventional methods to the Internet to achieve their objectives, "use of the Internet for terrorist purposes is a rapidly growing phenomenon, requiring a proactive and coordinated response from Member States."[313]

> The UNODC plays a key role in providing assistance to Member States, in furtherance of its mandate to strengthen the capacity of national criminal justice systems to implement the provisions of the international legal instruments against terrorism, and does so in compliance with the principles of rule of law and international human rights standards.[314]

The UNODC is providing assistance in all matters related to crimes, to prevent terrorism from U.N member states. In 2011, the General Assembly, in its resolution 66/178, reaffirmed the mandate of UNODC "to continue to develop specialized legal knowledge in the area of counter-terrorism and pertinent thematic areas of relevance to the mandate of the Office and to provide assistance to requesting Member States with regard to criminal justice responses to terrorism, including, where appropriate, nuclear terrorism, the financing of terrorism and the use of the Internet for terrorist purposes, as well as assistance to and support for victims of terrorism."[315] Thus, the UNODC has power to provide assistance to all U.N member states to prosecute criminals who are using the internet for their illegal activities. Despite increasing threat posed by "terrorists' use of the Internet in recent years, furthermore, there is limited specialized training available on the legal and practical aspects of the investigation and prosecution of terrorism cases involving the use of the Internet."[316] Besides addressing the importance of developing integrated, specialized knowledge to respond to

[313] Ibid, v.
[314] Ibid.
[315] A/RES/66/178. Article 4 of this resolution is produced in the main text.
[316] *The Use of the Internet for the Terrorist Purpose* (Vienna: United Nations, 2012), v.

the technical assistance needs of (UN) Member States in combating this continually evolving threat."[317]

3.6 Establishment of the UN Cyber Crime Court

Whether there is a dire need for establishment of cyber crime court at International level as International Court of Justice (ICJ) or International Criminal Court (ICC)? Whether existing ICC setup can be opted for this purpose or not? Some people may think that cyber space does not have any clear boundary or border, but that's true, as the criminal is residing in one state and attacking other country.

Cyberspace is in great need for coordination, cooperation and legal measures among all nations, for a collective response to the increasing cyber threats besides creating awareness among the international community. A Global Virtual Taskforce (GVTF) for the Internet should be established with key stakeholders in the global ICT industry, financial service industry, academia, multi-national organizations, non-governmental organizations, corporations, private sector, and the global law enforcement agencies coordinated by U.N or UNODC or ITU. If GVTF is established then it will help the states to investigate the cyber-space crimes.

An independent International Court for Cyberspace is indispensable to enable countries to adopt measures on global cyber attacks of the most serious nature. Whereas harmony in cyberspace can be protected by international law. This can also be guaranteed by expanding the jurisdiction of the ICC.

Nobody has been investigated, prosecuted and sentenced in most serious cyber attacks in previous years, due to non-cooperation and lack of international forum. Such acts can be included in a treaty

[317] Ibid.

for cyberspace to investigate and prosecute the criminals. Further, it will help the states to avoid jurisdiction issues. The jurisdiction of this court or tribunal should not cross the most serious cyber crimes of concern to the international community as a whole.

International Court for Cyberspace can be established by the U.N. Security Council. The Security Council under chapter seven of U.N charter can establish an International Court for cyberspace for the "investigation, prosecution, and sentencing of global cyberattacks, as the cyberattacks are global threat to the peace"[318] of international community, which are covered under said charter.[319] However, establishment of International Court is not the focus of this research. If this court is established it will bring so many blessing for the world. U.N. is also working to establish a court for cybercrimes.

Few decades ago, countries concentrated on their own protection. But, now the scenario has changed, it is no longer a question of a nation protecting its own security, it is a question of the global community protecting itself. When criminals are crossing the borders of their own countries and affecting other nations, why not there be an International Court dealing with this problem. While investigating the crime, the Investigator has to the cross other country's boundary, which is not permissible in many cases, hence the offender cannot be convicted due to lack of cooperation by the other country.

3.7 Work of other Regional and International Organizations

Currently there is little international legislation that contains criminal defense mechanisms against cyber crimes. There are, however, a few multi-jurisdictional legislations exist. The U.N, UNODC,

[318] Article 39 of chapter seven of the U.N charter is provided for detail reading. The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.

[319] U.N. CHARTER, art. 39.

ITU and EU are not the only leaders of the world for the cyber legislation, other regional organizations has also worked on prevention of cybercrimes, but those measures are limited. Though, main focus of this study is on U.S legislation, therefore other regional and international work is discussed briefly below.

1- The Commonwealth of Independent States: (CIS)

Agreement on Cooperation in Combating Offences related to Computer Information (2001)

2- The Commonwealth:

Model Laws on Computer and Computer-related Crime (2002)/Electronic Evidence (2002)/Harare Scheme

3- The Shanghai Cooperation Organization:

Agreement on Cooperation in the Field of Information Security (2009)

4- League of Arab States:

Convention on Combating Information Technology Offences (2010)

5- Caribbean:

ITU/Caribbean Community/CTU Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010)

6- Pacific:

ITU/Secretariat of the Pacific Community Model Law on Cybercrime (2011)

7- Africa

EAC Legal Framework for Cyber laws (2008)

ECOWAS Directive on Fighting Cybercrime (2011)

COMESA Cybersecurity Draft Model Bill (2011)

African Union Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (2012)

SADC Model Law on Computer Crime and Cybercrime (2012)

This is not the whole work which has been carried out by the different organizations, there is lot of work which has been done by the regional and international organization to combat digital crimes.

3.8 ITU and Cyber Laws

Mostly the internet is accessed through telephone cables, without the use of these devices, transmission of data is problematic assignment. Due to single technical standards the Internet services are globally available, whereas the legal frameworks that address cybercrime can differ significantly and legislation plays an important role, including as part of preventive strategies.

The International Telecommunication Union (ITU) is United Nations specialized agency for ICT, which provides a unique platform to address cyber threats and cyber crime; since cyber security is a multidimensional issue, cutting across different sectors and stakeholders. In May 2011, ITU and UNODC signed a Memorandum of Understanding for capacity building and related matters, both are providing many services, including assessment, legislation, capacity building and technical assistance.

Keeping in view the development in online business industry ITU decided to help developing countries to legislate, create awareness and facilitate in investigation. ITU has facilitated these countries to take security measures to protect online business transactions and safeguard people from different frauds. Consequently, ITU has prepared many books and reports to help developing countries to understand the true nature of these

crimes. "Understanding Cyber crime: Phenomena, Challenges and Legal Response"[320] is the ITU report which has been prepared by Prof. Dr. Marco Gercke for the developing countries. The purpose of this report is to "assist countries in understanding the legal aspects of cybersecurity and to harmonize legal frameworks" of ITU members, particularly the developing countries.

There are six chapters in this report, 6.7 of this report is very important because it deals with "Liability of the Internet Providers". Internet service providers (ISP) are center of "criminal investigations involving offenders who use the ISPs' services to commit an offence, the providers located within the country's national borders are a suitable subject for criminal investigations without violating the principle of national sovereignty."[321] However, it is difficult to take help beyond the country's jurisdiction without explicit agreement or treaty.

Cyber crime can not be committed without the involvement of the ISPs, whether they have ability to prevent these crimes or not. One may think that the ISPs are not competent to avoid the commission of an offence. This is not the case, they are able to prevent such crimes by providing information to the investigation agencies. The work of law-enforcement agencies very often depends on cooperation of, and with ISP, if they are not providing the relevant data and IP address location, then it will be very difficult to trace the cyber-criminals. Resultantly, some liability also falls on ISPs to provide relevant and accurate data to law enforcement agencies. (On this topic U.S has provided ample legislation which will be discussed in relevant part of this research).

---

[320] Marco Gercke. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva: International
Telecommunication Unit, 2012. A new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries published by ITU in April 2009.

[321] *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* (Geneva: International Telecommunication Unit, 2012), 281.

States refer to the means of criminal law which enable investigation of acts of cyber crime without adequate criminalization, law enforcement agencies will not be able to carry out investigations and identify those who put security at risk.

3.9 Comparison of Pakistani and U.S.A legislations

In Pakistan the legal regime of cyber crimes is not keeping pace with the modern international standards, whereas the U.S legislation is covering almost all fields of present regime's demands. Pakistan does not have adequate legislation to keep pace with the growing trends of cyber crimes, therefore, instead of comparing Pakistani legislation with U.S legislation, Pakistani legislation will be discussed at the end of U.S legislation. U.S telecommunication, computer, privacy, decency, surveillance, intellectual property, spyware and espionage laws will be discussed.

The Internet is based upon connecting line which is usually provided by Telecom industry to access the internet facility. Therefore, before going through any other legislation it is important to discuss the Telecommunications laws of U.S and Pakistan respectively to understand whether there is any remedy provided in those Acts or not?

Advancement in IT made is easy to transmit information easily including wireless telephones; prudent consumer wants more protection to keep pace with advance communications technology to ensure protection of privacy and time; to protect the privacy of wireless phone user it was necessary to prohibit the use of unsolicited transmission. Therefore the U.S. enacted the Wireless Telephone Spam Protection Act (WTSPA) to deal with this issue, a new provision in 47 U.S.C. 227(b) (e) was inserted in "Communications Act of 1934" through WTSPA to keep pace with the

advancement of IT which says "to use any covered messaging system to transmit an unsolicited advertisement."[322]

Every telecommunications carrier has the duty "for the transmission and routing of telephone exchange service and exchange access"[323] which provides "access to advanced telecommunications and information services in all regions,"[324] including the rural, high cost areas,[325] schools, health cares and libraries[326] and direct-to-home satellite services.[327] Meaning thereby, its primary source for providing access for the internet services. Further, carrier can provide video programming services as well.[328] Moreover, it will not disclose the confidential information in any case, and it is bound by law to protect that information.[329]

It is established principle that the services provided by Telecom sector are being used while committing cybercrimes. Where it is used for research, information sharing and communication it is also used for illegal activities as well, ''Communications Decency Act (CDA) of 1996'' prohibits these activities by amending the Telecommunication Act of 1934. Any person "by means of a telecommunications device knowingly makes, creates, or solicits,"[330] and ''initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person";[331] or do any act "knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated

---

[322] 47 U.S.C. 227(b) (e).
[323] 47 U.S.C. 251 (a) (c) (2) (a).
[324] 47 U.S.C. 254 (b) (2).
[325] 47 U.S.C. 254 (b) (3).
[326] 47 U.S.C. 254 (b) (6).
[327] 47 U.S.C. 605 (e) (4).
[328] 47 U.S.C. 651.
[329] 47 U.S.C. 222 (a).
[330] 47 U.S.C. 223 (a) (1) (A) (i).
[331] 47 U.S.C. 223 (a) (1) (A) (ii).

the communication";[332] "makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications"[333]; "makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number"[334] makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication"[335] "knowingly permits any telecommunications facility under his control to be used for any activity prohibited" shall be liable to fine or imprisonment or both. Further, in subsection (d) has provided many other things which are not permissible for the computer user to do the same in addition to this, if anybody "knowingly uses an interactive computer service to send to a specific person or persons under 18 years of age;[336] or

> uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication;[337]

or permits any telecommunications facility under such person's control to be used for an activity prohibited, with the intent that it be used for such activity, shall be fined, or imprisoned not more

---

[332] 47 U.S.C. 223 (a) (1) (B) (i) &(ii).
[333] 47 U.S.C. 223 (a) (1) (C).
[334] 47 U.S.C. 223 (a) (1) (D).
[335] 47 U.S.C. 223 (a) (1) (E).
[336] 47 U.S.C. 223 (d) (1) (A).
[337] 47 U.S.C. 223 (d) (1) (B).

than two years, or both."[338] Law permits the operators to block any unwanted program which provides "sexually explicit adult programming or other programming that is indecent on any channel of its service primarily dedicated to sexually-oriented programming, a multichannel video programming distributor shall fully scramble[339] or otherwise fully block the video and audio portion of such channel so that one not a subscriber to such channel or programming does not receive it"[340] and the distributor can also limit the access to the children by not providing such programming during the day time.[341]

In addition to this, cable operator may refuse to transmit any public access,[342] or leased access program or portion of a leased access program which contains obscenity, indecency, or nudity".[343] Above mentioned provisions are not limited to the manual publication of obscene material only, these are also applicable to cybercrimes as discussed in 18 U.S.C 1462 and 1465 respectively.

Question arises whether private individual or parents can block access to offensive material or not? U.S legislature provide "guidelines and recommend procedures for the identification and rating of video programming that contains sexual, violent, or other indecent material about which parents should be informed before it is displayed to children";[344] "with respect to any video programming that has been rated, and in consultation with the television industry, rules requiring distributors of such video programming to transmit such rating to permit parents to block the display of video programming that they have suggested inappropriate for their children."[345] Further, it also imposes

[338] 47 U.S.C. 223 (d) (2).
[339] Scramble means to rearrange the content of the signal of the programming so that the programming cannot be viewed or heard in an understandable manner.
[340] 47 U.S.C. 641 (a).
[341] 47 U.S.C. 641 (b).
[342] 47 U.S.C. 531(e).
[343] 47 U.S.C. 532(c) (2).
[344] 47 U.S.C. 303(w) (1).
[345] 47 U.S.C. 303(w) (2).

restrictions on television (TV) manufacturers to manufacture such TV which have capacity to block programs,[346] besides it also impose few restriction on imported TVs.[347]

The Internet service providers (ISPs) are cause of flow of information from one place to any other place whether they are liable or not for any offence, committed by using their services. U.S law provides that "no provider or user of an interactive computer service[348] shall be treated as the publisher or speaker of any information provided by another information[349] content provider",[350] Furthermore, service provider will not be liable for account of "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected";[351] "any action taken to enable or make available to information content providers or others technical means to restrict access to material".[352] Moreover, service provider will not be accountable for criminal,[353] intellectual property,[354] and communication privacy laws.

In case of any investigation the service provider is responsible to provide relevant information to investigating agency and he will take proper measures for assistance to such agencies. The assistance capability requirements are that the "telecommunications carrier shall ensure that its

---

[346] 47 U.S.C. 303(x)

[347] 47 U.S.C. 303(c) (1).

[348] The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

[349] The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.

[350] 47 U.S.C. 230 (c) (1).

[351] 47 U.S.C. 230 (c) (2) (A).

[352] 47 U.S.C. 230 (c) (2) (B).

[353] 47 U.S.C. 230 (d) (1).

[354] 47 U.S.C. 230 (d) (2).

equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of expeditiously isolating and enabling the government, (pursuant to a court order or other lawful authorization), to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government"[355]; "expeditiously isolating and enabling the government, to access call-identifying information that is reasonably available to the carrier"[356] "delivering intercepted communications and call-identifying information to the government, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier";[357] "facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service".[358] Though, Communications Assistance for Law Enforcement Act (CALEA), 1994, provides provisions for assistance but does not allow design or systems configuration for such purposes. This does not authorize any officer or law enforcement agency "to require (or prohibit the adoption of)[359] any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services".[360]

[355] CALEA, S. 103 (a) (1).
[356] CALEA, S. 103 (a) (2).
[357] CALEA, S. 103 (a) (3).
[358] CALEA, S. 103 (a) (4).
[359] CALEA, S. 103 (b) (1) (B).
[360] CALEA, S. 103 (b) (1) (A).

Furthermore, the service provider is not responsible for "decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication"[361] however he will allow the law enforcement agencies to monitor any activity at his premise[362] besides providing assistance in mobile services.[363] CALEA also improves the telecommunications carriers to fulfill maximum capacity building requirements,[364] to ensure Systems Security and Integrity[365] cooperation of equipment manufacturers and providers of telecommunications support services,[366] technical requirements and standards,[367] and enforcement of courts orders in given time period.[368] If service provider is not assisting law enforcement agencies then Attorney General will move an application before concerned court for permission and after that service provider will provide relevant information and allow for surveillance,[369] if again refuses to provide information, he will pay a fine of ten thousand dollars per day from the day of order till he provides the information.[370] Cordless Telephone[371] and Radio-Based Data Communications[372] are also covered under this law.

Privacy is the fundamental right of every citizen, whether law enforcement agencies are allowed to intercept communication? If allowed under what circumstance? U.S Electronic Communications Privacy Act (ECPA) 1986[373] deals with this issue. The service provider shall not

---

[361] CALEA, S. 103 (b) (3).
[362] CALEA, S. 103 (c).
[363] CALEA, S. 103 (d).
[364] CALEA, S. 104.
[365] CALEA, S. 105.
[366] CALEA, S. 106.
[367] CALEA, S. 107.
[368] CALEA, S. 108.
[369] 18 U.S.C, 2252.
[370] 18 U.S.C, 2252 (c) (1).
[371] CALEA, S. 202.
[372] CALEA, S. 203.
[373] This Act was amended vide "Electronic Communications Privacy Act Amendments Act of 2011".

disclose any information to any person or entity.[374] However, he can divulge with "lawful consent of the originator, or any addressee, or intended recipient of such communication"[375], to a person employed or authorized, or whose facilities are used, to forward such communication to its destination"[376], which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency".[377] If above mentioned section is violated the person who's "wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation" of this Act can claim damages.[378] Any attorney on behalf of Government can move an application before competent court for authorization to intercept the communication for investigation purposes,[379] which can also permit installation of tracking device in mobile phones.[380] Moreover, this Act authorizes Court to issue restraining order, if someone is engaged in illegal interception.[381]

If someone is involved in unlawful access then he can be prosecuted in civil court as well as in criminal court. If someone internationally accesses without authorization a facility and "thereby obtains, alters, or prevents authorized access to a wire or electronic communication"[382] shall be punished. However, the quantum of punishment is different for different intentions, "if the offence is committed is commercial advantage, malicious destruction or damage, or private commercial gain" shall be liable to pay $ 250,000 or imprisonment for one year (in case he is punished first time).[383]

---

[374] 18 U.S.C, 2511 (3) (a).
[375] 18 U.S.C, 2511 (3) (b) (ii).
[376] 18 U.S.C, 2511 (3) (b) (iii).
[377] 18 U.S.C, 2511 (3) (b) (iv).
[378] 18 U.S.C, 2520.
[379] 18 U.S.C, 2516 (b) (3).
[380] 18 U.S.C, 3117 (a).
[381] 18 U.S.C, 2521.
[382] 18 U.S.C, 2701 (a) (1) & (2).
[383] 18 U.S.C, 2701 (b) (1) (A).

Under this Act no one is entitled to disclose any information except permitted by law;[384] government after following due course of law, can obtain such information up-to 180days,[385] while issuing order for communication information the court should observe that this particular information is needed for investigation or inquiry purpose, if government establish the need then court will allow to get wire or electronic communication information.[386] Moreover, no cause of action lie against any service provider or his employees if the information is provided against court order.[387]

Interception and devices used for intelligence gathering or for information gathering including pen register, trap and trace devices are also prohibited by this Act except as allowed by law.[388] An attorney for the government can make an application to competent court for the installation of these devices,[389] however, if needed the service providers shall assist the law enforcement agencies to install such devices.[390]

Cable Communications Policy Act (CCPA) of 1984 is core legislation which is relevant to cable matters, basic purpose of this Act is to facilitate and establish cable channels for public, educational and government purposes.[391] However, this is extended to commercial use as well.[392] Service provider can collect identifiable information,[393] but no one can intercept the communication without the permission of court or authorized by law,[394] but still consumer rights will be

[384] 18 U.S.C, 2702.
[385] 18 U.S.C, 2703 (a).
[386] 18 U.S.C, 2703 (d).
[387] 18 U.S.C, 2703 (e).
[388] 18 U.S.C, 3121 (a).
[389] 18 U.S.C, 3122 (a).
[390] 18 U.S.C, 3124 (a).
[391] 47 U.S.C, 531.
[392] 47 U.S.C, 532.
[393] 47 U.S.C, 551.
[394] 47 U.S.C, 553.

protected.[395] If any person intercepts communication than he will be liable to pay $ 50,000 and imprisonment of two years.[396] Furthermore, cable operators are exempted from civil and criminal liabilities.[397] Although penalty is imposed for transmitting obscene program; imprisonment of two years and $10,000 fine.[398]

Computer Fraud and Abuse Act (CFAA) of 1986 is basic legislation pertaining to computer frauds and misuse of it. CFAA has prescribed different punishments for those who are intentionally involved, in (without authorization) access any government or private computer and alter, damage, destroy, modify, or impair any record shall be liable to pay the compensatory damages and imprisonment up-to ten years.[399] However, law enforcement agencies are exempted from this law.[400] In United States v. Drew, the defendant was acquitted from the charge of cyberbullying due to insufficient evidence.[401]

Fraud and Related Activity in Connection with Computers (FRACCA) Act of 1996, further elaborates the definition and includes many other things which were not covered under the CFAA, and enhances above mentioned crimes and increases punishments up-to twenty years of imprisonment. However, it particularly discusses unauthorized access to financial institution's computer that anybody "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer."[402] This provision is missing in CFAA, which is relevant for

[395] 47 U.S.C, 552.
[396] 47 U.S.C, 553 (b) (2).
[397] 47 U.S.C, 558.
[398] 47 U.S.C, 559.
[399] 18 U.S.C, 1030 (c) (3) (B).
[400] 18 U.S.C, 1030 (f).
[401] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).
[402] 18 U.S.C, 1030 (a) (2) (A).

corporations, further it covers "transmission of a program, information, code, or command"[403] which causes damage to the computer system, while leaving the corporation to face many difficulties. Punishments of these crimes depends upon different natures of the offences, however, imprisonment can be awarded up-to twenty years,[404] and courts are competent to forfeit any person's interest or property.[405] Further, FRACCA authorizes, U.S Secret Service[406] and Federal Bureau of Investigation[407] (FBI) to investigate digital crimes.[408] Law enforcement agencies under this law are exempted (if they after authorization are investigating any crime)[409] but they will be liable to pay compensatory damages in case they cause any loss or damage.[410]

The U.S has adopted many measures to combat these issues, including to strengthen the judiciary and law enforcement agencies by legislation. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001" is the important legislation dealing with many issues including digital crimes and money laundering.

The U.S.A PATRIOT Act has given a task to the Director of U.S Secret Service to develop a national network of electronic crimes task forces[411] "for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."[412] There are many other powers which have

---

[403] 18 U.S.C, 1030 (a) (5) (A).
[404] 18 U.S.C, 1030 (c)
[405] 18 U.S.C, 1030 (i) (1).
[406] 18 U.S.C, 1030 (d) (1).
[407] 18 U.S.C, 1030 (d) (2).
[408] The FBI is the primary authority to investigate the following cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, and Restricted Data.
[409] 18 U.S.C, 1030 (f)
[410] 18 U.S.C, 1030 (g)
[411] This task force is based on the New York Electronic Crimes Task Force model, throughout the United States.
[412] USA PATRIOT Act, S.105.

been bestowed under this Act such as authority to intercept wire, oral, and electronic communications relating to terrorism[413] and computer fraud and abuse offenses;[414] "authority to share criminal investigative information;[415] seizure of voice-mail messages pursuant to warrants;[416] scope of subpoenas for records of electronic communications;[417] emergency disclosure of electronic communications to protect life and limb;[418] access to records and other items under the Foreign Intelligence Surveillance Act (FISA);[419] Pen Register and Trap and Trace Authority under FISA;[420] interception of computer trespasser communications;[421] nationwide service of search warrants for electronic evidence;[422] trade sanctions,[423] and assistance to law enforcement agencies.[424] If investigating officer or law enforcement agency violates any provision of this Act, will be punished and disciplinary action shall be taken against him" [425] and "no cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person[426] that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act".[427]

The U.S.A PATRIOT Act's title III is related to "International Money Laundering Abetment and Antiterrorist Financing Act of 2001" which discuss many issues related to money laundering. Though it discuss money laundering which is financial crime but manual money laundering is

---

[413] Ibid, 201.
[414] Ibid, 202.
[415] Ibid, 203.
[416] Ibid, 209.
[417] Ibid, 210.
[418] Ibid, 212.
[419] Ibid, 215.
[420] Ibid, 214.
[421] Ibid, 217.
[422] Ibid, 220.
[423] Ibid, 221.
[424] Ibid, 222.
[425] Ibid, 223.
[426] Including any officer, employee, agent, or other specified person thereof.
[427] 50 U.S.C, 1805 (h).

discussed in this Act, not digital. So, it will be discussed in money laundering section. Department of Development and Support of Cybersecurity Forensic Capabilities is "responsible to establish regional computer forensic laboratories and provide support to existing computer forensic laboratories to provide forensic examinations of seized or intercepted computer evidence;"[428] and "to provide training and education for law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer related crime."[429] Above mentioned department is also responsible to investigate cyber terrorism.

U.S Homeland Security Act (HSA) of 2002 discusses U.S Security including cyber-security such as enhancement of Non-Federal cybersecurity,[430] net guard,[431] enchantment of cybersecurity,[432] and use of technology in safeguarding the country. In addition to this, it discusses "authority to share electronic, wire, and oral interception information";[433] and "information acquired from an electronic surveillance."[434] Cyber Security[435] Research and Development Act (CSRDA) provides for the establishment of Cyber Security Research Centers, funding for computer and network security research and development and research fellowship programs.

Unlawful Internet Gambling Enforcement Act of 2006 discusses the internet gambling, which is primarily funded through personal use of payment system instruments, credit cards, and wire transfers. Where Internet gambling sites or the banks, which represent such sites, are used to do this illegal business, which creates debt collection problems for insured depository institutions and

---

[428] USA PATRIOT Act, S.816 (a) (1).
[429] Ibid, 816 (a) (2).
[430] 6 U.S.C, 143.
[431] Ibid, 144.
[432] Ibid, 145.
[433] 18 U.S.C, 2517 (7).
[434] 50 U.S.C. 1806.
[435] Cybersecurity Information Sharing Act of 2015 is introduced in the Congress, but not passed yet.

the consumer credit industry. Feeling the need of present era, the U.S government enacted this law, which prohibits the internet gambling, that provides the "acceptance of any financial instrument for unlawful Internet gambling."[436]

Privacy Protection Act of 1980 authorizes the law enforcement agencies to search for materials if "there is cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate"[437] and "there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to a human being."[438] In *mala fide* intention investigator can be prosecuted and he will be liable to pay damage[439] and damages.[440]

Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E–PRIVACY) Act allows the use of encryption, development and manufacture, sale, distribution and import of encryption products, regardless of the encryption algorithm selected, encryption key "length chosen, existence of key recovery or other plaintext access capability, or implementation or medium used."[441]

Spyware Control and Privacy Protection Act of 2000 protects the privacy of computer users, which provides that "any computer software made available to the public (whether by sale or without charge), that includes a capability to collect information about the user of such computer software, the hardware on which such computer software is used, or the manner in which such computer software is used, and to discloses information to any person other than the user of such computer

[436] 31 U.S.C, 5363.
[437] 42 U.S.C, 2000 (aa) (1) (a) (1).
[438] 42 U.S.C, 2000 (aa) (1) (a) (2).
[439] 42 U.S.C, 2000 (aa) (f) (a).
[440] 42 U.S.C, 2000 (aa) (6) (a).
[441] E–PRIVACY, S. 101.

software, shall include " a clear and conspicuous written notice, on the first electronic page of the instructions for the installation of such computer software, that such computer software includes such capability";[442] or "a description of the information subject to collection and the name and address of each person to whom such computer software will transmit or otherwise communicate such information";[443] and "a clear and conspicuous written electronic notice, in a manner reasonably calculated to provide the user of such computer software with easily understood instructions on how to disable such capability without affecting the performance or operation of such computer software for the purposes for which such computer software was intended".[444] However, collecting person shall establish and maintain reasonable procedures to protect the security, confidentiality, and integrity of such information.[445] Moreover information collector can disclose such information to law enforcement agency under court order[446] but this information shall not be disclosed further and court will impose restriction.[447] Victim can sue for the recovery of damages.[448] To protect the privacy of the computer owner, it is prohibited to install any software or program without the consent of computer owner.[449]

Enhanced Consumer Protection against Spyware Act (ECPSA) of 2005 has enhanced punishments. If anybody violates above mentioned Act, shall be penalized such deceptive acts or practices by tripling the amounts prescribed in the Federal Trade Commission Act 11 (15 U.S.C.

---

[442] Spyware Control and Privacy Protection Act of 2000, S. 2 (a) (1) (A).
[443] Ibid, S. 2 (a) (1) (B).
[444] Ibid, S. 2 (a) (1) (C).
[445] Ibid, S. 2 (a) (6).
[446] Ibid, S. 2 (d) (1)
[447] Ibid, S. 2 (d) (2)
[448] Ibid, S. 2 (e) (1) (B).
[449] Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY BLOCK Act), S, 2 & 3.

41 et seq.),[450] $3,000,000 penalty for each pattern or practice violation[451] disgorge and seize any ill-gotten gains procured through such deceptive acts or practices.[452]

Personal Data Privacy and Security Act (PDPSA) of 2005, provides "to prevent and mitigate identity theft; to ensure privacy; and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information."[453] The basic purpose of this legislation is to "ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the privacy, security, confidentiality, integrity, storage, and disposal of personally identifiable information".[454] It prohibits "fraud and related criminal activity"[455] and "organized criminal activity in connection with unauthorized access to personally identifiable information";[456] "concealment of security breaches involving personally identifiable information";[457] "aggravated fraud in connection with computers";[458] and "to award grants to establish and develop programs to increase and enhance enforcement against crimes related to fraudulent, unauthorized, or other criminal use of personally identifiable information".[459] Further, this Act makes it compulsory for business entity to take measures for data protection and security of identifiable information.[460]

---

[450] ECPSA, S. 5 (b).
[451] ECPSA, S. 5 (c) (1).
[452] ECPSA, S. 5 (d).
[453] PDPSA preamble.
[454] PDPSA, S.401.
[455] 18 U.S.C, 1030 (a) (2).
[456] 18 U.S.C, 1030(a) (2) (D).
[457] 18 U.S.C, 1039.
[458] 18 U.S.C, 1030 A.
[459] PDPSA, S.201.
[460] PDPSA, S.401 (b)

Social security numbers are also protected,[461] if any business entity discloses information related to business transactions and records, it must follow the restriction imposed by this Act.[462]

Identity Theft and Assumption Deterrence Act (ITADA) of 1998, is related to identity thefts.[463] ITADA has defined identity theft that anybody "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of law, or that constitutes a felony under any applicable law";[464] for this offence criminal will be sentenced and imprisonment up-to twenty years[465] and his property will be forfeited if it is used or intended to be used.[466] If anyone attempts or conspires to commit any offence, will also be punished as he had actually committed that offence.[467] To facilitate the victim, U.S government has also introduced "centralized complaint and consumer education service for victims of identity theft".[468] Moreover, Identity Theft Penalty Enhancement Act (ITPEA) has enhanced punishment two years further in addition to the "punishment provided for such felony",[469] and for terrorism offences 5years punishment is awarded in addition to the punishment provided for such felony.[470]

Anti-Counterfeiting Consumer Protection Act (ACCPA) of 1996[471] deals with commercial counterfeiting. This Act includes the computer programs, computer program documentation, and

---

[461] PDPSA, S.501
[462] PDPSA, S.502.
[463] Identity Theft and Tax Fraud Prevention Act of 2015 bill is presented in the congress, and not passed yet.
[464] 18 U.S.C, 1028 (a) (7).
[465] 18 U.S.C, 1028 (b) (B) (3).
[466] 18 U.S.C, 1028 (b) (B) (5).
[467] 18 U.S.C, 1028 (f).
[468] 18 USC 1028.
[469] 18 USC 1028A (a) (1).
[470] 18 USC 1028A (a) (2).
[471] This Act was amended later on vide "Anti-Counterfeiting Amendments Act of 2004".

packaging. For violation of this Act, victim can claim "statutory damages up-to $100,000 per counterfeit mark per type of goods or services sold, offered for sale, or distributed."[472]

According to "Ryan Haight Online Pharmacy Consumer Protection Act (RHOPCPA) of 2008", it is "illegal to deliver, distribute, or dispense any drug by means of the Internet" without a valid prescription.[473] An online pharmacy will be responsible to display in a visible and clear manner on its homepage a statement or declaration of compliance of this Act,[474] including name, address, phone number, email of Pharmacy; name, professional degree of the pharmacist-in-charge, and a telephone number at which the pharmacist-in-charge can be contacted etc.[475] If someone violates this section, then suit will be instituted against the owner for damages, restitution, compensation or any equitable relief.[476]

Foreign Intelligence Surveillance Act of 1978 (FISA) authorize U.S government to gather electronic surveillance for intelligence purposes, with the consent of the President.[477] Employees of intelligence agency can use such devices for testing purposes to test the electronic devices.[478] Moreover, the Cyber Intelligence Sharing[479] and Protection Act (CISPA) of 2013 provides for establishment of entities for the cyber security.

Digital Millennium Copyright Act (DMCA) of 1998 was enacted to implement the World Intellectual Property Organization (WIPO) Copyright Treaty and other treaties for the protection of intellectual property rights. Copy rights are protected under section 1201 (b) of this Act;[480]

---

[472] ACCPA, S. 7.
[473] Ryan Haight Online Pharmacy Consumer Protection Act (RHOPCPA) of 2008, S.2.
[474] RHOPCPA, s.311 (a).
[475] RHOPCPA, s.311 (c).
[476] 21 U.S.C, 512 (c) (1).
[477] 50 U.S.C, 1802.
[478] 50 U.S.C, 1805.
[479] Cybersecurity Information Sharing Act of 2015 is presented in congress, but not passed yet.
[480] 17 U.S.C, 1201 (b).

nonprofit library, archives, or educational institution are exempted from this Act, however they cannot not use this exception for commercial purposes.[481] In case of infringement, civil court is competent to provide remedy including grant of temporary and permanent injunctions, award of damages (actual and statutory up-to $ 25,000), recovery of costs, profits[482] and seizure of infringed material.[483] Court will ensure that "confidential, private, proprietary, or privileged information contained in such records is not improperly disclosed or used."[484] Damages will be awarded up-to $ 500,000 and imprisonment up-to five years (in case of first time violation), and $ 1,000,000 and imprisonment up-to ten years (in case of second time violation).[485] According to Trademark Act of 1946 penalty has been increased up-to $ 2,000,000.[486] If infringer repeats offence within 3years, then the court will award triple the amount that otherwise awarded. Moreover, under this law, the service provider is not liable for any kind of action,[487] however, he is bound to provide information to the author or his agent.[488] Faculty and students are not responsible while they are acting prudently for research purposes.[489] If for maintenance or repair of machine or computer a copy of software or program is made, then this is not infringement.[490] In case, a counterfeit mark is involved, the court will award "three times such profits or damages, whichever amount is greater, together with a reasonable attorney's fee."[491]

[481] 17 U.S.C, 1201 (d).
[482] 17 U.S.C, 1203 (a).
[483] 17 U.S.C, 503 (a) (1) (C).
[484] 17 U.S.C, 503 (a) (2)
[485] 17 U.S.C, 1204.
[486] 15 U.S.C, 1117 35(c).; Prioritizing Resources and Organization for Intellectual Property Act of 2008.
[487] 17 U.S.C, 512.
[488] 17 U.S.C, 512 (h).
[489] 17 U.S.C, 512 (e).
[490] 17 U.S.C, 117.
[491] 15 U.S.C. 1117(b).

Fair and Accurate Credit Transactions Act (FACTA) of 2003, protects the identity and privacy of card holder and prohibits that "no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction."[492] In case of theft or fraud business entity is responsible to provide information without any charge.[493]

Under the E-Government Act of 2002, U.S government amended U.S.C and inserted chapter 36 in title 44 for the "management and promotion of electronic government services". There are many objectives of this Act, among them are the "compatibility of executive agency methods for use and acceptance of electronic signatures"; "federal internet portal"; "federal courts websites"; "regulatory agencies' to improve performance in the development and issuance of agency regulations by using information technology to increase access, accountability, and transparency; accessibility, usability, and preservation of government information"; to "ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government"; "enhancing crisis management through advanced information technology"; "disparities in access to the internet; common protocols for geographic information systems";[494] and to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources.[495]

National Institute of Standards and Technology (NIST) is responsible to develop, prescribe, enforce, and oversee the Standards and guidelines for national security systems.[496]

---

[492] 15 U.S.C. 1681(g) (1).
[493] 15 U.S.C. 1681(e) (4).
[494] 44 U.S.C. 3501.
[495] 44 U.S.C. 3541.
[496] 40 U.S.C, 11331.

Anybody who is "engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined or imprisoned not more than two years, or both."[497]

According to "Family Entertainment and Copyright Act of 2005" any person who uses or attempts to use any motion picture shall be fined and imprisoned not more than three years and if he commits second time than he shall be imprisoned not more than six years, and court is competent to order to destroy or forfeit the unauthorized copies.[498]

Anybody who willfully infringes a copyright, if the infringement is committed for the purposes of commercial advantage or private financial gain,[499] he will be punished under S. 2319 of title 18 and his liability will be fine and imprisonment up-to six years. Nonetheless infringement for skipping audio and video content in motion pictures is exempted.[500]

Children are the assets of coming generations, without their protection no one can protect the people from evils of the society. Keeping in view the importance of children the U.S government has enacted many laws to protect the children from sex related activities which are being carried by conventional means or by the use of the internet.

[497] 18 U.S.C, 1084 (a).
[498] 18 U.S.C, 2319 B.
[499] 17 U.S.C, 506 (a).
[500] 17 U.S.C, 110.

Protection of Children from Sexual[501] Predators Act (PCSPA) of 1998 provides that "whoever, using the mail (or any facility) knowingly initiates the transmission of the name, address, telephone number, social security number, or electronic mail address of another individual, knowing that such other individual has not attained the age of 16 years, with the intent to entice, encourage, offer, or solicit any person to engage in any sexual activity for which any person can be charged with a criminal offense, (or attempts to do so), shall be fined, or imprisoned not more than 5 years, or both",[502] and whoever knowingly use this facility to "persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution (or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so), shall be fined, or imprisoned not more than 15 years, or both."[503]

Anybody who is involved in transportation of minors for illegal sexual activity (and related crimes) shall be fined or imprisoned not more than 15 years, or both.[504] The maximum term of imprisonment for a "prior sex offense conviction shall be twice the term of imprisonment otherwise provided by law."[505] If the sexual contact that "violates this section is with an individual who has not attained the age of 12 years, the maximum term of imprisonment that may be imposed for the offense shall be twice that otherwise provided in this section";[506] and anybody using the mail (or any facility) or knowingly "transfers obscene matter to another individual who has not attained the age of 16 years, (or attempts to do so), shall be fined, or imprisoned not more than 10 years, or both."[507]

[501] 18 U.S.C, 2427.
[502] 18 U.S.C, 2425 (a).
[503] 18 U.S.C, 2422 (b).
[504] 18 U.S.C, 2423 (a).
[505] 18 U.S.C, 2426 (a)
[506] 18 U.S.C, 2444 (c).
[507] 18 U.S.C, 1470 (a).

Penalties increase in case of use of a "computer in the sexual abuse or exploitation of a child;[508] knowing misrepresentation in the sexual abuse or exploitation of a child",[509] and for pattern of activity of sexual exploitation of children.[510] Moreover, criminal[511] and civil[512] law provisions of forfeiture will also apply to these offences.

If it comes to the knowledge of electronic communication service provider that some law is being violated, he shall report such circumstances to law enforcement agency (agencies),[513] and if he willfully fails to make a report, he will be fined in the "case of an initial failure to make a report, not more than $50,000"; and in the case of any "second or subsequent failure to make a report, not more than $100,000".[514] Service provider, if he acted in good faith, will not be liable for any civil liability.[515]

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM ACT) of 2003 provides that "no person may initiate the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material."[516] It is unlawful for a person to "promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of law."[517]

---

[508] PCSPA, s.503.
[509] PCSPA, s.504.
[510] PCSPA, s.505.
[511] PCSPA, s.602.
[512] PCSPA, s.603.
[513] PCSPA, s.227 (b) (1).
[514] PCSPA, s.227 (b) (3).
[515] PCSPA, s.227 (c)
[516] 15 U.S.C, 7704 (d) (1).
[517] 15 U.S.C, 7705 (a).

Adam Walsh Child Protection & Safety Act of 2006 provides that if anybody uses "the Internet to distribute a date rape drug to any person, knowing or with reasonable cause to believe that, the drug would be used in the commission of criminal sexual conduct; or the person is not an authorized purchaser; shall be fined or imprisoned not more than 20 years, or both";[518] "penalties for coercion and enticement by sex offenders shall not be less than 10 years or for life";[519] "penalties for conduct relating to child prostitution shall be10 years or for life";[520] "penalties for sexual abuse is imprisoned for any term of years or for life";[521]and "penalties for sexual offenses against children is imprisoned for not less than 30 years or for life."[522]A person who, in the course of an offense "murders an individual, will be punished by death or imprisoned for any term of years or for life."[523]

In any criminal proceedings, "any property or material that constitutes child pornography, shall remain in the care, custody, and control of either the Government or the court,"[524] and court can deny, "any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography, so long as the Government makes the property or material reasonably available to the defendant."[525] Any person who "engages in a child exploitation enterprise shall be fined and imprisoned for any term of years not less than 20 or for life",[526] and anybody who "embeds words or digital images into the source code of a website with the intent to deceive a person into viewing material constituting obscenity shall be fined and

[518] 21 U.S.C, 841 (g) (1).
[519] 18 U.S.C, 2422 (b).
[520] 18 U.S.C, 2423 (a).
[521] 18 U.S.C, 2242.
[522] 18 U.S.C, 2241 (c).
[523] 18 U.S.C, 2245.
[524] 18 U.S.C, 3509 (m) (1).
[525] 18 U.S.C, 3509 (m) (2) (A).
[526] 18 U.S.C, 2252A (g).

imprisoned for not more than 10 years";[527] and anyone who acts to "deceive a minor into viewing material harmful to minors on the Internet shall be fined and imprisoned for not more than 20 years."[528]

Child Protection Act of 2012 provides that "any visual depiction involved in the offense involved a prepubescent minor or a minor who have not attained 12 years of age, such person shall be fined and imprisoned for not more than 20 years.[529] In case a "minor is witness or victim, the court will issue a protective order prohibiting harassment or intimidation of the minor victim or witness if the court finds evidence that the conduct at issue is reasonably likely to adversely affect the willingness of the minor witness or victim to testify or otherwise participate in criminal case or investigation."[530]

In Gramm-Leachy-Bliley Act, 1999, the Congress have provided guidelines for the protection of privacy and private information of individual as well as the customers which provides that every agency shall "establish appropriate standards for the financial institutions relating to administrative, technical, and physical safeguards, to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer"[531] and a financial institution will not provide this information to any third person except with prior notice to customer.[532] It is unlawful for any person to obtain any information of financial

[527] 18 U.S.C, 2252C (a).
[528] 18 U.S.C, 2252C (b).
[529] 18 U.S.C, 2252 (b) (2).
[530] 18 U.S.C, 1514 (C) (2).
[531] 15 U.S.C, 6801 (b).
[532] 15 U.S.C, 6802.

institutions, however the law enforcement agencies are authorized to do so.[533] Whoever violates section 521(15 U.S.C, 6821) of this Act (Gramm-Leachy-Bliley Act) shall be "fined or imprisoned for not more than 5 years, or both."[534]

Any automated teller machine operator who imposes a fee on any consumer for providing host transfer services to such consumer, to provide notice to the consumer that the fee is imposed, without such notice the operator cannot claim the fee.[535] Furthermore, "a notice to the consumer that a fee may be imposed by an automated teller machine operator, if the consumer initiates a transfer from an automated teller machine that is not operated by the person issuing the card or other means of access; and any national, regional, or local network utilized to effect the transaction", [536] and if this notice is damaged then the operator will not be responsible.[537]

Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers beyond Borders Act of 2006 (U.S. SAFE WEB Act of 2006) provides that "upon a written request from a foreign law enforcement, if the requesting agency states that it is investigating, or engaging in enforcement proceedings against, possible violations of laws prohibiting fraudulent or deceptive commercial practices, or other practices substantially similar to practices prohibited by any provision of the laws."[538] This Act further provides that U.S government can conclude an international agreement with other countries.[539]

---

[533] 15 U.S.C, 6821.
[534] 15 U.S.C, 6823.
[535] 15 U.S.C, 1693 (b) (d) (3).
[536] 15 U.S.C, 1693 (c) (a) (10).
[537] 15 U.S.C, 1693 (h) (d).
[538] 15 U.S.C, 46 (j) (1).
[539] 15 U.S.C, 46 (j) (4).

Trade secrets[540] are valuable assets of any company or corporation, which they always keep confidential and in safe custody whereas other competitors try to steal those secrets to compete with other company or corporation. The U.S enacted the "Economic Espionage Act (EEA) of 1996" to protect the valuable secrets of the companies. EEA provides that anybody;

> intending or knowingly steals, or without authorization appropriates, takes carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; attempts to commit any offense; or conspires with one or more other persons to commit any offense shall be fined not more than $ 500,000 or imprisonment not more than 15 years, or both.[541]

Any person with intent to "convert a trade secret into economic benefit of anyone other than the owner, that the offense will injure any owner of that trade secret, will be fined or imprisoned not more than 10 years, or both,"[542] and if any organization is involved to commit above mentioned offense that will be "fined not more than $ 5,000,000.[543] Government entity is exempted from above mentioned punishments."[544]

---

[540] 'Trade Secret' means "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns plans, compilations, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if the owner thereof has taken reasonable measures to keep such information secret; and the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public". 18 U.S.C, 1839 (3).

[541] 18 U.S.C, 1831.

[542] 18 U.S.C, 1832 (a).

[543] 18 U.S.C, 1832 (b).

[544] 18 U.S.C, 1833.

The court imposing sentence on a person for violation of 18 U.S.C., section 1831 and 1832, shall order in addition to any other sentence imposed, the forfeiture of his property.[545] Court is also bound to preserve the confidentially of these secrets in prosecution or proceeding.[546] In addition to criminal proceeding, the civil remedy can be availed as well.[547]

There are many crimes prevailing in our society, but the trend of cyber crime is new and complicated, the complexity is added due to great revolution of technology. If we pinpoint the issues we will find that PPC is only applicable to conventional crimes, not the cyber crimes. ETO is only meant for violation of privacy of information[548] and damage to information system,[549] and does not cover many prevailing crimes, which U.S legislation covers. Even punishment prescribed in ETO is less severe as compared to U.S. laws and are not according to severe nature of these crimes. Advance fee fraud, email frauds, cyber terrorism, electronic fraud, electronic forgery, bank fraud, data diddling, misuse of electronic system, cyber-extortion, unauthorized access to code, online child pornography, illegal sale of articles, cyber defamation, misuse of encryption, cyber stalking, unauthorized interception, spoofing, spamming, digital privacy, fake websites, fake social media accounts, internet time theft, identity theft, online gambling, salami attacks, stock robot manipulation, Trojans & key-loggers, virus/worm attacks, web defacement, web-jacking, use of encryption by terrorist and economic espionage are not covered under the Pakistani legislation. There are many laws related to Intellectual Property Rights, but they are not keeping pace with the digital privacy. Therefore, IPRs laws need to be amended according to digital requirements.

[545] 18 U.S.C, 1834.
[546] 18 U.S.C, 1835.
[547] 18 U.S.C, 1836.
[548] ETO, s.36.
[549] ETO, s.37.

Pakistani procedural law and law of evidence also need to be amended according to demands of present era.

3.10 Findings and Conclusion

In Pakistan, the legal regime of cyber crimes is not keeping pace with the modern international standards, Pakistan is far behind in digital legislation. Therefore, it is the need of present era to enactment new laws to cope with new trends of technology as per U.S and International standards. Pakistan is still relying upon the centuries old legislation to tackle digital crimes. Owing to non-availability of particular legislation the criminals are not prosecuted, if brought before the courts of law then they are acquitted in the absence of legislation and admissibility of digital evidence.

In Pakistan, legislation is required in all areas, including criminalization, procedural powers, jurisdiction, and international cooperation and internet service provider responsibility and liability (though Pakistan has legislation on ISPs but that is not sufficient).

Pakistan should also adopt the following measures to tackle this situation;

a- Improved computer security is of great importance for the current regime to tackle digital related problems;

b- Administrative changes to the criminal defense system that looks more unified laws being enacted against cyber criminals;

c- Many cyber crimes are heinous offences which must be punished, with death sentence or life imprisonment along with compensatory damages, according to the nature of offence;

d- Where possible, the transferred money should be recovered and forfeitured.

Chapter 4:

Conclusion and Recommendations

Conclusion

There are many crimes prevailing in our society, but the trend of cyber crime is new and complicated, the complexity is added due to great revolution of technology. If we pinpoint the issues we will find that existing legislation is only applicable to conventional crimes. ETO is only meant for violation of privacy of information and damage to information system, and does not cover many prevailing crimes, which U.S legislation covers. Even punishment prescribed in ETO is less severe as compared to U.S. laws and are not according to severe nature of these crimes. Cyber crimes are not covered under the Pakistani legislation. Therefore, there is a dire need to legislate on cyber crimes to protect the innocent victims.

Pakistani procedural law and law of evidence also need to be amended according to demands of present era.

Recommendations

1. Cyber privacy should be incorporated in Constitution as a fundamental right, law enforcement agencies should be stopped from interfering the private data of people, and should not be allowed to intercept without the permission of competent court.
2. Internet Service Providers will not be responsible for any offence which is committed by using their service, however they will provide information to the investigation agency after due process of law, and will be fined for violation of court order.

3. In case, wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation of law; victim should be allowed to ask for damages along with other legal remedies.
4. Corporate Espionage Act should be introduced to protect the corporate secret
5. Special courts for cybercrimes should be established at district level. Judge should be aware of cyber forensics, electronic transactions, and data protection. Judge should consider the following factors for awarding the punishment or damages according to nature of each case
    a. the possible and actual loss resulting from the offense;
    b. the level of planning involved in the offense;
    c. purposes offense, whether the offense was committed for commercial advantage or private financial benefit, or for terrorist purpose;
    d. intention for committing the offence;
    e. extent of privacy rights disturbed by the criminal;
    f. whether computer used in crime is owned by the government or corporation or any individual;
    g. whether it is creating a threat to public safety, or injury to any person; and the serious nature of the offenses;
    h. the misuse of digitized or electronic personally identifiable information, including identity theft
    i. the sale of fraudulently obtained or stolen personally identifiable information to an individual who is engaged in terrorist activity or aiding other individuals engaged in terrorist activity or finance terrorist activity or other criminal activities

j. the extent to which, the number of victims are involved in the offense, including harm to reputation, inconvenience, and other difficulties resulting from the offense,

k. the number of means of identification, identification documents, or false identification documents; and

l. other related matter to the commission of offense.

6. New tools for enforcing gambling laws on the Internet are necessary and to enact law to prohibit wire transfers to Internet gambling sites or the banks which represent such sites.
7. Online consumer protection legislation should be introduced to protect the online consumer and online business industry. Goods are not provided as per standard or not delivered, consumer protection is also mandatory.
8. Kid dot domain should be introduced to protect the children from viewing the immoral contents.
9. Qunan e Shahadat Order (law of evidence) should be amended to bring with the conformity of present era needs, and one chapter should be added for cyber evidence, including collection, seizure, preservation, and production into the court.
10. The telecommunication is directly involved for providing services to the internet user, data is transmission is very fast. There is a dire need to get the information as early as possible for the investigation purposes. If the telecommunication industry is not providing latest data and detail of it. It will make very difficult for law enforcement agencies to investigate crimes. If ample legislation is provided to keep and protect the relevant data. Then it will bring many opportunities for law enforcement agencies for collection of sufficient evidence.
11. Proper legislation should be introduced for online distribution of hate material.

12. Code of Criminal Procedure, 1898, is not keeping pace with ICT. Therefore special procedure should be introduced for speedy procedure for speedy criminal trial; following things should be observed for special procedure:
    a. expedited preservation of stored computer;
    b. data/expedited preservation and partial disclosure of traffic data (Data Retention scheme);
    c. Production orders;
    d. search and seizure of stored computer data;
    e. real-time collection of traffic data;
    f. interception of content data; and
    g. Jurisdiction condition should be abolished and authority should be given to every agency to catch the criminal.
13. Pakistan Penal Code, 1860, is not sufficient to deal with digital crimes, new special legislation should be introduce for advance fee fraud, email frauds, cyber terrorism, electronic fraud, electronic forgery, bank fraud, data diddling, misuse of electronic system, cyber-extortion, unauthorized access to code, online child pornography, illegal sale of articles, cyber defamation, misuse of encryption, cyber stalking, unauthorized interception, spoofing, spamming, digital privacy, fake websites, fake social media accounts, internet time theft, identity theft, online gambling, salami attacks, stock robot manipulation, Trojans & key-loggers, virus/worm attacks, web defacement, web-jacking, use of encryption by terrorist and economic espionage.
14. Electronic Transactions Ordinance, 2002, does not provide ample punishments, these punishments should be enhanced.

15. To equip the judges, lawyers and law students; new courses of forensic science should be introduced at University Level and awareness program should be introduced at every possible level.
16. Law enforcement agencies are not well equipped with latest techniques, capacity building course should be introduced.
17. Illegal purchase and sale of goods on the internet shall also be prohibited.
18. A National Security Council for Prevention of Cyber Crimes (NSCPCC) should be established;
    a. To access, receive and analyze information, and involve private sector entities for gathering of information and data;
    b. To ensure, the timely and efficient access by the Government to all information necessary to discharge the responsibilities;
    c. To develop a comprehensive national plan for securing the key resources of the Pakistan, related to ICT systems;
    d. to serve as the national focal point for work on law enforcement technology;
    e. to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology;
    f. To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by the law enforcement agencies, including, the;
        i. monitoring systems and alarm systems capable of providing precise location information

ii. wire and wireless interoperable communication technologies

iii. tools and techniques that facilitate investigative and forensic work, including computer forensics;

iv. equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;

v. guides to assist law enforcement agencies for related matters to tools and techniques that facilitate investigations of computer crime

g. To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications;

h. To develop, and disseminate to enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors, judges and law students;

i. To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist, law enforcement agencies in combating cyber crime;

j. To support research fellowships for its mission; and

k. To serve as a clearinghouse for information on law enforcement technologies.

Bibliography

Statutes

U.S Statutes

Adam Walsh Child Protection & Safety Act of 2006

Anti-Counterfeiting Consumer Protection Act of 1996

Check Clearing for the 21st Century Act (Check 21 Act), 2003.

Child Protection Act of 2012.

Communications Assistance for Law Enforcement (CALEA), 1994.

Computer Fraud and Abuse Act of 1986

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CANSPAM ACT) of 2003

Cyber Intelligence Sharing and Protection Act (CISPA) 2013.

Cyber Security Research and Development Act, 2009.

Digital Millennium Copyright Act of 1998.

Dot-Kids Implementation and Efficiency Act of 2002.

Economic Espionage Act of 1996

E-Government Act of 2002

Electronic Communications Privacy Act (ECPA) 1986

Electronic Communications Privacy Act Amendments Act of 2011

Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E–PRIVACY) Act, 1998

Enforcement of Intellectual Property Rights Act of 2008

Enhanced Consumer Protection against Spyware Act of 2005

Fair and Accurate Credit Transactions Act (FACTA) of 2003

Family Entertainment and Copyright Act of 2005

Foreign Intelligence Surveillance Act of 1978 (FISA)

Fraud and Related Activity in Connection with Computers of 1996

Gramm-Leachy-Bliley Act, 1999

Homeland Security Act of 2002

Identity Theft and Assumption Deterrence Act of 1998

Identity Theft Penalty Enhancement Act, 2004

Justice Enhancement and Domestic Security Act of 2003

Personal Data Privacy and Security Act of 2005

Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act).

Prioritizing Resources and Organization for Intellectual Property Act of 2008

Privacy Protection Act of 1980

Protection of Children from Sexual Predators Act of 1998

Ryan Haight Online Pharmacy Consumer Protection Act of 2008

Social Security Misuse Prevention Act of 2001

Spyware Control and Privacy Protection Act of 2000

Stop Online Piracy Act, 2011

Telecommunications Act of 1996

The Certification Council Transaction of Business Regulations, 2004

The Communications Decency Act (CDA) of 1996

The National Information Infrastructure Protection Act of 1996

Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers beyond Borders Act of 2006 (U.S. SAFE WEB Act of 2006)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Unlawful Internet Gambling Enforcement Act of 2006

Pakistani Statutes

Anti-Counterfeiting Amendments Act of 2004

Anti-Money Laundering Act, 2010

Associated Press of Pakistan Corporation Ordinance, 2002

Code of Civil Procedure, 1908

Code of Criminal Procedure, 1898

Constitution of the Islamic Republic of Pakistan, 1973

Copyright Ordinance, 1962

Electronic Media Regulatory Ordinance, 1997

Electronic Transactions Ordinance, 2002

Federal Investigation Agency Act, 1974

Freedom of Information Ordinance, 2002.

Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance, 2002

Pakistan Penal Code 1860

Pakistan Telecommunication (Re-organisation) Act, 1996

Patents Ordinance, 2000

Prevention of Electronic Crimes Ordinance, 2009

Registered Designs Ordinance, 2000

The Payments Systems and Electronic Fund Transfers Act 2007

The Telegraph Act, 1885

The Wireless Telegraphy Act, 1933

Trade Marks Ordinance, 2001

Articles

Dion, Michel. "Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives" *International Journal of Cyber Criminology* 1 & 2 (2010): 630-642.

Dombrowski, Stefan C., John W. LeMasney, and C. Emmanuel Ahia. "Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations." *Professional Psychology: Research and Practice* 1 (2004): 65-73.

Dombrowski, Stefan C., Karen L. Gischlar and Theo Durst. "Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet." *Child Abusive Review* 16 (2007): 153-170.

Fidelie, Laura Woods. "Internet Gambling: Innocent Activity or Cybercrime?" *International Journal of Cyber Criminology* 1 (2009): 476-491

Frieden, Jonathan D. and Leigh M. Murray. "The Admissibility of Electronic Evidence under the Federal Rules of Evidence." *Richmond Journal of Law and Technology* 2 (2011): 1-39.

Galbreth, Michael R. and Mikhael Shor. "The Impact of Malicious Agents on the Enterprise Software Industry." *MIS Quarterly* 3 (2010): 595-612.

Goldschmidt, Orly Turgeman. "Meanings that Hackers Assign to their Being a Hacker" *International Journal of Cyber Criminology* 2 (2008): 382–396.

Higgins, George E. "Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value" *International Journal of Cyber Criminology* 1 (2007): 33-55

Hinduja, Sameer. "Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future." *International Journal of Cyber Criminology* 1 (2007): 1-26.

Hinduja, Sameer. "Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future" *International Journal of Cyber Criminology* 1 (2007): 1-26.

Jaishankar, K. "Sexting: A new form of Victimless Crime?" *International Journal of Cyber Criminology* 1 (2009): 21-25.

Kigerl, Alex Conrad. "CAN SPAM Act: An Empirical analysis" *International Journal of Cyber Criminology* 2 (2009): 566-589.

Lavranos, Nikolaos. "Regulating Competing Jurisdictions Among International Courts and Tribunals" *ZaöRV* 68 (2008): 575-621.

Maghaireh, Alaeldin. "Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cybercrime?" *International Journal of Cyber Criminology* 2 (2008): 337-345.

Marion, Nancy E. "The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation" *International Journal of Cyber Criminology* 1 & 2 (2010): 699-712.

Ophardt, Jonathan A. "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield." *Duke Law & Technology Review* 3 (2010): 1-27.

Rege, Aunshul. "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud" *International Journal of Cyber Criminology* 2 (2009): 495-512.

Roberts, Lynne. "Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking" *International Journal of Cyber Criminology* 1 (2008): 271–285.

Weismann, Miriam F. Miquelon. "The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?." *The John Marshall Journal of Information Technology & Privacy Law* 2 (2005): 329-362.

Young, Kimberly. "Understanding Sexually Deviant Online Behavior from an Addiction Perspective" *International Journal of Cyber Criminology* 1 (2008): 298-307.

Yu, Szde. "Fear of Cyber Crime among College Students in the United States: An Exploratory Study" *International Journal of Cyber Criminology* 1 (2014): 36-46.

Zaheer, Muhammad. "Territorial Jurisdiction on Cyber Defamation in Pakistan's Perspective." *Corporate Law Decisions, Journal Section* (2011): 7-11.

Books

Akehurst, Michael. *Modern Introduction to International Law*. 7th ed. New York: Routledge, 1997.

Anastasi, Joe. *The New Forensics Investigating Corporate Fraud and the Theft of Intellectual Property*. New Jersey: John Wiley & Sons, Inc., Hoboken, 2003.

Baggili, Ibrahim. *Digital Forensics and Cyber Crime*. New York: Springer, 2011.

Banks, Michael A. *On The Way to the Web the Secret History of the Internet and Its Founders*. New York: Springer-Verlag Inc., 2008.

Brenner, Joel. *America in the Vulnerable inside the new threat Matrix of Digital Espionage, Crime and Warfare*. New York: Penguin Group Inc., 2011.

Casey, Eoghan. *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*. 3rd ed. California: Elsevier Inc, 2011.

Colarik, Andrew Michael. *Cyber Terrorism: Political and Economic Implications*. Hershey: Idea Group Inc., 2006.

Czosseck, Christian and Kenneth Geers. The Virtual Battlefield: *Perspectives on Cyber Warfare*. Amsterdam: IOS Press, Inc., 2009.

Daniels, Jessie. *Cyber Racism White Supremacy Online and the New Attack on Civil Rights*. Maryland: Rowman & Littlefield Publishers, Inc., 2009.

Donovan, Pamela. *No way of knowing Crime, Urban Legends, and the Internet*. New York: Routledge, 2004.

Fijnaut, Cyrille and Letizia Paoli. *Organised Crime in Europe Concepts, Patterns and Control Policies in the European Union and Beyond.* Dordrecht: Springer, 2004.

Gercke, Marco. *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Geneva: International Telecommunication Unit, 2012.

Giacomello, Giampiero. *National Governments and control of the internet a digital challenge.* New York: Routledge, 2005.

Gladyshev, Pavel and Marcus K. Rogers. *Digital Forensics and Cyber Crime.* New York: Springer, 2012.

Goel, Sanjay. *Digital Forensics and Cyber Crime.* New York: Springer, 2010.

Golumbic, Martin Charles. *Fighting Terror Online The Convergence of Security, Technology, and the Law.* New York: Springer Science+Business Media, LLC, 2008

Gottschalk, Petter. *Policing Cyber Crime.* Hershey: Petter Gottschalk & Ventus Publishing ApS, 2010.

Hafner, Katie and Matthew Lyon. *Where wizards stay up late (The origins of the internet).* New York: Touchstone Rockefeller Center, 1996.

Halder, Debarati and K. Jaishankar. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations.* Hershey: Information Science Reference, 2012.

Head, Tom. *It's your World, so change it: Using the power of the internet to create social change.* Indiana: Pearson Education, Inc. 2010.

Holt, Thomas J. and Bernadette H. Schell. *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Hershey: Information Science Reference, 2011.

Howard, Rick. *Cyber Fraud Tactics, Techniques, and Procedures*. New York: Auerbach Publications, 2009.

Jaishankar, K. and Natti Ronel. *Global Criminology Crime and Victimization in a Globalized Era.* New York: CRC Press, 2013.

Kahn, David. *The Code Breaker the Comprehensive History of Secret Communication from the Ancient times to the Internet.* New York: The New American Library, Inc., 1973.

Li, Chang-Tsun. *Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions*. New York: IGI Global, 2010.

Mali, Prashant. *Text book of Cyber Crime and Penalties* [As per ITA A 2008 and IPC] (Draft Version).

Manley, Anthony D. *The Elements of Private Investigation An Introduction to the Law, Techniques, and Procedures.* New York: Taylor and Francis Group, LLC, 2010.

Marcella, Albert J. and Doug Menendez. *Cyber Forensics A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.* 2nd ed. New York: Auerbach Publications, 2008.

Marcella, Albert J. and Robert S. Greenfield. *Cyber Forensics-A field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. New York: Auerbach Publications, 2002.

Marzilli, Alan. *Policing the Internet*. New York: Chelsea House, 2005.

Middleton, Bruce. *Cyber Crime Investigator's Field Guide*. New York: Auerbach Publications Taylor & Francis Group, 2005.

Middleton, Bruce. *Cybercrime investigator's field guide*. New York: CRC Press LLC, 2002.

Mitra, Ananda. *Digital Communications: From E-mail to the Cyber Community*. New York: Chelsea House, 2010.

Moore, Robert. *Search and Seizure of Digital Evidence*. New York: LFB Scholarly Publishing LLC, 2005.

Nagpal, Rohas. *Commentary on Information Technology Act*. Pune: Asian School of Cyber Crimes Laws, 2014.

_____. *Cyber Crime Law in India*. Pune: Asian School of Cyber Crimes Laws, 2012.

_____. *Data Privacy Law (India)*. Pune: Asian School of Cyber Crimes Laws, 2010.

_____. *Evolution of Cyber Crimes*. Pune: Asian School of Cyber Crimes Laws, 2008.

_____. *Facebook law in India*. Pune: Asian School of Cyber Crimes Laws, 2013.

_____. *Fundamentals of Cyber Law*. Pune: Asian School of Cyber Crimes Laws, 2012.

Naughton, John. *A Brief History of the Future The origins of the Internet*. 3rd ed. London: Orion Books Ltd, 2001.

Nyazee, Imran Ahsan Khan. *Legal Research and Writing in Pakistan.* Lahore: Federal Law House, 2014.

Pedneault, Stephen. *Fraud 101Techniques and Strategies for Understanding Fraud.*3rd ed. New Jersey: John Wiley & Sons, Inc., 2009.

Philipp, Aaron, David Cowen and Chris Davis. *Hacking Exposed Computer Forensics.* 2nd ed. New York: McGraw-Hill, 2010.

Reyes, Anthony. *Cyber Crime Investigations Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors.* Rockland: Syngress Publishing, Inc, 2007.

Richards, Sally. *Future Net The Past, Present, and Future of The Internet as Told By Its Creators and Visionaries.* New York: John Wiley & Sons, Inc., 2002.

Schuler, Karen. *E-discovery: Creating and Managing an Enterprise wide Program A Technical Guide to Digital Investigation and Litigation Support.* Burlington: Syngress Publishing, Inc., Burlington, 2009.

Shah, Aaushi and Ravi Srinidhi. *A to Z of Cyber Crime.* Pune: Asian School of Cyber Laws, 2012.

Shalhoub, Zeinab Karake and Sheikha Lubna Al Qasimi. *Cyber Law and Cyber Security in Developing and Emerging Economies.* Massachusetts: Edward Elgar Publishing, Inc., 2010.

Shaw, Malcolm. N. *International Law.* 6th ed. New York: Cambridge University Press, 2008.

Steffen, George S. and Samuel M. Candelaria. *Drug Interdiction Partnerships, Legal Principles, and Investigative Methodologies for Law Enforcement*. New York: CRC Press LLC, 2003.

Stephenson, Peter. *Investigating Computer-Related Crime a Handbook for Corporate Investigators*. New York: CRC Press LLC, 2000.

Vacca, John R. *Computer Forensics: Computer Crime Scene Investigation*. 2nd ed. Massachusetts: Charles River Media, Inc. Boston, 2005.

Wilson, Janet K. *The Praeger handbook of victimology*. California: ABC-CLIO, LLC, Santa Barbara, 2009.

Yar, Majid. *Cyber Crime and Society*. London: SAGE Publications Ltd, 2006.

Documents

Additional Protocol to the Convention On Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems.

Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World

Developments in the Field of Information and Telecommunications in the Context of International Security, 4 January 1999, A/RES/53/70

Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children

Special measures to be adopted to fight the menace of international terrorism, resolution adopted by the General Assembly, on its 2nd meeting, held on 23 March 2010, A/RES/4/3.

The United Nations Global Counter-Terrorism Strategy, 20 September 2006 A/RES/60/288.

Encyclopedias

Encyclopedia of White-Collar & Corporate Crime. Sage Publications, Inc. Thousand Oaks, California. 2005.

Encyclopedia of Cybercrime. Greenwood Press London. 2009.

Websites:

1- www.crs.gov

2- www.dawn.com

3- www.elibraryusa.gov

4- http://cyberbullying.us/

5- www.cybercrime.gov

6- www.unodc.org

7- www.itu.int

8- http://uscode.house.gov/

9- http://www.justice.gov/criminal/cybercrime/

10- http://www.olemiss.edu/depts/ncjrl/

11- http://tribune.com.pk/story/718865/cyber-crime-fia-arrests-alleged-facebook-blackmailer/

12- http://pklegal.org/content/legal-services-relating-cyber-crimes-laws-pakistan

13- http://www.ljcp.gov.pk/

14- www.supremecourt.gov.pk/ijc/articles/10/5.pdf

15- http://www.cybercrimelaw.net/Cybercrimelaw.html

16- http://www.cyberlawdb.com/gcld/

17- www.cyber-rights.org

18- http://www.emeraldinsight.com/doi/abs/10.1108/13639510610684674

19- http://www.coe.int

20- http://www.cybercrimelaw.net

21- www.govtrack.us

22- www.gao.gov

23- www.oas.org

24- www.coppa.org

25- csrc.nist.gov

26- www.ussc.gov

27- www.copyright.gov

28- http://cyberlaw.stanford.edu/our-work/cases

29- http://partners.nytimes.com/library/tech/reference/indexcyberlaw.html

30- http://cyberlawcases.com/

31- http://www.cyberlawsindia.net/cases.html

32- http://www.cyberlawclinic.org/casestudy.asp

33- http://www.prashantmali.com/cyber-law-cases

34- http://cyber.law.harvard.edu/property00/domain/CaseLaw.html

35- http://www.insidecounsel.com/2013/07/26/five-hackers-charged-in-biggest-cyber-crime-case-i