CYBER CRIME: PAKISTANI PERSPECTIVE

Mahboob Usman*

Abstract

Many scholars, lawyers, students and legislatures working on the cybercrime found it difficult to know what cybercrime exactly is? How many cybercrime are prevailing in the Pakistani legal system and how much is punishment for these crimes? Lack of proper awareness and understanding of the issue has caused many difficulties for the researchers, law enforcement agencies, legislatures and judiciary because when they talk of the cybercrime they include many things which are not cybercrime or they exclude which are cybercrime. The present paper analyzes in some detail the cybercrime, definition, origin of the internet, complications, famous cybercrimes, their punishments and role of NR3C in some details. It concludes that the existing legislation on the subject is not sufficient; therefore, the legislator needs to legislate on the matters which are not covered under the existing legislation.

Introduction

Rapid evolution of information technology is transforming our society and its institutions which have created many problems, *inter alia*, is a Cybercrime. It has a wide range of applications in every walk of life, and has directly or indirectly affected almost all sectors of the society. Nevertheless, developing countries are not acquainted with technology, these lag in technological progress which leads to computer crimes and other associated complications. Numerous electronic crimes which are prevailing in Pakistan are not covered under any suitable legislation. Even though the recently enacted Prevention of Electronic Crimes Act, 2016 (PECA) does not cover many of the existing crimes.

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. In Pakistan, however, three decades ago commission of cyber-crimes was not significant as most of people were unaware of 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 part of Pakistan's legal system, because the world is enacting many laws for tackling emerging cyber-crimes, and the legislature in Pakistan is not taking it seriously to control the emerging situation. The Pakistan internet market has grown multiple 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."[29] 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."[30] Hence, we can easily conclude that Pakistan is not free from cyber space problems.

In Pakistan, first law on cyber-crime was enacted through "Electronic Transactions Ordinance, 2002,"[31]which addressed a few crimes, as the main purpose of the Ordinance was "to recognize and facilitate documents, records, information, communications and transactions in electronic form, and to provide for the accreditation of certification service providers."[32] Thus, it was a step towards the new era, till the promulgation of PECA, the provisions of this Ordinance

[29]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.
[30]Ibid.
[31]Electronic Transactions Ordinance, 2002 (LI of 2002).
[32] Ibid. Preamble.

were used to cover the cyber-crime. Under this Ordinance many aspects of cyber-crime were not covered. With the emergence of electronic crime, the demand for legislation on the subject increased. Consequently, in 2007, the then President of Pakistan promulgated "the Prevention of Electronic Crimes Ordinance, 2007", to give legal cover to few of the existing crimes. Similarly, the same Ordinance was again promulgated in May 2008, February 2009 and the last promulgation took place on 4th July 2009. These Ordinances were not tabled in parliament and lapsed on completion of constitutional time as, in Pakistan; the Presidential Ordinance is only applicable for one hundred and twenty days[33] from the date of its promulgation. These Ordinances were a stop gap arrangement, which borne no fruit for judiciary as well as for law enforcement agencies. We can easily conclude that there was no particular law to cover the cyber related issues in Pakistan till the enacted of PECA.

Masses are not seriously looking forward for significant steps to protect the nation from cybercrimes where in most cases it is not possible to apprehend the offenders who are either not within national borders or because they are working secretly. However, the newly enacted legislation strengthens the law enforcement agencies by extending the International cooperation for investigation purposes.[34] Elimination of cybercrime totally from the cyber space is challenging, it is quite possible to take suitable initiatives to reduce it by creating awareness among the users of the internet. The initial step is to make people aware of the sensitiveness of these crimes and further make the application of the laws more severe to check the commission of crime.[35]

[33]Pak. Const. art. 89, cl. (2) (a) (i)
[34] S. 42 of PECA, 2016.
[35]Mohiuddin, "Cyber Laws in Pakistan, 19.; http://supremecourt.gov.pk/ijc/articles/10/5.pdf (accessed on 5th March 2015)

Definition of Cyber Crimes

The foremost problem for the cyber crime's study is the absence of proper definition for the term cyber-crime, some jurists tried to define this term but still there is no consensus on the definition of the term. Cyber-crime is generally described as "cyber-crime is a generic term that refers to all criminal activities done using the medium of computers, the internet, cyber space and the worldwide web."[36] In other words, it is a crime in which a computer is the target of the crime or is used as a tool to commit an offense.[37] This definition does not cover many aspects of the cyber-crime as sometimes mobile phone is used for committing crime but the given definition does not include the mobile. Dr. Debarati Halder and Dr. K. Jaishankar have provided a useful definition that covers other modern day devices. Their definition 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).[38]

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.[39] Rather, instead of trying to understand cybercrime as a single

---

[36]Prashant Mali, *A Text Book of Cybercrime and Penalties* (Indiana: Repressed Publishing LLC, 2006), 3.
[37]http://www.techopedia.com/definition/2387/cybercrime (accessed on 10th December 2014).
[38]DebaratiHalder and K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* (Hershey: Information Science Reference, 2012), 15.
[39]*Encyclopedia of Cybercrime.*eds. Samuel C. and McQuade (Westport: Greenwood Press, 2009), s.v. "Cybercrime".

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."[40]

Origin of the Internet and cybercrime

Cyber-crime has evolved with the evolution of the Internet and expansion of IT, which have provided many opportunities for criminals to destroy the society by using new techniques.[41]It begins with the advancement of the Internet, assuming that without the latter, the former could and would not exist. To put it differently, it is the Internet that provides the essential electronically generated atmosphere in which it takes place as we use Internet for communication, so we become the victim of cybercrime.[42]

Cybercrime's history starts with the development of a network, the Advanced Research Projects Agency Network (ARPANET),[43] funded by the U.S military in the 1960s. Basic purpose of the ARPANET was to launch means by which "secure and resilient communication and coordination of military activities could be made possible" in the threat of nuclear confrontations.[44] 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."[45] Establishment of ARPANET played significant role in the advancement of the internet, which also opened doors for research and

[40]MajidYar, *Cyber Crime and Society* (London: SAGE Publications Ltd, 2006), 9.
[41]*Encyclopedia of Cybercrime, s.v. "Cybercrime".*
[42]Yar, *Cyber Crime and Society*, 83.
[43] 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*".*
[44]Yar, *Cyber Crime and Society*, 7.
[45] Ibid.

cyber-crime. 1n the 1970s other networks parallel to the ARPANET, like 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.[46] In 1981, access to ARPANET was expanded and in 1982, the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol.[47] In early 1980s the NSF provided funds for the establishment of national supercomputing centers at "several universities, and 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."[48]

However, in 1980s the Commercial Internet Service Providers (ISPs) began to emerge,[49] and Private connections to the Internet by commercial entities became widespread rapidly, 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 mid-1990s, the Internet has had a revolutionary impact on culture and commerce."[50] 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.[51] Netscape browser was the first commercial browser which was launched in the year 1994 by the Microsoft by its own browser the Internet Explorer.[52]Since the commercialization of the Internet it has created many problems for the world. Developing countries generally lag behind on scientific developments, while computer has presented a new and complex situation like white-collar computer crimes. Digital crimes "occur within the white-collar crime, which is a special domain

[46]http://en.wikipedia.org/wiki/History_of_the_Internet (last accessed on 30th December 2014)
[47] Ibid
[48]Ibid.
[49]Ibid.
[50] Ibid.
[51] Ibid.
[52]Yar, *Cyber Crime and Society*, 7-8.

of financial crime."[53] It is a crime against property for individual or organizational gain, committed by upper class members of society who are educated, wealthy, socially connected and are employed in any legitimate organization. In fact, in this situation elite class criminal is less likely to be apprehended because of his social status in the society. Despite the efforts made by law enforcement agencies, more often offenders escape punishment.

Cyber Crimes and Conventional Crimes

Crime[54] is as old as the human society, but modern devices have introduced cybercrimes. Those crimes which are committed by using computer, directly or indirectly, are called cyber-crimes however those which are committed by using old techniques or methods are called conventional crimes. Apparently, there is no difference between both forms of crimes, nonetheless 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 where technological devices are not used then it is called conventional crimes.

The Internet use in Pakistan

In Pakistan, since the mid-90s the Internet access is available. The Pakistan Telecommunication Company Limited started offering access via the nationwide local call network[55] since then the cybercrimes started emerging in our society. Pakistan is among the top Asian net users countries.[56]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. 3G and 4G technology has also brought revolution in the IT field. Due to increased number of internet user, the

[53]Petter Gottschalk.*Policing Cyber Crime* (Hershey: Petter Gottschalk &Ventus Publishing ApS, 2010), 14.
[54] 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.
[55]http://www.internetworldstats.com/asia/pk.htm (last accessed on 3rd March 2015)
[56] Ibid.

manual business is shifting on the internet, which has reduced paper work replacing the manual system with computer. Although, it is a blessing for human beings to save their precious time, but fraud, cheating and many other illegal activities are also being carried out through internet and computer.

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 requisite expertise nor the required experience to deal with investigation, evidence collection, evidence preservation and presentation to the court. Therefore, the offender cannot be punishment. 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."[57] Due to alteration of data, the investigation of cybercrimes is very complicated as compare to manual crimes. However, by adopting latest techniques the complexity of the digital crime can be reduced.

National Response Centre for Cyber Crimes

The Government of Pakistan has established the "National Response Centre for Cybercrime"[58] (NR3C) under the administrative control of Federal Investigation Agency (FIA), to investigate the cybercrimes, trace the criminals and use their efforts to stop misuse of the internet.NR3C has expertise to deal in the following subjects' i.e. digital forensics, information system security audits, technical investigation, penetration testing and training in these fields.[59] Since its establishment, it is working for the capacity building of law enforcement agencies, Bench and bar, and other Government organizations. In addition to this, it has also piloted a large number of seminars, workshops and training programs to create awareness among the academia, print and

[57] Vacca. *Computer Forensics: Computer Crime Scene Investigation*, 219.
[58] S. 29 of PECA, 2016. NR3C was established in 2007 under section 25 of the PECO, 2007, since then this department is dealing with cybercrimes.
[59] http://www.nr3c.gov.pk/about_us.html (accessed on 3rd March 2015).

electronic media and lawyers. NR3C has also arrested and prosecuted many criminals including two boys for hacking Supreme Court website.[60]NR3C is a law enforcement agency of the Federal Government to fight the cybercrime. Feeling importance of the issue, this Hi-Tech crime fighting unit was established in 2007 to identify and curb the phenomenon of technological abuse in society.[61]NR3C's primary function is to deal with technology based crimes committed in Pakistan or abroad committed by Pakistani nationals. This is the only unit which directly receives complaints and assists other law enforcement agencies in cyber cases.[62]

1. **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 secret social, economic and military information."[63] In addition to this, the databases of banks and private organization are also the target of these criminals.

Types of Cyber Crimes

Owing to continuous evolution and development of IT, many new crimes are being faced by the world. There is no limit to such crimes, therefore it is difficult to cover all of them in present article. Thus, few of them are discussed to understand their nature and complication. The emergence of World Wide Web has enabled unprecedented access to information, and has created unexpected "opportunities to attack information assets."[64] Proper understanding of these

[60] http://propakistani.pk/2010/10/27/nr3c-arrests-two-boys-for-hacking-sc-website/ (accessed on 3rd March 2015)
[61] http://www.nr3c.gov.pk/about_us.html (accessed on 3rd March 2015).
[62] Ibid.
[63] http://whitepaper.techweekeurope.co.uk/advertiser/secunia (accessed on 15th December, 2015).
[64] Michael R Galbreth and MikhaelShor."The Impact of Malicious Agents on theEnterprise Software Industry".MIS Quarterly 3 (2010), 595-612.

crimes is important to legislate on these issues, without proper understanding, measures cannot be adopted to prevent them.

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 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."[65] The theory of these crimes suggests that "financial crimes are opportunity driven, where executive and managers identify opportunities for illegal gain."[66] 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."[67]

Advance Fee fraud

Few decades ago, it was very difficult to cheat, to get money and deprive someone of his earnings. Nevertheless, the internet has made it easy for criminals to cheat and deprive innocent people of their earnings. One of them is the advance fee fraud which is "intentional misrepresentation for the purpose of gain."[68]Advance fee fraud[69] is a financial crime that spreads with the introduction of the internet communication, electronic business and electronic

[65] Gottschalk. *Policing Cyber Crime*, 14.
[66] Ibid.
[67] Mali, *A Text Book of Cybercrime and Penalties*, 6.
[68] Gottschalk. *Policing Cyber Crime*, 21.
[69] Advance fee fraud is also known as lottery scam and email fraud.

commerce,[70] 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 surprising 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 occasionally it contains name of any famous corporation or company. "Most of these scam emails promise the receiver millions of dollars."[71] 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 charges, when fee is received, the receiver disappears. In this way millions of people get defrauded every year through these scams. Besides, "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."[72] Mostly greedy people try to keep secret and 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..

Bank Fraud

Bank fraud is a new method for 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

[70] Gottschalk. *Policing Cyber Crime,* 21.
[71] Mali, *A Text Book of Cyber crime and Penalties,* 62.
[72] Aaushi Shah and Ravi Srinidhi, *A to Z of Cyber Crime* (Pune: Asian School of Cyber Laws, 2012), 150.

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.

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 of the above mentioned element is missing so it will not be considered 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. Many companies are destroying 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.

Cyber Pornography

Over the last few decades, the "internet has provided an expedient mode of communication and access to a wealth of information."[73] It is a "valuable tool; however, it can also be detrimental to the wellbeing of children due to numerous online hazards."[74] Cyber pornography is assumed to be the largest business on the Internet in contemporary 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.[75]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."[76] 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."[77] There is the "potential for children to be abused via cyberspace through online sexual solicitation and access to pornography."[78] Indeed, the internet is "replete with inappropriate material, including pornography, chat-rooms with adult themes and access to instant messaging wherein others could misrepresent themselves."[79] As children are actively "utilizing the internet where unknown others can have access to them or where they can be exposed to inappropriate sexual materials,

[73]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.
[74]Ibid.
[75]Ibid.
[76]"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.
[77] Ibid.
[78]Dombrowski, **"**Safeguarding Young People from Cyber Pornography and Cyber Sexual Predation: A Major Dilemma of the Internet.": 153-170.
[79]Ibid.

they require safeguarding and education in safe internet use."[80] To put it another way, we can say that "the cost to children and society of sexual perpetration is too great to overlook the hazards of online solicitation."[81]

In March 2016, in Pakistan, the child pornography was defined[82] and criminalized.[83] In August 2016, similar offence was defined through PECA[84] which increased the maximum fine from seven hundred thousand rupees to five million rupees but the imprisonment was same as in the Pakistan Penal Code.[85] Hence, we can easily conclude that where the computer is used for distribution or transmition of any child pornographic material is more serious as compared to conventional means.

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."[86] 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."[87] In other words, it refers to the use of "the internet, e-mail, or other electronic communications devices to stalk another person."[88] Same principle is applicable to companies where larger and powerful companies stalk weaker to

[80]Ibid.
[81]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.
[82] S. 292 B 0f the Pakistan Penal Code, 1860,
[83]Ibid., S. 292 C.
[84] S. 22 of PECA, 2016
[85] Ibid.
[86]Shah, *A to Z of Cyber Crime,* 42.
[87]*Black's Law Dictionary, v.s. "stalking."*
[88] Mali, *A Text Book of Cybercrime and Penalties,* 35.

destroy their business and to control the market. Whoever commits this office is liable for imprisonment up-to three years or fine up-to one million rupees or both and in case of minor, imprisonment will be up to-five years and fine up-to ten million rupees or both.[89]

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."[90]Cyber terrorism is defined as "the premeditated 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."[91] Keeping in view the different prospective of it, many scholars have defined it differently. 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."[92] Some countries have legislated to curb this situation including the UK[93] and US.[94]

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

[89] S. 24 (2) of PECA, 2016.
[90]Yar, *Cyber Crime and Society,* 50-51.
[91]This was proposed by RohasNagpal, in a conference held in Madrid, Spain in 2002.
[92]Yar, *Cyber Crime and Society,* 51.
[93]UK Terrorism Act of 2000.
[94]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (The USA PATRIOT) Act, was passed on 26th October 2001.

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 can cause billions of dollars' loss to any financial institution and company, because detection of such alteration is not possible to curb this situation within shortest possible time. This is called "electronic forgery" in Pakistani legal system and the criminal is awarded punishment up to three years and fine up to two hundred and fifty thousand rupees or both[95] and if the criminal commits this crime is respect to critical infrastructure, he will be imprisoned up to seven years and fine up to five million rupees or both.[96]In other words, 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.

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."[97] 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"[98] and "results in authorized users being unable to access the service offered by the computer."[99] 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

[95] S. 13 of PECA, 2016.
[96]Ibid., 13 (2).
[97] Ibid.,30.
[98] Mali, *A Text Book of Cybercrime and Penalties*, 46.
[99] Ibid.

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.[100]

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."[101] In the meantime, it is a growing threat with the growth of digital technologies and Internet file sharing networks.[102]Digital piracy[103] 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."[104] Copyright infringement, trademarks violations, theft of computer and software piracy etc., are the few examples of intellectual property crimes. Copyright protected material's downloading is not only the digital piracy but posting a copyrighted work without the explicit permission of the owner is also copyright infringement.

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."[105] 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."[106] The DOS attack and email bombing are not similar, as a

[100] Ibid.
[101] Shah, *A to Z of Cyber Crime*, 37.
[102] Ibid.
[103] Digital piracy is also known as copyright infringement and intellectual property crimes.
[104] Gottschalk. *Policing Cyber Crime*, 25.
[105] Shah, *A to Z of Cyber Crime*, 152.
[106] Mali, *A Text Book of Cyber crime and Penalties*, 41.

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.

Email/Web Spoofing

Cambridge dictionary has defined spoof as "to try to make someone believe in something that is not true."[107]A spoofed email is one that "appears to originate from one source but actually has been sent from another source."[108] 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 communications designed to socially engineer people into giving up confidential information that can then be used to commit crimes."[109]Web and email spoofing typically occur together "as when an attacker sends an e-mail with a link to a spoofed web site."[110] 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. Spoofing is a crime in Pakistani legal system, and whoever commits this crime is imprisoned up-to three years and fine up-to five hundred thousand rupees or both.[111]

Fake Social Media Accounts

Fake social media accounts are those which are created by using other persons' name instead of their 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, this illegal and immoral activity is carried out throughout the world, especially in Pakistan there is no mechanize to check fake accounts. According to The Cable News Network (CNN) 83 million Facebook

[107] Cambridge Advanced Learner's Dictionary, s.v. "spoof"
[108]Shah, *A to Z of Cyber Crime,* 83.
[109]*Encyclopedia of Cybercrime,*s.v. "fraudulent schemes and theft online" 75.
[110] Ibid.
[111] S. 26 of PECA.

accounts are fake and dupe[112] 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.

In other words, it is called Identity fraud/theft which is the fastest growing while-collar crime in many countries, especially in developed countries.[113] It is a "form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity."[114] This is done to access someone's credit card or other personal information for financial gain for personal use, leaving the victim upset emotionally and financially. While 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."[115] It deprives the real owner of his causing right while loss to his interests. This has been penalized through enactment of PECA which prescribed imprisonment up-to three years and find up-to five million rupees or both.[116]

Similar to fake social accounts, fake websites are created throughout the world to cheat the innocent people. These websites look identical to original ones but it involves "manipulating the domain name system to take unsuspecting victims to fake websites."[117] The browser reaches some fake website, rather 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

---

[112] http://edition.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/ (accessed on 18th February 2015).
[113] Gottschalk. *Policing Cyber Crime*, 23.
[114] Shah, *A to Z of Cyber Crime*, 138.
[115] Ibid.
[116] S. 16 of PECA, 2016.
[117] Shah, *A to Z of Cyber Crime*, 165.

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."[118]

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,"[119] 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.

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."[120] 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".[121] If website of any organization or corporation is hacked; visitors, consumers and clients may lose faith in such sites that cannot

[118] Gottschalk. *Policing Cyber Crime*, 17.
[119] Ibid.
[120] Shah, *A to Z of Cyber Crime*, 231.
[121] Ibid.

promise security. As after defacement "sites have to be shut down for repairs, (sometimes for an extended period of time), causing expenses and loss of profit."[122]

Internet Time Theft

This connotes the usage by "an unauthorized person of the Internet hours paid for by another person."[123] 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.

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." [124] 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 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."[125]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."[126] This includes "spy ware, botnets, keystroke loggers, and dialers. In a botnet, the malware logs in to a chat system while a key logger intercept the user's keystrokes when entering a password, credit card number, or other

[122] Ibid, 232
[123] Mali, *A Text Book of Cyber crime and Penalties*, 56.
[124] Gottschalk. *Policing Cyber Crime*, 22.
[125] Ibid.
[126] Ibid.

information that may be exploited."[127] This software automates a "variety of attacks for criminals and is partially responsible for the global increase in cybercrimes."[128]In Pakistani legal system, it is called malicious code, which is punishable up-to two years and fine up-to one million rupees or both.[129]

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?

Salami Attacks

The attack is called salami attack as it is "analogous to slicing the data thinly, like a salami."[130] 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."[131]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."[132] For instance, a bank employee inserts a program, into bank's servers, that deducts a small amount of money from all customers' accounts. Due to small amount of deduction from the

[127] Ibid.
[128] Ibid.
[129] S. 23 of PECA.
[130] Mali, *A Text Book of Cybercrime and Penalties*, 45.
[131] Encyclopedia of White-collar & Corporate crime, v.s. "Salami"
[132] Mali, *A Text Book of Cybercrime and Penalties*, 45.

accounts, no account holder will be able to notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.[133]

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"[134] due to "several online payment gateways that can transfer money around the world at the click of a button."[135] Likewise, 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"[136] which pose a "serious potential threat to the health and safety of patients."[137]

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."[138] This type of manipulation is illegal, 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.

A Trojan is "an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing."[139] Common types of Trojans

---

[133] Ibid.
[134]Shah, *A to Z of Cyber Crime*, 193.
[135] Mali, *A Text Book of Cybercrime and Penalties*, 19.
[136] Ibid.
[137]Shah, *A to Z of Cyber Crime*, 193.
[138] Gottschalk. *Policing Cyber Crime*, 23.
[139]Mali, *A Text Book of Cyber crime and Penalties*, 52.

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. Thus, many hackers use it as a tool to get the password and personal information of the victim.

Use of Encryption by Terrorists

Encryption 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."[140] Stating differently, 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. 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."[141] 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."[142]Lot of 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 of messages. Notably, terrorist groups make use of the Internet "in support of their conventional, terrestrially based activities to finance their illegal activities."[143]

Virus / Worm Attacks

Computer viruses are "small software programs that are designed to spread from one computer to another and to interfere with computer operations."[144] It "might corrupt or delete data on the

[140]Yar, *Cyber Crime and Society*, 58.
[141] Ibid.
[142] Ibid.
[143] Ibid.
[144] Mali, *A Text Book of Cybercrime and Penalties*, 49.

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."[145] These are mostly spread by "attachments in e-mail messages, instant messaging messages, attachments of funny images, greeting cards, and audio and video files."[146] These can also spread through downloads on the Internet, where "they are hidden in illicit software or other files or programs."[147] Whereas 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."[148]

Web 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."[149]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."[150]Even the Supreme Court of Pakistan's website was hacked by hackers[151] in 2010 to put pressure on Pakistani government for release of Dr. Afia., and they also posted some objectionable material on it.[152] 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."[153]

---

[145] Ibid.
[146] Ibid.
[147] Ibid.
[148] Ibid.
[149]Mali, *A Text Book of Cyber crime and Penalties*, 59.
[150] Ibid.
[151] Two hackers were involved in hacking the Supreme Court website, one was Pakistani national and other was Indian national.
[152]www.ndtv.com/world-news/pakistan-supreme-courts-website-hacked-433856 (accessed on 13th February 2015)
[153]http://timesofindia.indiatimes.com/world/pakistan/Pakistan-Supreme-Courts-website-hacked/articleshow/10136938.cms (accessed on 13th February 2015)

Conclusions

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 unaware 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 cannot make adequate laws to punish the criminals. 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. Besides, online consumer protection legislation should be introduced to protect the online consumer and online business industry. Moreover, goods are not provided as per standard or not delivered, consumer protection is also mandatory. Illegal purchase and sale of goods on the internet shall also be prohibited.

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. However, if the telecommunication industry is not providing latest data and detail of it, then it will make very difficult for law enforcement agencies to investigate the crimes expeditiously. Keeping in view the demands of 21st century, if ample laws are enacted to keep and protect the relevant data. This will bring many opportunities for law enforcement agencies for collection of sufficient evidence for prosecutions of the offenders.

***