- **p- ISSN:** 2521-2982
- **e-ISSN:** 2707-4587
- **ISSN-L:** 2521-2982

GLOBAL Political REVIEW

URL: http://dx.doi.org/10.31703/gpr.2019(IV-II).02

DOI: 10.31703/gpr.2019(IV-II).02

Zia UL Islam* | Muhammad Aqeel Khan† | Muhammad Zubair‡

Cybercrime and Pakistan

- **Vol.** IV, **No.** II (Spring 2019)
- **Pages:** 12 – 19

Headings

Abstract *Cybercrime or electronic crime is a very diverse and expanding phenomenon. It has no boundaries. For people from different walks of life, it's really hard to understand it. No exact definition of cybercrime can be given. Cybercrime in Pakistan has immensely increased in the past two decades. We had no digital forensic and information data experts. No latest system was available. Previously we had no legislation on cybercrimes until when Prevention of Electronic Crimes Act (PECA) 2016, was passed by the government. This research paper analyzes cybercrime, its meaning and origination, different difficulties, laws of cybercrime and its punishment given under the PECA. Some deficiencies along with few suggestions have been highlighted in the current setup of cybercrime and policy making at the end.*

Key Words: Impersonation, Legislation, phishing, Spoofing and Stalking.

Introduction

As with the advancement of different technologies and their diverse nature, different corporations, top MNC's and the whole human race are dependent upon it. A few decades ago, companies were largely dependent upon human resources but with the ever expanding technological advancement, now computers have replaced humans. The 21st century is a century of highly sophisticated technologies. New technologies, new discoveries and newer inventions have brought revolution to the human race. Two decades ago the generation of the computer for different purposes up to-day's modern system of networking and usage, computer has become an extremely essential part of the life of every man. (Seacord 2004)

Before the computers came there would be an old type -writer and all of the records were kept and stored in hard form. With the invention and development of computers, people have become more dependent upon computers and the typewriters are now lost in the pages of history. Charles Babbage is known as the father of modern computing. He was the one who invented it. He was an English mathematician and philosopher who gave the idea of modern computing. Later on with time different scientists worked on computers and gave their own idea as to how the computer shall work and look. Today the computers that we work on, is the hard work of those scientists, mathematicians, philosophers and professors.

Then came the idea of Internet in the '60's. The owners of this idea were Paul Baran and Donald Davies. The projects and ideas leading to the development and creation of Internet were ARPANET, MERIT, and TELENET. Afterwards another network system X.25 was developed. Another program developing alongside X.25 was RFC 675. In 1982 Internet protocol suite was developed. When WWW

*Lawyer, District Courts Mardan, KP Bar Council, KP, Pakistan.
†Assistant Professor, Department of Law, Abdul Wali Khan University Mardan, KP, Pakistan. Email: aqeel@awkum.edu.pk
‡Associate Professor, Department of Law, Abdul Wali Khan University Mardan, KP, Pakistan.

(World Wide Web) was launched in the 90's, it changed the dimensions of Internet. The flow of users increased and raised day by day. However, having a positive side, it has a darker side too. Computers can be helpful in almost every field of life but can be used to harm others too through Cybercrime.

The question that arises in many minds is that, what actually is a cybercrime and how does it affect people, cybercrime or in other words computer crime is a crime which is done via computers. It includes fraud, impersonating someone or stealing someone's identity, pornography, and theft of intellectual property. It is a highly growing and highly sophisticated kind of theft in the contemporary world. Every year different hacking groups steal billions of dollars. The crimes committed via the Internet are elaborated herein; Almost 2.3 billion humans of the world access the Internet and the majority of them being teens and people below the age of 25. (Hick 2000). It is estimated that by the year 2020 these electronic devices will outnumber people by six to one.

The General Assembly passed a Resolution (55/63) on 4th of December 2000 to ensure that states must safeguard their laws against criminal misuse of information technologies. They should safeguard the privacy, integrity and provision of date and computer systems from abuse (Nations 2001).

Definition of Cyber-Crime

"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." (Mali 2006)

In other words, cybercrime 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)" (Jaishankar 2012)

According to Grabosky, cybercrime means:

Any computer related crime such as digital child pornography piracy, stalking, forgery, harassment and intellectual property, hacking or drug Trafficking with digital proof. (Grabosky 2004).

Origin of Cyber Crime

In America, a group called "phreakers" emerged in the '70's. They would commit crimes by using telephones. John Draper was a famous member of the group. This group would replicate the tones that were used in America telephoning purposes and would make free calls. According to some scholars, the history and origin of cybercrime is related and connected to ARPANET (Advance Research Projects Agency Network). It was a project funded by the US Department of Defense. Its main aim was to make secure communications for military purposes. The same technology allows communications to be divided into packets and regenerate them in their Original form (Cybercrime and Society 2006).

The term "hacking" first practically came to be known when a group of extremely skilled computer programmers started to attack telephones in the telecommunication sector. This group of highly skilled computer programmers was known as phreakers. They were able to somehow break into the system and found a way as to how to call for free in different ways. They found ways as to how by knowing the system one can call for free anywhere they want. An American investigation agency conducted a covert operation in which different data storing devices and different operating systems were recovered. These devices were used by different hackers for free calls and different kinds of credit theft. Despite different punishments in many jurisdictions, still cybercrime is an immensely increasing problem.

Pakistan and Cybercrime

Internet was made available in the 90's. Pakistan ranks in the list of top Internet user countries. Internet

has made life easier and is less time consuming, but at the same time it has given birth to theft, fraud, child pornography, extortion etc. In Pakistan, people misuse Internet and the extreme usage being for criminal and unlawful acts (Mohiuddin, 2006). About 7500000 users were reported to be using Internet in the year 2004 in Pakistan. A few years from now we had no proper scheme for investigation of cybercrime neither expertise. There was no proper procedure and often the offenders were set free. National response center for cybercrime was established by the government under the control of Federal Investigation Agency (FIA). The main purpose of its establishment was to stop the misuse of internet. This agency has the expertise as to dealing with cyber security, cyber fraud, technical investigation, digital forensics. The first ever case related to cybercrime in Pakistan was reported in 2003. Five Pakistanis were involved in a business related to import and export while using fake info and misusing credit cards.

As per the FIA reports 65% cybercrimes are committed on Facebook which includes black-mailing and harassment of women and the majority of cases are committed in Karachi. The Karachi cyber wing receives almost 20 complaints relating to cybercrime daily. Almost 5500 cases relating to cybercrime very reported in Lahore in the year 2018. These included harassment, blackmailing, stalking, violation of privacy, impersonation, fraud etc. A brief sketch of the cybercrimes reported in Pakistan in previous years is given below; (DAWN, 2018)

Year	Number of inquiries conducted	Number of Cases Registered	Number of arrests made
2016	514	47	49
2017	1290	207	160
2018	20295	255	209

There is a need to be a separate court for cybercrimes and increase in the number of cybercrime experts. Advance systems are required to tackle the current crime rate situation. Prevention of electronic crimes act was passed in 2016, which included the following crimes and their punishments:
Here are some of the notable cybercrimes in detail:

Bank Fraud

Bank Fraud is an illegal and unauthorized way of getting hands on someone else's money. It is a white - collar crime. In this case a person pretending to be working in a bank either calls or send an email to the bank account holder, and informing them that due to some damage or attack on our banking systems they'd lost some of your personal info, data, credit number etc. To revalidate and update your profile they'd need all of your personal information, credit number etc. Now when they acquiring the account holder's personal info and credit and other data, they withdraw all of the money in the account of the account holder and disappears. Sometimes it's really hard to trace and find them because they're expert criminals and experts in programming. They leave no trace behind them.
By adopting the following techniques, bank fraud can be avoided to a great extent:

- Keep the software updated
- Keep the security level high
- Keep 2 to 3 protective layers
- Keep yourself updated about all of the transaction

Illegal Access to Data

According to sections 3 and 14 of the PECA 2016 Act, the punishment for un-authorized access to information system is three months or with fine or both. While the punishment for intentional wrongful

gain, misuses the device or data or agrees any other person enter into a relationship or cause damage to other person is two years or fine up to ten million Rupees or both (Pakistan, 2016).

Advance Free Fraud

Advance Free Fraud is a typical type of deception, which is done online. Getting hands on someone else's money in past was hard but now with technological advancement, it has indeed become very much easy. With the help of internet, it has become much easier.

In this type of fraud, the scammer sends an email regarding a lucky draw or lottery and informs the respondent that he has won a certain sum of money. The reason that's mostly given is either charity or a company or organizations 100th anniversary or lucky draw or lottery etc. They make the respondent believe that what they're doing is correct and accurate, they gain their confidence. Then afterwards some fee is requested to submit. When the transaction takes place, the receiver of money disappears.

Advance Free Fraud is the intentional misrepresentation for the purpose of gain. (Gottschalk, 2010)

The history of advance Free Fraud sates back to the 18th century where a person from a wealthy family had to escape from prison and for that purpose the assistance of some criminal minded people was required. In such a case, all of the officials from jailer to watchmen were given their shares.

Cyber Stalking

Cyber stalking is committed when someone intentionally uses information system via internet, website, Email to coerce or intimidate another person by repeatedly contacting him despite a clear unwillingness from the other or to monitoring the activities of other via electronic communications or watching or spying on other resulting in serious fear in his mind or taking a photograph or making a video without his permission in a manner to harm the reputation of that person. The punishment awarded for the above crime is imprisonment for three years or with fine which may extend to 1 Million Rupees or both.

Pornography

The first ever pornographic movie production started in 1895 by two persons, Eugene Pirou and Albert Kirchner. In today's world there are indeed countless pornographic sites, magazines, nude snaps etc. Pornography is considered in some parts of the world as a taboo. In some jurisdiction around the world it is a criminal offence.

According to a survey conducted by Google, Pakistan, Egypt, Vietnam, Iran, Morocco, India, Turkey, Philippines, and Poland are amongst the top porn watching countries. (Staff 2015). Child sex is a very big industry and it is expanding at a very high rate, it is a very alarming situation for the world. As per reports of different international organizations working in the field of child sex, many young girls are sexually exploited and in different parts of the world, they are forced to enter the child sex industry. Some of these young girls are sold to the highest bidder; some are used for smuggling purposes. Some countries in Europe like Nederland, their economy is dependent upon sex and it includes up to some extent child sex too. This industry contributes a lot to their countries GDP.

The people or groups involved in running a child sex industry, become very rich in a very short span of time. The sexual exploitation of young girls is indeed a very profitable business for such bad and horrific people. Ukraine is considered to be a very big market of the child pornography. A very large of it is even made there. It won't be wrong to say that Ukraine is kind of a central hub of child pornography in the modern world. Girls at very young age are sexually exploited and their nude and explicit content is shared on different pornographic sites. The international agencies have failed to control or limit such shameful acts.

According to section 22 of PECA 2016;

Anyone who makes, offers, distributes any information system or material that visually depicts a minor engaged in sexually explicit action or identifying a minor shall be punished with imprisonment of seven years or fine extendable to 5 million Rupees or both (Pakistan 20160.

Electronic Forgery

Anyone who makes a misuse of information system or data having the intention to cause damage or harm to the public or any other person or make any illegal claim or title to some property or enter an agreement to commit fraud will be punished with imprisonment of three years or fine of two LACS and fifty thousand Rupees or both. Anyone who commits the same offence with regard to a sensitive information system or data will be punished for seven years imprisonment or a fine of 5 million Rupees or both (Pakistan, 2016).

Spoofing

It is an act of deceiving a communication from a not known source pretending to be a trusted or known source (Forcepoint, 2019). In this scenario a programmer pretends that a certain type of data is true while in reality it isn't and that data is used for criminal purposes.

As per section 26 of PECA 2016 (Pakistan, 2016), anyone who creates a web portal or communicates any information with a deceptive source with intention to be believed to be valid by the receiver commits spoofing. The punishment for such crime is three years jail or with 5 Hundred thousand rupees or both.

Virus Attacks

The virus is a computer program. Two brothers from Sialkot were the pioneers of this idea and constructed this computer program and with good intention, the reason being to stop piracy. The first virus which they made was given the name of 'Brains".

The purpose of this program was to restrict and stop the making of pirated and copied original software. But with the development of time and technology, this program was also used for illegal purposes. Viruses are small software programs that are made to expand from one computer to another and to interfere with computer systems and operations (Yar, 2006). Once a virus enters a system, it corrupts and damages all the files and data present in a hard disk or hard drive. In majority of cases it is an irreversible phenomenon because in such situations the data damaged cannot be retrieved.

The following are the most destructive viruses ever made:

i. ILOVEYOU
ii. Code red
iii. Melissa
iv. Sasser
v. Zeus

Impersonation

To attempt to deceive someone by pretending that you are another person (DAWN news, 2018). Since the emergence of different social networking sites, the issue of impersonation has become very common. It is an illegal and immoral thing to do. Such types of acts are done either to defame a person or company or any other institution by spreading fake and untrue news, explicit content etc. It is a form of identity theft. As per section 16 of PECA 2016,

Anyone who misuses another person's identity without his formal approval will be punished for three years' imprisonment or fine up to five million Rupees or both. The aggrieved person whose identity has

been stolen may apply to the concerned authority to ask for destroying or blocking that identity and take necessary steps to prevent that identity theft in future (Pakistan, 2016).

Protection Modesty

As per section 21 of PECA 2016, anyone who with a willful intention publicly exhibits or transfer any information by editing a photograph of the face over an obscene image or video or entice such a person to engage in a sexual activity resulting in hatred, blackmailing shall be penalized for a five years term imprisonment or fine of five million or both (Pakistan 2016) Anyone who commits the same crime with respect to a minor shall be punished to seven years jail with five million Rupees.

Modern Trends in Cyber Crime

As per the reports of the World Economic Forum, two billion data was compromised in 2017and 4.5 billion in 2018. Here are some cybercrime trends:

Phishing

It is an unlawful practice in which an email representing a well reputed MNC is sent to a user in order to get all the personal data of the user. It is a fraudulent practice. The user gets trapped easily and this makes phishing one of the most successful cyber-attacks. The phishing sites are active for just a few hours.

Remote Access Attacks

An attack that targets one or more than one network of computers. The attacker finds vulnerable points to access the system. Its main aim is to steal data and leave a virus to further damage the system. In the recent past there was another type of attack known as crypto jacking which targeted the cryptocurrency owners. Computers, smart phones and other electronic devices can easily be targeted.

Smartphones

It is a very common phenomenon in today's world, attacking someone's smartphone due to no security and unsafe browsing. 80% of mobile fraud is done by mobile apps. In today's busy world where one does not have enough time, smartphone is used for transactions and other work purposes, this increase the probability of one being at risk of getting attacked by a hacker due to insecure browsing. The threat rises when a mobile phone is lost or stolen.

Artificial Intelligence

Artificial intelligence is the ability of a computer to think and learn. The biggest industries of the world use artificial intelligence. At the same time AI systems are easy to use and cheap and for hackers it's a piece of cake to attack it.

United States VS Kevin Mitnick

The Kevin Mitnick case is a case of great significance and this case drew a lot of crowd nationally and internationally. He is an American computer programmer and an expert hacker. Born in California and educated at Pierce College, he worked as a consultant in an American security company. Since he was very young, he had this love for electronics and computers. He hacked into systems of top companies and caused damage to it resulting in millions of dollars. He was accused of computer trespassing and intrusions into systems of big companies and commercial sector systems. Those international companies themselves were of millions of dollars in worth. He was also previously accused of hacking and disturbing other

computer systems and damaging different networks. One of his notorious acts also included hacking into transport systems for free rides.

According to a rough estimate, the damages caused by him coasted different corporations nearly 300million dollars. The famous companies that he hacked into are Nokia, Samsung, and Motorola etc. They also hacked into a mainframe computer of a telecommunication company and obtained different patterns, codes, keys and manuals.

His way of working and techniques were so difficult and highly sophisticated that it was nearly impossible for the investigative agencies to catch him red handed. He hacked into many other corporations' too and un-authoritatively copied different keys, codes and patterns of different access points. He was caught in 1995 and pleaded guilty for the illegal acts that he committed and was sentenced imprisonment for 3 years and 10 months. As of now, he owns a security company for better computing security solutions.

Conclusion

Today's era is the era of data and a decade from now on there will be an era of data currency. But this success of technology is directly proportional to cybercrime. The diverse nature of cybercrime makes investigation difficult for different agencies, because every day a new app is made and also a new way to crack that specific act. Sophistication is being achieved in the technological development and as both the phenomenon of cybercrime and technology are intertwined, there is a long way to tackle it. With the advancement of technology, a new way of tampering and hacking into it is discovered. Countries like China, United States of America, England, France, Japan, Korea etc. are considered to be the top digital and information technology hubs, but still due to cyber-criminal activities, the above mentioned countries have to face serious trouble and damage resulting in billions and billions of dollars. No proper system or software can be introduced by any company and corporation that could tackle all the cyber criminals and all of their cybercriminal activities. Can cybercrime be ended? The answer is "no", it can only be restricted to a limited extent.

In Pakistan cyber stalking, cyber harassment, spoofing, spamming, extortion, kidnapping, terrorism is a very big problem. In 2016 the "Prevention of Electronic Crime Act" was legislated by the government. It indeed helped the Federal Investigation Agency (FIA) a lot. But still there remain many flaws. With no policy on cybercrime, no proper investigation techniques lack of latest systems, experts in computer and digital forensics the problem still remains. The role of academia, experts and military in combating cybercrime is inevitable. However, a balance must be maintained between cyber security and fundamental rights of citizens. The former would fail if it infringes upon the latter. Such problems need to be dealt with on emergency grounds. Overcoming such problems isn't a very difficult task. The digital world is evolving at a very high speed. All of the modern economies and education systems etc. of the developed countries are based on Information Technology and advanced digital systems. Pakistan is still in developing process and slowly and gradually keeping pace with the world. Because of this technology they're a century ahead of us. In order to compete with the modern developed world, we have to pay special attention to our IT sector. The government must set forth a flawless policy on cybercrime, digital world and information technology so that we stand amongst the first world countries.

Reference

Black, S. K. (2007). Child Pornography . Retrieved April 14, 2019, Retrieved from: https://www.sciencedirect.com/topics/social-sciences/child-pornography

Dawn news, (2018). FIA report on Cyber crime. Retrieved June 27, 2020 from the Dawn news website: http://www.dawn.com/news/1440854

Forcepoint. (n.d.). What is Spoofing? Retrieved April 15, 2019, Retrieved from: https://www.forcepoint.com/cyber-edu/spoofing

Garner, B. A. (2001). *Blacks Law Dictionary*. Minnesota: West Publishing Company.

Grabosky, P. (2004). The Global Dimension of Cybercrime. Global Crime , 146-157.

Hick, s. (2000). Human Rights and the Internet. London: Palgrave Macmillan.

Jaishankar, D. H. (2012). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations . Hershey: Information Science Reference.

Mali, P. (2006). A Text Book of Cybercrime and Penalties. Indiana : Repressed Publishing.

McQuade, S. C. (2009). Encyclopedia of Cybercrime. Westport: Greenwood Press.

Mohiuddin, Z. (2006). Cyber Laws in Pakistan; A situational Analysis and way forward. Islamabad: Ericsson Pakistan (PVT.) LTD. .

Nations, U. (2001, January 22). General Assembly. Retrieved April 15, 2019, from UN Docs: https://undocs.org/A/RES/55/63

Pakistan, N. A. (2016, August 22). The Gazette of Pakistan. Retrieved april 13, 2019, from National Assembly: http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

Parker, D. B. (1989). Computer Crime: Criminal Justice Resource Manual. New York: Davis Assoc.

Saqib. (2017). The Defamation Ordinance 2002. Islamabad: Federal Law House.

Seacord, R. C. (2004). Formatted Output. Pittsburgh: Carnegie Mellon University.

Security, P. (2018, august 20). Types of cyber crime. Retrieved febuary 24, 2019, from O panda: https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/

Staff, P. (2015, January 17). Top 10 Countries That Watch The Most Porn. Retrieved April 14, 2019, from Postober : https://postober.com/2015/01/17/top-10-countries-that-watch-the-most-porn/#

Tech, F. (2019). A Brief History of Cyber Crime. Retrieved Febuary 24, 2019, from Florida Tech Onilne: https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/

Townsend, C. (n.d.). (In)Famous Hacking Groups. Retrieved april tuesday, 2019, from United States Cyber security magazine: https://www.uscybersecurity.net/infamous-hacking-groups/

University, C. (n.d.). Legal Information Institute. Retrieved April 14, 2019, from Cornell: https://www.law.cornell.edu/wex/pornography

Yar, M. (2006). Cybercrime and society . Lancaster: SAGE Publications Ltd.