Cyber Crime in India: An Empirical Study

Prof. Saquib Ahmad Khan

ABSTRACT:
Cybercrime can be defined as an "illegal act in which a computer is a tool or a goal or both". Late, the use of computers has become extremely common and popular. However, the misuse of technology in cyberspace has led to cybercrime both nationally and internationally. With the intention of regulating criminal activities in the cyber world and protecting the technological advancement system, the Indian parliament approved the law on technological information, 2000. It was the first global law of India to deal with technology in the field of e-commerce, e-governance, electronic banking services, as well as penalties and punishments regarding computer crimes. This document will discuss the common types of cyber-crime and measures to prevent cybercrime.

KEYWORDS: Cyber bullying, cyberspace, phishing, spam.

I. INTRODUCTION:

Computer crimes include criminal activities carried out using computers that further perpetrate crimes such as phishing, counterfeiting, cyber-bullying, pornography, bombardment of e-mails, spam, sale of illegal articles, etc. Although cyber-crime has its general meaning as "A legal error that can be followed by criminal proceedings that can result in punishment".

Cyber Security is defined as a crime in which a computer is subject to crime (piracy, phishing, spam) or used as a tool to commit a crime (child pornography, hate crimes). Cyber-criminals can use computer technology to access personal information, trade secrets or use the Internet for malicious or exploitative purposes.

Cyber security laws helps in preventing or reducing large-scale damage to cyber-crime activities and protects access to information, privacy, communications, intellectual property (IP) and freedom of expression in relation to the use of the Internet, websites, and email, computers, mobile phones, software and hardware, such as data storage devices. The increase in Internet traffic has led to a greater percentage of legal problems worldwide. Since cyber laws vary according to jurisdiction and country, the application is a challenge and the restitution goes from fines to imprisonment.

- *Author name is currently pursuing Ph.D. from Shri Jagdishprasad Jhabarmal Tibrewala University (Registration Id: 29117038), Rajasthan. Holding a degree of Masters in Business Administration from Himalayan University, Masters in Commerce from University of Mumbai and Masters in Computer Management from University of Pune, backed with Bachelor of Commerce from University of Mumbai.*

II. LITERATURE REVIEW:

2.1. Animesh Sarmahand and Amlan Jyoti Baruah (2017):

The authors of this article claim that criminal activities or Internet related offenses / crimes are called cybercrime. To stop or punish cyber criminals, the term "Cyber Law" has been introduced. The authors believe that cyber law is the part of legal systems that deals with the Internet, cyberspace and legal issues. It covers a large area, covering many secondary topics, as well as freedom of expression, Internet access and use and online security or online privacy. It is generally referred to as web law. The primary goal of the author when writing this document was to spread the content of cybercrime among ordinary people. At the end of the document "A Brief Study on Cyber Crime and Cyber Laws in India", the authors said that cybercrime can never be recognized. If someone falls into the cyber-attack dam, file and register a case at the nearest police station. If criminals are not punished for their actions, they will never stop.

2.2. Anuraj Singh (2007):

Cyber law in India needs such laws so that people can make online purchase transactions via credit cards without fear of abuse. The law provides the much needed legal framework so that information is not denied for legal effect, validity or enforceability, just because it is in the form of electronic records. Cybercrime is inevitable, omnipresent and increasingly linked to different parts and areas of criminal contexts. This evolution and this network have given rise to cyberspace which controls and manages to provide equal opportunities and facilities for all people to access any type of information. Due to the gradual growth of the Internet, technology abuse is gradually expanding, leading to cybercrime. Cybercrime is basically an illegal act that leads to criminal activity. Cyber security, a mechanism by which information about computers and equipment is protected

from unauthorized and illegal access. This document illustrates and focuses on cybercrime, its impact on society, the types of threats and cyber security. Today, cybercrime problems and theft have become tremendously evident, particularly those related to copyright infringement, piracy, child pornography, and childcare and identity theft.

III. OBJECTIVE:

- To. Understand the concept of cyber-crime.
- To get an overview of the common types of cyber-crime.
- Know the steps to prevent cybercrime.

3.1CYBER CRIME AND CYBER LAW:

Cybercrime is the result of our high dependence on cyberspace or the so-called Internet world. Computer crimes are illegal / illegal acts in which the computer is used as a tool or a target or both. The first reported computer crime was in the 1820s. The enormous growth of e-commerce (e-commerce) and the exchange of online shares led to a phenomenal outbreak in cybercrime incidents. The Information Technology Act, 2000, is the main legislation dealing with the rules and regulations relating to the cyber world; it provides a step forward in the field of law with the changing and modernized dimension of the crime world. The main objective of the law is to provide legal recognition for electronic commerce and to facilitate the submission of electronic registers to the government. The computer law also criminalizes various computer crimes and establishes severe penalties (prison sentences of up to 10 years and compensation of up to 1 rupee rupee).

3.2. COMMON CYBER CRIMES:

The different types of computer crimes are:

- Unauthorized access and piracy:
  Unauthorized access means any type of access without the authorization of any legitimate or responsible computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and / or a network. Every act committed to enter a computer and / or network is piracy. Hackers write or use ready-to-use computer programs to attack the target computer. They have the desire to destroy and get the kick of that destruction. Some hackers compromise personal monetary gains, such as stealing credit card information, transferring money from different bank accounts to their account, followed by withdrawing money. Government websites are the most specific sites for hackers.
- Hijacking the Web:
  Web hijacking means taking strong control of another person's website. In this case, the website owner loses control over his website and its content.
- Pornography:
  Pornography means showing sexual acts to cause sexual arousal. The definition of pornography also includes pornographic websites, pornographic magazines produced using computers and Internet pornography provided via mobile phones.
- Child pornography:
  Pedophiles attract children by distributing pornographic material and then try to meet them to have sex or take nude photographs, including their participation in sexual positions. Pedophiles sexually exploit children, using them as sexual objects or taking their pornographic photos to sell them on the Internet.
- Cyber bullying:
  Cyberbullying means repeated acts of harassment or threatening behavior of the cyber-criminal against the victim through the use of Internet services.
- Denial of Service attack:
  This is an attack in which the criminal floods the victim's network bandwidth or fills his spam inbox that deprives him of the services to which he has the right to access or provide. This type of attack is designed to block the network by flooding it with unnecessary traffic.
- Virus attacks:
  Viruses are programs that have the ability to infect other programs and make copies of themselves and spread on another program. Viruses generally affect data on a computer by modifying or deleting them. Trojan Horse is a program that behaves like something.
- Software piracy:
  Software piracy refers to the illegal copying of original programs or the falsification and distribution of products intended to pass through the original. These types of crimes also include copyright infringement, trademark infringement, theft of computer source code, patent infringements, etc.
- Salami attacks:
  These type of attacks are used for the commission of financial crimes. The motive here is to make the changes so insignificant that, in a single case, it would go completely unrecognized. For an illustration, if an employee on the banks server, inserts a program that deducts a small amount of

money (for example ₹ 5 per month) from each client's account. No account holder will probably notice this unauthorized debt, but the bank employee will earn a significant amount of money each month.

- Phishing:
  Phishing is the act of sending an e-mail to a user who falsely claims to be a legitimate company founded in an attempt to defraud the user in providing private information that will be used for identity theft.
- Sale of illegal items:
  This category of cybercrime includes the sale of drugs, weapons and wild animals, etc., by publishing information on websites, auction and bulletin board websites or simply using e-mail communication.
- Online game:
  There are millions of websites; all hosted on servers abroad, offering online gambling. Indeed, it is believed that many of these websites are actually money laundering fronts. Cases of hawala transactions and money laundering have been reported online.
- Email spoofing:
  E-mail representation refers to e-mail that appears to come from a source but has actually been sent from another source. Representation by e-mail can also cause monetary damage.
- Cyber Defamation:
  When a person posts a defamatory question about someone on a website or sends e-mails that contain defamatory information to all of that person's friends, it is called cyber defamation.
- Falsification:
  Computers, printers and scanners are used to counterfeit invoices, postal and entry labels, brand sheets, etc. They are manufactured with high quality computers and scanners and printers.
- Theft of information in electronic format:
  This includes theft of information stored on computer hard drives, removable storage media, etc.
- Bombardment by email:
  The Bombardment by email refers to sending a large number of e-mails to the victim resulting in blocking of the victim's e-mail account (in the case of an individual) or mail servers (in the case of a company or an email service provider).
- Data distribution:
  This type of attack involves altering the raw data before the computer processes them and then changes them again after processing is complete.
- Theft of time on the Internet:
  Internet time refers to the use by an unauthorized person of Internet hours paid by another person.
- Theft of the computer system:
  This type of crime involves theft of a computer, some parts of a computer or a device connected to the computer.
- Physical damage to a computer system:
  Computers or its peripherals are damaged physically under this types of crime
- Violation of privacy and confidentiality:
  Privacy refers to an individual's right to determine when, how and to what extent their personal data will be shared with others. Violation of privacy involves the use or unauthorized distribution or disclosure of personal information.
- Data distribution:
  Data deletion involves modifying the data before or while entering a computer. The information changes in the way a person who enters the data must enter it, a virus that modifies the data, the database or application programmer or any other person involved in the process of storing information in a computer file. It also includes the automatic exchange of financial information for some time before processing and therefore restoring the original information.
- Investment fraud:
  Securities fraud, also known as equity fraud and investment fraud, is a deceptive practice in equity or commodity markets that causes investors to make buying or selling decisions based on false information, which often results in losses, in violation of the Securities Laws Securities fraud, also known as equity fraud and investment fraud, is a deceptive practice in equity or commodity markets that causes investors to make buying or selling decisions based on false information, which often results in losses , in violation of securities laws
- Cyber terrorism:
  The most likely targets are attacks against military installations, power plants, air traffic control, banks, and track traffic control and telecommunications networks. Others such as police, doctors, fire and rescue systems, etc. Cyber terrorism is an interesting option for modern terrorists for several reasons.

3.3. STATISTICS ON CYBER CRIME:

India has seen a 457% increase in cybercrime incidents under the Information Technology (IT) Act, 2000 from 2011 to 2016, according to a recent joint study by ASSOCHAM-NEC.

Symantec Corp ranked India among the top five cybercrime countries, revising 2012-17, the number of Internet users grew at a compound annual rate of 44%, of which India ranked third after the United States and China. The use of the latest technologies such as artificial intelligence, big data analysis, facial recognition, IoT, etc., to identify and capture suspects / criminals, has gained a lot of awareness among different law enforcement agencies. However, the implementation of these technologies is not at the national level but at the state level, which makes it crucial for the central government to fund and support state-level law enforcement agencies to use technologies to upgrade their surveillance methods, has said the study.

The Indian government and several law enforcement agencies have taken the initiative to contain the growing cyber-crime. The state government and the state police are developing new cybercrime measures and collecting methods to deal with it with the help of central government and private organizations.

3.4. STEPS TO PREVENT CYBER CRIME:

The Information Technology Act of 2000, together with the Penal Code of India, has adequate provisions to deal with prevailing computer crimes. It provides for penalties in the form of imprisonment ranging from two years to life imprisonment and fines / penalties depending on the type of cyber-crime.

However, the government has taken the following measures to prevent cybercrime:

- The cybercrime cells were established in the States and territories of the Union to report and investigate cases of cybercrime.
- The government has set up IT research and forensic training laboratories in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu and Kashmir for the training of the police and the judiciary in these states.
- In collaboration with the Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs were established in Mumbai, Bangalore, Pune and Calcutta for awareness and training.
- Cybercrime investigation programs. National Law School, Bangalore and NALSAR University of Law, Hyderabad, are also involved in conducting various awareness-raising and training programs on law and cybercrime for court officials.
- Training is provided to police and judicial agents in training laboratories set up by the government.
- The program for the Universalization of Women Helpline was approved to provide a 24-hour emergency and non-emergency response to all women affected by the violence.

IV. METHODOLOGY:

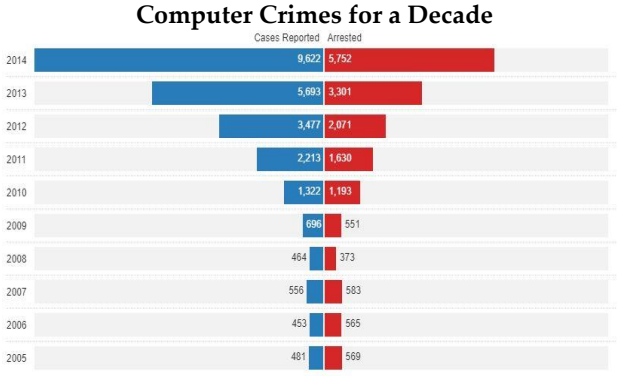
4.1. PRIMARY DATA

Primary data was not collected for the research paper.

4.2. SECONDARY DATA

Secondary data was collected. Several magazines and newspapers have been used for this, as it is a conceptual document. Therefore, the goal is to better understand the concept, its application and the impact on the economy through other parameters. Therefore, qualitative and quantitative data were used.

India ranks third in the world, after the United States and China, as a source of malicious activity in 2015, according to this 2016 report by Symantec Corp, a software security company. In 2015, India was ranked second as a source of malicious code and fourth and eighth as a source or source of web attacks and network attacks. In 2014, 9,622 computer crimes were reported, with a 69% increase compared to 2013. Of the 9,622 computer crimes reported, 7,201 were reported as crimes pursuant to the Information Technology (IT) law, 2,272 pursuant to the Criminal Code of India (IPC) and 149 under special and local laws (SLL).



Under the information technology law, most - 5,548 cases - have been referred to computer crimes, of which 4,192 in section 66A, which allows prison sentences of up to two or three years for sending offensive messages through communication service "and related crimes. Section 66A of the computer law was rejected by the Supreme Court in March 2015, stating that "this law has affected the root of freedom and freedom of expression, the two fundamental pillars of democracy". India Spend has previously reported that India has followed Turkey and Russia in restrictive laws on the Internet. India ranked 136, Turkey 149 and Russia 152

in the Press Freedom Index 2015, published by Reporters without Borders, a non-profit organization based in Paris.

V. CONCLUSION:

Cybercrime is one of the most crucial problems for countries around the world these days. Includes unauthorized access to information and violate security such as privacy, passwords, etc. anyone who has Internet use. Cyber theft is part of the cybercrime, which means robbery performed via computer or the Internet. With the increase in the number of cyber security fraud and crimes, the government is developing refined rules to protect people's interests and protect them from any negative events on the Internet. Furthermore, stricter laws regarding the protection of "confidential personal data" have been formulated in the hands of intermediaries and service providers (corporate body), thus guaranteeing data protection and privacy.

REFERENCES:

1. http://www.mondaq.com
2. https://telecom.economictimes.indiatimes.com/news
3. https://securitycommunity.tcs.com/infosecsoapbox/articles
4. http://www.helplinelaw.com/employment-criminal-and-labour
5. Anuraj Singh (2007), Volume 05, Issue 06, PP. 11273-11279.
6. Animesh Sarmahand and Amlan Jyoti Baruah (2017), Volume 04, Issue 06, PP. 1633-1640.