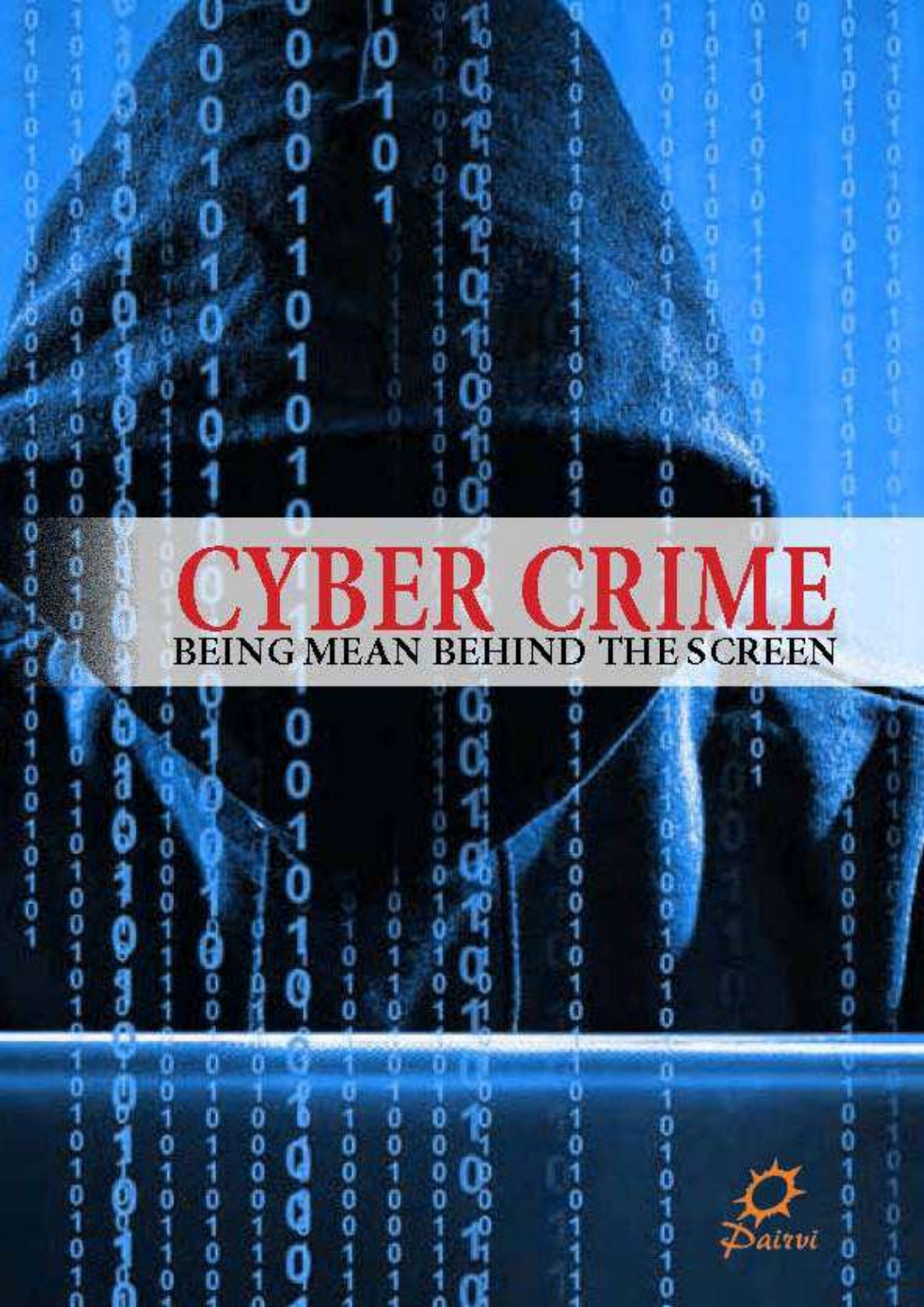

CYBER CRIME

BEING MEAN BEHIND THE SCREEN

Pairvi

CYBER CRIME; BEING MEAN BEHIND THE SCREEN

August 2018

Compiled by: Dhankakshi Gandhi
Edited by Ajay K. Jha

Layout by Rajneesh
Cover images from gettyimages.in

Published by PAIRVI
E-46, Upper Ground Floor, Lajpat Nagar-III, New Delhi-110024
Phone: +91-11-29841266, 65151897
e-mail: pairvidelhi1@gmail.com
website: www.pairvi.org

In the current era of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.

INTRODUCTION

A. MEANING OF CYBER CRIME

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet.

Cybercrimes is any criminal activity that involves a computer networked device or a network. While most cyber crimes are carried out in order to generate profit for cyber criminals , some cybercrimes are carried out against computers or devices directly to damage or disable them, while other use computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both i.e. target computers to infect them with viruses, which are then spread to other machines and sometimes entire networks.[1]

A primary impact from cybercrime is financial, and cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may target private personal information, as well as corporate data for theft and resale.

B. HOW CYBERCRIME WORKS

Cybercriminals use a number of attack vectors to carry out their cyber attacks

1 https://www.legalindia.com/cyber-crimes-and-the-law/

and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest. Here are common types of attacks cybercriminals have been known to use:

- **Distributed DoS attacks** (DDoS) are often used to shut down systems and networks. This type of attack uses a network's own communications protocol against it by overwhelming its ability to respond to connection requests. DoS attacks are sometimes carried out simply for malicious reasons or as part of a cyber extortion scheme, but they may also be used to distract the victim organization from some other attack or exploit carried out at the same time.
- **Infecting systems and networks with malware** is used to damage the system or harm users by, for example, damaging the system, software or data stored on the system. Ransomware attacks are similar, but the malware acts by encrypting or shutting down victim systems until a ransom is paid.[2]
- **Phishing** campaigns are used to infiltrate corporate networks by sending fraudulent email to users in an organization, enticing them to download attachments or click on links that then spread viruses or malware to their systems and through their systems to their company's networks.
- **Credentials attacks**, where the cybercriminal aims to steal or guess user IDs and passwords for the victim's systems or personal accounts, can be carried out through the use of brute force attacks by installing key sniffer software or by exploiting vulnerabilities in software or hardware that can expose the victim's credentials.
- Cybercriminals may also attempt to hijack a website to change or delete content or to access or modify databases without authorization. For example, an attacker may use an SQL injection exploit to insert malicious code into a website, which can then be used to exploit vulnerabilities in the website's database, enabling a hacker to access and tamper with records or gain unauthorized access to data, such as customer passwords, credit card numbers, personally identifiable information (PII), trade secrets, intellectual property and other sensitive information.

Cybercriminals often carry out their activities using malware and other types of software, but social engineering is often an important component for executing most types of cybercrime. Phishing email is an important

2 http://www.cyberlawsindia.net/index1.html

component to many types of cybercrime, but especially so for targeted attacks, like business email compromise (BEC), in which the attacker attempts to impersonate, via email, a business owner in order to convince employees to pay out bogus invoices.

C. TYPES AND CLASSIFICATION OF CYBERCRIMES

There are a huge number of cyber crimes in the world. Some of them are discussed below by classifying them into various categories. Cybercrime can be classified into four major categories as -

1. CYBER CRIME AGAINST INDIVISUALS
2. CYBER CRIME AGAINST PROPERY
3. CYBER CRIME AGAINST ORGANISATION
4. CYBER CRIME AGAINST SOCIETY

1. CYBER CRIME AGAINST INDIVISUALS

This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

- **Harassment via E-Mails:** It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter etc. increasing day by day.[3]
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system

3 http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp

and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account malafidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. CYBER CRIME AGAINST PROPERTY

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which effects person property are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents,

designs and service mark violation, theft of computer source code, etc.

- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.comand www.yaahoo.com.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hackers attacks those famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.[4]
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

4 http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp

3. CYBER CRIME AGAINST GOVERNMENT ORGANISATION[5]

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

4. CYBER CRIME AGAINST SOCIETY AT LARGE

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes :

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.
- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through

5 http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp

internet. Ex: Using credit cards by obtaining password illegally.[6]

- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

D. WHO INVOVED IN CYBER CRIME[7]

1. THE GREED MOTIVTAED (CAREER CRIMINALS)

This type of cyber criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime as long as it brings money to them. They are usually very smart and organized and they know how to escape the law enforcement agencies. These cyber criminals are committing grievous crimes and damages particularly in child pornography and cyber gambling is a serious threat to the society.

2. THE IDEALISTTS (TEENAGERS)

They are usually not highly trained or skillful but youngsters between the ages of 13-26 who seek social recognition. They want to be in spotlight of the media. Their actions are globally damageable but individually negligible. Most often they attack systems with viruses they created causing harm to other individuals.

3. THE CYBER TERRORISTS

They are the newest and the most dangerous groups. Their primary motive is just not money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems . The threat of cyber terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. They have no state frontier and they operate from anywhere in the world thus making it difficult for them to get caught.

---

6 http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp

7 https://prezi.com/srqxdk-xfode/the-causes-of-cyber-crime-and-the-effect-of-cyber-crime/

E. CAUSES OF CYBER CRIME[8]

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber crime. Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber crime across the world.

1. THE SAKE OF RECOGNITION[9]

Basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular. They fall into the category of the idealists who just want to be in spotlight.

2. MAKE QUICK MONEY

This group is greed motivated and is career criminals who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.

3. REVENGE

Based on the statistics about 78% of cyber criminal do this type of crime because they want to revenge to someone. Usually cyber-bully are bullied in a physical way in the real world. Since they can't revenge it by physically attacking the person so they use internet to take revenge.

4. ALLEVIATE BOREDOM

Sometimes youngsters will cyber-bully to fit in with a group of friends or a clique. As a result these youngsters succumb to peer pressure I order to be accepted by a group at school, even if it means going against their better judgment. They are more concerned with fitting in than they are worried about the consequence of cyber bullying. Others bully because there is a false sense of security in numbers.

---

8 https://www.google.co.in/search?rlz=1C1CHBD_enIN780IN780&q=causes+of+cybercrime+in+india&sa=X&ved=0ahUKEwiepfe-opTcAhXKso8KHTE2AzoQ1QIIpgEoAQ&biw=1137&bih=735

9 https://prezi.com/srqxdk-xfode/the-causes-of-cyber-crime-and-the-effect-of-cyber-crime/

F. HISTORY OF CYBER CRIME

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious[10] software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became more skillful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

G. CYBER CRIME IN MODERN SOCIETY

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

10 https://searchsecurity.techtarget.com/definition/cybercrime

IMPACT OF CYBER CRIME[11]

A. ON BUSINESS

The true cost of cybercrime is difficult to accurately assess. In 2018, McAfee released a report on the economic impact of cybercrime that estimated the likely annual cost to the global economy was nearly $600 billion, up from $45 billion in 2014.

While the financial losses due to cybercrime can be significant, businesses can also suffer other disastrous consequences as a result of criminal cyber attacks, including:

- Damage to investor perception after a security breach can cause a drop in the value of a company. In addition to potential share price drops, businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a cyber attack.
- Loss of sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data. Businesses may also be sued over the data breach.
- Damaged brand identity and loss of reputation after a cyber attack undermine customers' trust in a company and that company's ability to keep their financial data safe. Following a cyber attack, firms not only lose current customers, they also lose the ability to gain new customers.

Businesses may also incur direct costs from a criminal cyber attack, including the cost of hiring cyber security companies to do incident response and remediation, as well as public relations and other services related to an attack and increased insurance premium costs.

B. ON NATIONAL DEFENCE[12]

Cybercrimes may have public health and national security implications, making computer crime one of the Department of Justice's top priorities. In the United States, at the federal level, the FBI's Cyber Division is the agency within the Department of Justice that is charged with combating cybercrime.

11 https://link.springer.com/article/10.1007/s10611-016-9629-3

12 https://link.springer.com/article/10.1007/s10611-016-9629-3

The Department of Homeland Security (DHS) sees strengthening the security and resilience of cyberspace as an important homeland security[13] mission, and agencies such as the U.S. Secret Service (USSS) and U.S. Immigration and Customs Enforcement (ICE) have special divisions dedicated to combating cybercrime.

The Secret Service's Electronic Crimes Task Force (ECTF) investigates cases that involve electronic crimes, particularly attacks on the nation's financial and critical infrastructures. The Secret Service also runs the National Computer Forensics Institute (NCFI), which provides state and local law enforcement, judges and prosecutors with training in computer forensics. The Internet Crime Complaint Center (IC3), a partnership between the FBI, the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA), accepts online complaints from victims of internet crimes or interested third parties.

13 https://searchsoftwarequality.techtarget.com/definition/SQL-injection

PRESENT TRENDS OF CYBER CRIME IN INDIA

In the case of cyber crime, large numbers of suitable targets may emerge through increasing time spent online, and the use of online services such as banking, shopping and file sharing making users prone to phishing attacks or fraud. The major cyber crimes reported in India are denial of web services, hacking of websites, computer virus and worms, pornography, cyber Squatting, cyber stalking and phishing. Nearly 69 percent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information.

According to Symantec's (American Global Computer Security Software Corporation) internet security threat report on April 29, 2017, India has seen a 280 percent increase in both infections that is continuing to spread to a larger number of emerging cities in India. India has the highest ratio in the world of outgoing spam or junk mail of around 280 million per day worldwide. India's home PC owners are the most targeted sector of cyber attacks. Mumbai and Delhi emerging as the top two cities for cyber crime.

In India, at least one cyber attack was reported every 10 minutes in the first six months of 2017.[14] In 2017, as per the Indian Computer Emergency Response Team (CERT-In), a total of 27,482 cases of cybercrimes have been reported across the world. These include phishing, site intrusion, virus, and ransomware. The cyber experts told that with the programs such as Digital India in place, more Indians are surfing the Internet and hence, it is crucial to put critical infrastructure in place to predict and prevent cybercrimes.

With the high percentage of cybercrime coming forward this year, the numbers are expected to shoot up in future. Mirza Faizan Asad, a cyber crime expert was quoted by saying : " The government is making an effort to reduce online crimes but the firms and the individuals need to be ready with a strong team that is programmed for preventing such crimes." He added: "It is not just enough to make efforts at the government level, which is, in some sense happening, but cybercrime affects hundreds of individual

14 https://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

systems and firms, all of whom need to be ready with specialized teams."

A total of 1.71 lakh cybercrimes were reported in India in the past three-and-a-half years. The number of crimes that have been reported so far (27,482) indicates that the total number is likely to cross 50,000 by December.

In the past three years, ransomware[15] attacks have increased. In this, the attacker threatens to publish the data of a person online until a certain amount of ransom is paid. The attackers demand ransom in bitcoins (a digital currency), a secure way for accepting this type of payment.

15 https://blog.ipleaders.in/need-know-cyber-laws-india

CYBER LAWS IN INDIA[16]

In India, cyber laws are contained in The Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

India has an extremely detailed and well-defined legal system in place. Numerous laws have been enacted and implemented and the foremost amongst them is the Constitution of India. We have inter alia, amongst others, the Indian Penal Code, the Indian Evidence Act 1872, the Reserve Bank of India Act, 1934, the Companies Act, and so on. However, the arrival of internet signaled the beginning of the rise of new and complex legal issues. It may be pertinent to mention that all the existing laws in place in India were enacted way back keeping in mind the relevant political, social, economic, and cultural scenario of that relevant time. Nobody then could really visualize about the Internet. Despite the vivid insight of our master draftsmen the requirements of cyberspace could hardly ever be anticipated. As such, the coming of the Internet led to the emergence of numerous tricky legal issues and glitches which required the enactment of Cyber laws.[17]

The existing laws of India, even with the most compassionate and liberal interpretation could not be interpreted in the light of the emergency cyberspace, to include all aspects relating to different activities in cyberspace. In fact, the practical experience and the wisdom of judgment found that it shall not be without major threats and pitfalls, if the existing laws were to be interpreted in the scenario of emerging cyberspace, without enacting new cyber laws. Hence the need for enactment of relevant cyber laws.[18]

None of the existing laws gave any legal validity or sanction to the activities in Cyberspace. For example, the Net is used by a large majority of users for email. Yet till today, email is not "legal" in our country. There

16 https://www.taxmann.com/bookstore/academic/cyber-crimes-and-laws.aspx?campaign=216327700&content=47545801420&keyword=&gclid=EAIaIQobChMI5s7GitT3AIVSIaPCh3X4gOFEAQYBCABEgLKzPD_BwE

17 http://www.legalserviceindia.com/cyber/cyber.htm

18 http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws

is no law in the country, which gives legal validity, and sanction to email. Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email in the absence of any specific law having been enacted by the Parliament. As such the need has arisen for Cyber law.

Internet requires an enabling and supportive legal substructure in tune with the times. This legal infrastructure can only be given by the enactment of the relevant Cyber laws as the traditional laws have failed to grant the same. E-commerce, the biggest future of Internet, can only be possible if necessary legal infrastructure compliments the same to enable its pulsating growth.

All these and other varied considerations created a conductive atmosphere for the need for enacting relevant cyber laws in India.

A. NEED OF CYBER LAWS IN INDIA

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit/debit cards for shopping.
- Most people are using email, phones and SMS messages for communication.

Even in "non-cyber crime" cases, important evidence is found in computers/cell phones ex : in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks,

cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.

- Digital signatures and e-contracts are fast replacing conventional method of transacting business.

Technology per se is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickle-down effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic matrix.

If a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India?

According to Section 1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further Section 75 of the I.T. Act, 2000[19] also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section,

The Act will apply to an offence contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

A Police officer not below the rank of Deputy Superintendent of Police should only investigate any offence under this Act. (Sec. 78 of I.T Act, 2000)

Without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition.

B. IMPORTANCE OF CYBER LAWS IN INDIA

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber law is a very technical field and that it does not have any bearing to most activities in Cyberspace. But

19 https://www.google.com/search?ei=Kac9W8r8OMX4vASV0Lm-QDg&q=cyber+crime+IN+INDIA&oq=cyber+crime+IN+INDIA&gs_l=psy-ab.3...16344.21259.0.22010.9.9.0.0.0.0.489.489.4-1.1.0..1..0...1.1.64.psy-ab..8.1.488...0j0i67k-1j0i131i67k1.0.Pu37ajfxor0

the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

1. INFORMATION TECHNOLOGY ACT,2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cyber crime and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.The original Act contained 94 sections, divided in 13 chapters and 4 schedules.[20] The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India the Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formation of Controller of Certifying Authorities was directed by the Act, to regulate issuing of digital signatures. It also defines cyber crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

2. AMENDMENTS

A major amendment was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

Notable features of the ITAA 2008 are:

- Focusing on data privacy
- Focusing on Information Security

20 https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offenses (as against the DSP earlier)

3. OFFENCES

List of offences and the corresponding penalties

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/ and with fine up to Rs200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/ and with fine up to Rs500,000

66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/ and with fine up to Rs100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/ and with fine up to Rs100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/ and with fine up to Rs100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/ and with fine up to Rs200,000
66F	Acts of cyber terrorism	If a person denies access to an authorized personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyber terrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave	Imprisonment up to five years, or/ and with fine up to Rs 1,000,000

		and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/ and with fine up to Rs1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to Rs1,000,000 on first conviction. Imprisonment up to seven years, or/ and with fine up to Rs1,000,000 on second conviction.
67C	Failure to maintain records	Person deemed a as intermediate (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/ and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules	Imprisonment up to three years, or/ and with fine up to Rs200,000

		or any regulations made there under. Any person who fails to comply with any such order shall be guilty of an offence.	
69	Failure/refusal* to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer	Imprisonment up to ten years, or/ and with fine.

* https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

		system or computer network to be a protected system. The appropriate Government** may, by order in writing, authorize the persons who are authorized to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	
71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/ and with fine up to Rs100,000

** http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

For other type of crimes such as cheating, fraud, forgery, threat, misappropriation, defamation , etc committed by using computer Indian Penal Code has certain sections that are listed below :

CYB ER CRIMES	ACT & SECTIONS
Sending threatening messages by email	Sec 506 IPC
Sending defamatory messages by email	Sec 500 IPC
Forgery of electronic records	Sec 465 IPC
Bogus websites , cyber fraud	Sec 420 IPC
Email spoofing	Sec 465 IPC
Online sales of drugs	NDPS ACT
Web Jacking	Sec 384 IPC
Online sales of arms	ARMS ACT

C. ADVANTAGES OF IT ACT 2000

The IT ACT 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.[21]

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.[22]
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities[23] for issuing Digital Signatures Certificates.
- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a

21 https://www.legalindia.com/cyber-crimes-and-the-law/

22 https://blog.ipleaders.in/need-know-cyber-laws-india/

23 https://www.informationvine.com/index?qsrc=999&qo=semQuery&ad=semD&o=758673&l=sem&askid=b256e4c1-4f30-4da6-95e2-c09de3a8acb0-0-iv_gsb&q=cybercrime%20and%20cyber%20law%20ppt&dqi=&am=broad&an=google_s

legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

- Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

D. LEADING CASES UNDER IT ACT 2000

Section 43 – Penalty and Compensation for damage to computer, computer system, etc [24]

Related Case: Mphasis BPO Fraud 2005

In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs. In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000.

Verdict:

Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.

Section 65 – Tampering with Computer Source Documents

Related Case : Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh

In this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocomm.

---

24 http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

Verdict:
Court held that tampering with source code invokes Section 65 of the Information Technology Act.

Section 66 – Computer Related offenses

Related Case: Kumar v/s Whiteley

In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users. Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers. The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.

Verdict:

The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Section 66A – Punishment for sending offensive messages through communication service

Relevant Case #1: Fake profile of President posted by imposter

On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook. The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Relevant Case #2: Bomb Hoax mail [25]

In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

Section 66C – Punishment for identity theft

Relevant Cases:

The CEO of an identity theft protection company, Lifelock, Todd Davis's social security number was exposed by Matt Lauer on NBC's Today Show. Davis' identity was used to obtain a $500 cash advance loan.

Li Ming, a graduate student at West Chester University of Pennsylvania faked his own death, complete with a forged obituary in his local paper. Nine months later, Li attempted to obtain a new driver's license with the intention of applying for new credit cards eventually.

Section 66D – Punishment for cheating by impersonation by using computer resource

Relevant Case: Sandeep Vaghese v/s State of Kerala

A complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code.

The company has a web-site in the name and and style www. jaypolychem.com' but, another web site www.jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the sister and brother-in-law of `Sam'

Defamatory and malicious matters about the company and its directors

25 http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

were made available in that website. The accused sister and brother-in-law were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused immense damage to the name and reputation of the Company.

The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

Section 66E – Punishment for violation of privacy

Relevant Cases: #1. Jawaharlal Nehru University MMS scandal[26]

In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university. Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

#2. Nagpur Congress leader's son MMS scandal

On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

Section-66F Cyber Terrorism[27]

Relevant Case:

The Mumbai police have registered a case of 'cyber terrorism'—the first in

26 http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

27 https://www.google.co.in/search?q=indiankanoon&rlz=1C1CHBD_enIN780IN780&oq=INDIANKA&aqs=chrome.0.0j69i57j0l4.9689j0j7&sourceid=chrome&ie=UTF-8

the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case. The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.comat around 10.44 am on Monday. The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna," said an officer.

Status:

The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act.

Section 67 – Punishment for publishing or transmitting obscene material in electronic form[28]

Relevant Case:

This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the lady's complaint, the police nabbed the accused. Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet.

Verdict:

The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000. He is convicted and sentenced for the offence as follows:

- As per 469 of IPC he has to undergo rigorous imprisonment for 2 years and to pay fine of Rs.500/-

28 http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

- As per 509 of IPC he is to undergo to undergo 1 year Simple imprisonment and to pay Rs 500/-
- As per Section 67 of IT Act 2000, he has to undergo for 2 years and to pay fine of Rs.4000/-

All sentences were to run concurrently.

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Relevant Case: Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation

The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Relevant Case:

In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut.The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m.

Verdict:

Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.

E. PREVENTIVE MEASURES FOR CYBER CRIMES

Prevention is always better than cure. A citizen should take certain precautions while operating the internet and should follow certain preventive measures for cyber crimes which can be defined as:

- Identification[29] of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers via e-mail or while chatting.
- One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the citizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.
- Web servers running public sites must be physically separately protected from internal corporate network.
- It is better to use a security programs by the body corporate to control information on sites.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of citizens.
- IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.
- As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.
- A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

29 https://www.legalindia.com/cyber-crimes-and-the-law/

HOW INDIAN POLICE IS TRAINED IN CONTROLLING CYBER CRIME[30]

Personnel from nearly 1,000 police stations in Karnataka will be trained to handle cybercrimes as the state plans one cybercrime station per district by 2019.

Praveen Sood, Director General of Police (CID), who has begun an intensive two-stage training programme on how to deal with hacking, online harassment, credit/debit card fraud, data theft et al, for ranks till the level of constable. He maintains that training personnel remains the challenge when it comes to dealing with digital crime.

Karnataka was the first to establish a dedicated police station to handle digital crime 15 years ago. Other states, including Uttar Pradesh and Maharashtra, have stepped up police training, including seeking out experts from industry.

The ministry of electronics and information technology has collaborated with the Data Security Council of India (DSCI) to set up cyber forensic labs in all metro cities for training and building awareness of cybercrime investigation.

The national Information Security Education & Awareness (ISEA) program expects to train over one lakh people — not just police personnel — by 2020.

Balasingh Rajput-Superintendent of Police Cyber Maharashtra says that currently Maharashtra Police has set up a nodal agency which connects with the specially set up cyber Police stations across the state.

The Delhi Police[31] has tapped into the expertise at the Indian Space Research Organization in order to develop a predictive policing tool called CMAPS – Crime Mapping, Analytics and Predictive System. The system identifies crime hotspots by combining Delhi Police's Dial 100 helpline calls data with ISRO's satellite imagery and visualizing it as cluster maps. Using CMAPS, Delhi Police has slashed its analysis time from the 15 days it took

30 https://tech.economictimes.indiatimes.com/news/internet/how-indian-police-is-being-trained-to-tackle-cybercrime/63652035

31 https://ccgnludelhi.wordpress.com/2017/03/24/law-enforcement-initiatives-towards-tackling-cyber-crime-in-india/

with its erstwhile mechanical crime mapping to the three minutes it takes for the system to refresh its database.

The Hyderabad City Police is in the process of building a database, called the 'Integrated People Information Hub' which, according to the City Police Commissioner, would offer the police a "360-degree view" of citizens, including names, aliases, family details, addresses and information on various documents including passports, Aadhaar cards and driving licenses.

The data is combed from a wide-ranging variety of sources, including information on arrested persons, offenders' list, FIRs, phone and electricity connections, tax returns, RTA registrations and e-challans. It is further indexed with unique identifiers, and is used to establish the true identity of a person, and present results to relevant authorities within minutes. While the system is aimed at curbing criminal activity and detecting fraud, a lack of clearly identified cyber security and privacy protocols is a worrying sign.

CYBER POLICE STATION[32]

Cyber police stations generally include trained personnel as well as the appropriate equipment to analyze and track digital crimes. Maharashtra , where cybercrime has risen over 140% in recent times, and which had the dismal distinction of only recording a single conviction related to cybercrime last year, is converting its existing cybercrime labs into cyber police stations. This will mean there is a cyber police station in each district of the state. The initiative in Maharashtra is useful especially because of the rise in online transactions in Tier II and Tier III cities and the rising cybercrime related thereto. However, despite the rise in cybercrime, complaints remain of low reportage and low success rates in solving crime. Police officers point to problems processing evidence, with complex procedures being required to retrieve data on servers stored abroad.

Further, there have been complaints in Bengaluru of the limited jurisdiction of cyber police stations. Pursuant to a standing order of the DG & IGP of Bengaluru City Police issued in June 2016, only cases with damages of over INR 5 lakh can be registered at cyber police stations in case of bank card fraud. In cases of online cheating, only those instances where damages exceed INR 50 lakh are amenable to the jurisdiction of cyber police stations. All other cases are to be registered with the local police

32 https://ccgnludelhi.wordpress.com/2017/03/24/law-enforcement-initiatives-towards-tackling-cyber-crime-in-india/

station which, unlike cyber police stations do not generally include trained personnel or the appropriate equipment to analyze and track digital crimes. While the order is undoubtedly creating problems for cybercrime victims, it was made taking into account the woefully under resourced cybercrime police station in Bengaluru which, at the time, consisted of a 15-member staff with two vehicles at its disposal.

Centre plans setting up of Cyber Warrior Police Force to tackle internet-related crimes[33]

The government has decided to set up a Cyber Warrior Police Force (CWPF) to tackle internet-related crimes such as cyber threats, child pornography and online stalking. The CWPF is likely to operate under the National Information Security Policy and Guidelines wing of the Union home ministry's Cyber and Information Security (CIS) division, which was created last November. It is proposed to be raised on the lines of the Central Armed Police Force.The other two wings under the CIS division are cyber crime and internal security. It's a policy decision, and the process has already begun. The Army is also planning to do something on similar lines. So far, there has been no decision on the CWPF's jurisdiction, where it will derive its powers or personnel from, and whether it would be empowered to make arrests. Meanwhile, the CIS division has already begun operations. The home ministry has already issued a communique asking states and Union territories to consider setting up state as well as district cyber crime coordination cells.

The Centre has suggested that state cyber crime coordination cells be headed by an additional director general or inspector-rank official, and district cyber cells by a deputy superintendent of police or additional superintendent of police-level official. State cyber security cells could likely form the foundation of the centralized CWPF. Both Prime Minister Narendra Modi and home minister Rajnath Singh had recently asked state police and paramilitary forces to lay special focus on cyber crime at the recently held annual director general-level conference in Takenpur, Madhya Pradesh. The home ministry also asked states to set up systems that will monitor "deep web activities" that enable the "planning and execution of nefarious deals by criminals". It has further instructed them to maintain

33 https://www.hindustantimes.com/india-news/centre-plans-setting-up-of-cyber-warrior-police-force-to-tackle-internet-related-crimes/story-1t9ehppjiHZVac7b3NgRKN.html

a list of suspected profiles linked with child pornography rackets, human trafficking and blackmailing; set up basic forensic labs; and focus on "capacity building". The home ministry has released Rs 82.9 crore to states under the Crime Prevention against Women and Children scheme for setting up cyber forensic training labs-cum- centers.

A. WHY POLICE IS FACING PROBLEM[34]

The major reason why police is facing problem lies in a sense of confusion as to whose jurisdiction the case will come under. For ex , it came into notice of a school teacher that an amount equal to Rs. 30000 was withdrawn from his savings account without his without his consent and knowledge. The ATM from which the amount was withdrawn located outside the city limits and some was withdrawn from the one located outside the state limits. In such situations, the complainant is troubled as to which jurisdiction, he should file the complaint to. Although, Section 75 of the Information Technology Act has provision for the extra-territorial operations of this law, but it makes sense only when backed with provision which recognize orders and warrants for information issued by competent authorities outside their jurisdiction and strategic measure which provides the cooperation to exchange material and evidence of computer crimes between law enforcement agencies.

The law regulating cyberspace in India has been enacted, but it lacks any operational manual of how to conduct an investigation relating to cybercrimes. A Standard Operating Procedure (SOP) is required to prevent ambiguity. With the arrival of cyber cells at various cosmopolitan cities in India, a need to build high technology crime and investigation infrastructure with highly technical staff has arisen. The current staff of cyber cells contains a mixture of police officers and IT experts. While additional recruitment is important, the main focus should be to improve the overall technical capabilities of the police staff rather focusing just on cyber cells.

Following are the gadgets without which police feels handicapped while carrying out any investigation[35] :

1. High capacity data transfer tools
2. Software's designed for analysis of phones

34 https://lawnn.com/article-cybercrime-menace-india/

35 https://www.hindustantimes.com/india-news/centre-plans-setting-up-of-cyber-warrior-police-force-to-tackle-internet-related-crimes/story-1t9ehppjiHZVac7b3NgRKN.html

3. Tools for recovering passwords using brute force, etc.
4. Assistance of Forensic science laboratories is also required which is scarce at the district level.

Consequences which have to be faced due to non availability of gadgets is that police heavily lean towards oral evidence, instead of focusing on circumstantial and scientific evidence.

Although government has taken this issue into account in the recent times. Maharashtra government gives the perfect example of this. It has planned to tackle the issue of cyber crimes by deploying 1000 police officers as cyber investigators. Moreover, statements/FIRS/police records are not fed to the computer to maintain a database because there is no network and personnel also are not trained in the specific department. FIRS/statements should be made online to reduce burden on police.

B. SUGGESTIONS AND MEASURES TO BE TAKEN TO REDUCE THIS PROBLEM[36]

- Specialized procedures along with expertise manpower are required to tackle cybercrime cases with excellence. Stringent punishment for cyber criminals has to be ensured so that it acts as a deterrent for others. Presently, the offenses which come under the Information Technology Act are bailable with imprisonment of 3 years. This should be increased to such an extent which would change the current mindset of a cyber criminal. Separate bench is required to be formed to fast track the cyber crime cases. The constitution of cyber judges has helped the law enforcement agencies to prove the merits of their cases without any hindrance.
- Similar to U.S. secret service or the FBI, which provides training to law enforcement officials on topics like cybercrime forensics, CBI can also start to conduct such kind of programs. The methods of the CBI can help police to closely supervise investigation of important cases by senior officers so that the investigating officer and Superintendents of police can get legal advice.
- Projects mentioned below have still not been implemented successfully by the Indian government, and these need to be implemented as soon as possible. These are:
  1. National Cyber Coordination Centre of India (NCCC).

36 https://lawnn.com/article-cybercrime-menace-india/

2. Cyber Attacks Crisis Management Plan of India.
3. Internet Spy System Network and Traffic Analysis System of India (NETRA).
4. Crime and Criminal Tracking Network and Systems Project of India (CCTNS).

- Cyber Crime can only be effectively countered when there is proper guidance and coordination available from various stakeholders like government, state and central government and local police. To facilitate the effective implementation of the initiatives taken, various adequately tasked and staffed agencies working at various levels should be executed. Indian Computer Emergency Response Team (CERT-In) is the national nodal agency set up to respond to computer security incidents as and when they occur. The activities which undertaken by CERT-In toward cyber security include the following:
  1. Coordination of responses to security incidents
  2. Timely advice regarding imminent threats
  3. Conduct training on specialized topics of cyber security
  4. Development of security guidelines on major technology platforms.
- There should be e-filing of FIRS to reduce the burden on victims to physically move to the police station.
- Process re engineering is required to replace the procedure of a complainant going to the police station with single emergency response interface which will help to bring the police to the doorstep of the victim.
- Centralized online cybercrime reporting mechanism in India is required that alert authorities of suspected criminal or civil violations.
- For law enforcement agencies at the local, state and national level, there should be a central referral mechanism for complaints involving cybercrime.
- There are many cases in which private corporations have more experience with cybercrime investigation than local police in those cases police can seek help with these corporations. E.g. In U.S. a privately led Identity Ecosystem steering group (IDES) has been established to support the National Strategy for Trusted Identities in Cyberspace (NSTIC).
- Various police departments have formed partnerships with computer science departments at local universities. Apart from providing expertise to the police, it also serves as a recruiting tool for students who have interest in cybercrime and policing. Thereby, a knowledge hub can be created.

CYBER SECURITY AGENCIES [37]

Internet Democracy, an initiative by the NGO Point of View, has released an interactive map of Indian Government's cyber security institutions. It provides a clearer picture of the hierarchy of the cyber security agencies under the Government. We have listed some of the most important agencies that are involved in cyber surveillance or dealing with cyber crime.
Institutes focusing on national cyber security:

1. The New Media Wing (NMW) and the Electronic Media Monitoring Centre (EMMC) come under the Ministry of Information and Broadcasting (MIB) and are involved in media surveillance. The EMMC reports breaking news aired on networks to the National Security Advisor and the Principal Secretary to the PM. The NMW tracks the internet, including micro blogs etc., to government relevant trends and gauge public opinions.

   Most of the institutes under the Ministry of Home Affairs (MHA) also fall in this category. The National Intelligence Grid (NATGRID) which keeps all sorts of citizen data in a single database that can be accessed by officers from RAW, CBI, IB etc., comes under the MHA. The National Cyber Coordination Center (NCCC) and the National Crime Records Bureau (NCRB) also come under this ministry.

   Other than this, the Home Affairs Ministry directly controls the Intelligence Bureau (IB), the National Investigation Agency (NIA), the Central Bureau of Investigation (CBI) and the Narcotics Control Bureau (NCB). All institutes under the MHA are in charge of internal security in some capacity. The NCB and IB are exempted under RTI.

   The Ministry of Communication and Information Technology controls CERT-In, the Indian Computer Emergency Response Team that performs emergency cyber security functions and releases annual reports of security incidents. The proposed

37 https://www.medianama.com/2016/04/223-indias-cyber-security-agencies/

National Media Analytics Centre (NMAC) and Digital Swachhata Kendra (DSK) will also come under the MCIT. NMAC will monitor and analyze content on the internet and counter negative content while DSK will look to deal with malware and botnets.

2. Department of Electronics and Information Technology (DEITY): Operating under the MCIT, DEITY is responsible for ensuring cyberspace security, other than delivering government services online and promoting the IT sector. It is directly responsible for institutes like UIDAI which operates the Aadhaar database, to NIXI, the National Internet Exchange of India.

3. Prime Minister's Office (PMO): Institutions under the PMO have a wide range of responsibilities from dealing with cybercrime, incident response, global internet and governance. Directly controlled institutions include:

   National Security Council (NSC) which directly controls the National Security Council Secretariat (NSCS), Strategic Policy Group (SPG) and National Security Advisory Board (NSAB)

   The Cabinet Committee on Security (CCS) through which decisions like the formation of a new body, or response after an attack, have to go through and the Research and Analysis Wing (RAW) which is responsible for international intelligence collection.

   The PMO administratively controls the National Technical Research Organisation (NTRO), which is directly responsible for the National Institute of Cryptology Research and Development as well as the National Critical Information Infrastructure Protection Centre.

4. Ministry of Finance (MoF): The Central Economic Intelligence Bureau (CEIB) operates under MoF. It directly controls various intelligence agencies that deal with economic offences.

Institutes which focus on external cyber security:

1. The Defence Intelligence Agency (DIA) operates under direct control of Ministry of Defence (MOD). MOD also administratively controls Defence Research and Development Organization (DRDO) and the Institute of Defence Studies and Analysis. These institute focus on international level offensive and defensive capabilities of the nation.

2. Global Cyber Issues Cell operates under the direct control of the Ministry of External Affairs (MEA). This cell tracks the international processes that affect national policy making.

Policy

The National Information Board (NIB), a policy making body for cyber security, operates independently and is chaired by the National Security Advisor. Established in 2002, it deals with issues related to surveillance and cyber crime.

Comparison of India with other countries on the basis of cyber law , crime and it services

This blog is about a small comparison between developing countries like India and developed countries like USA and China . India is developing day by day in every sector but in IT and cyber sectors it is far back than other developed countries like USA and China .In developed countries awareness and knowledge among the people regarding cyber and IT law is much better than the developing countries. People are more aware regarding their rights and privacy in developed countries . Most of the countries have the separate rules , regulations and laws which maintain n deals with the cyber sectors of the country which provides a security to the citizens of that country . India also has a separate act called IT Act which was amended in 2008 last time which was come into force in the year 2000 first time. But this act not that sufficient that it can manage the IT and cyber sectors of India properly . It is like a coin which has two faces; good as well as bad.

IT act (amended)2008 provides many reliefs regarding cyber crimes to the common people of India because of which common people are now safe from different types of crimes like voyeurism which is mentioned under section 66 E of IT act and section 345C of the IPC 1860 also provides same ; one of these crimes is hacking mentioned under section 43 of IT act and some others are cyber terrorism , identity theft etc. But in developed countries there are so many advanced laws and acts are imposed for the security of cyber users like in China and USA there are some special acts for the individuals.

In developed countries like China and USA the new Cyber security law is too tight and brings restrictions to foreign companies doing business

in the countries which protects the countries and controls the cyber crime rates . On the other hand India also making many efforts to make the country efficient to provide better services and protection in cyber sector. In 2013 , government of India introduced a National Cyber Security Policy with the aim of protecting information infrastructure, reducing vulnerability , increasing capabilities and safeguarding it from cyber attacks . India is now on the way to make the IT act more efficient which needs some more amendments which can be possibly done in near future and our country will also compete the foreign developed countries in cyber and IT protection sector.

CONCLUSION

To sum up, though a crime free society is perfect and exists only in illusion, it should be constant attempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even Dos or DDos) are all technologies and per se not crimes, but falling into the wrong hands with an illicit intent who are out to exploit them or misuse them, they come into the array of cyber-crime and become punishable offences. Hence, it should be the tenacious efforts of rulers and law makers to ensure that technology grows in a healthy manner and is used for legal and ethical business growth and not for committing crimes.

It should be the duty of the three stake holders viz. i) the rulers, regulators, law makers and agents ii) Internet or Network Service Suppliers or banks and other intercessors and iii) the users to take care of information security playing their respective role within the permitted limitations and ensuring obedience with the law of the land.

Pairvi

Public Advocacy Initiatives for Rights and Values in India

E-46, Upper Ground Floor, Lajpat Nagar-III, New Delhi-110024

Phone: +91-11-29841266, 65151897 | e-mail: pairvidelhi1@gmail.com

website: www.pairvi.org