CYBER CRIME AND CYBER LAW'S OF INDIA

Written by *Udit Malik* & Rahesha Sehgal***

**3rd Year Cadet, National Cadet Corps, India*

***3rd Year Student, Delhi University*

Abstract - *As we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. The internet technology has been using by the few people for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime related to the internet is termed as cyber crime. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, encompassing many subtopics as well as freedom of expressions, access to and utilization of the Internet, and online security or online privacy. Generically, it is alluded as the law of the web.*

Key Words: **Internet, Unauthorized access, Cyber crime, Cyber law, Cyberspace, Punish, Network**

1. INTRODUCTION

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or

computer network and are usually take place over the cyber space especially the Internet. Now comes the term "Cyber Law". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model.

2. OBJECTIVE

The principle target of our paper is to spread the knowledge of the crimes or offences that take place through the internet or the cyberspace, along with the laws that are imposed against those crimes and criminals. We are additionally trying to focus on the safety in cyberspace.

3. CYBER CRIME AND CYBER LAW

We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved.

We can define "Cyber law" as the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world.

3.1 Cyber Crime

Sussman and Heuston first proposed the term "Cyber Crime" in the year 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or

conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high-technology crime, information age crime etc.

In simple term we can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal.

The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

3.1.1 History of Cyber Crime

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future.

3.1.2 Evolution of Cyber Crime

The cyber crime is evolved from Morris Worm to the ransomware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

Cyber Crime can be classified into four major categories.

They are as follows:

a) **Cyber Crime against individuals**: Crimes that are committed by the cyber criminals against an individual or a person. A few cyber crime against individuals are:

b) **Email spoofing**: This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.

c) **Spamming**: Email spam which is otherwise called as junk email. It is unsought mass message sent through email. The uses of spam have become popular in the mid 1990s and it is a problem faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated programs that crawls the internet in search of email addresses. The spammers use spam bots to create email distribution lists. With the expectation of receiving a few number of respond a spammer typically sends an email to millions of email addresses.

d) **Cyber defamation**: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.

e) **IRC Crime (Internet Relay Chat)**: IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other.

Online threatening etc. Intellectual property crime includes:

- **Software piracy**: It can be describes as the copying of software unauthorizedly.
- **Copyright infringement**: It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials unauthorizedly such as music, software, text etc.
- **Trademark infringement**: It can be described as the using of a service mark or trademark unauthorizedly.

- **Cyber Crime against organization**: Cyber Crimes against organization are as follows:
    - Unauthorized changing or deleting of data.
    - Reading or copying of confidential information unauthorizedly, but the data are neither being change nor deleted.
- **DOS attack**: In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them.
    - **Email bombing**: It is a type of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow or flood the mailbox with mails or to flood the server where the email address is.
    - **Salami attack**: The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's information like bank details, credit card details etc. Attacker deduces very little amounts from every account over a period of time. In this attack, no complaint is file and the hackers remain free from detection as the clients remain unaware of the slicing.

Some other cybercrimes against organization includes-Logical bomb, Torjan horse, Data diddling etc.

3.1.4 Safety in cyberspace

List are some points, one should keep in mind while surfing the internet:

- If possible always use a strong password and enable 2 steps or Two-step authentication in the webmail. It is very important in order to make your webmail or your social media account secured.

Guideline of strong password:

a) Password should be of minimum eight characters.
b) One or more than one of lower case letter, upper case letter, number, and symbol should be included.
c) Replace the alike character.

Example- instead of O we can use 0, instead of lower case l we can use I etc.

Example of strong password: HelL0 (%there %); Thing need to avoid while setting the password:

- Never use a simple password that can easily be decrypt Example- password
- Personal information should never set as a password.
- Repeating characters should be avoided. Example- aaaacc
- Using of same password in multiple sites should be avoided.

What is 2 step or Two-step authentication?

This is an additional layer of security that requires your user name and the password also a verification code that is sent via SMS to the registered phone number. A hacker may crack your password but without the temporary and unique verification code should not be able to access your account.

- Never share your password to anyone.
- Never send or share any personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail.

Websites that doesn't have the lock icon and https on the address bar of the browser are the unencrypted site.

The "s" stands for secure and it indicates that the website is secure.

- Don't sign to any social networking site until and unless one is not old enough.
- Don't forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided.
- Don't respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.

- Try to avoid pop-ups: Pop-ups sometimes comes with malicious software. When we accept or follow the pop-ups a download is performed in the background and that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may contain the malicious code.

3.1.5 Cyber Crime's scenario in India (A Few Case study)

a) The Bank NSP Case

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

b) Bazee.com case

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold- out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.

c) Parliament Attack Case

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry

into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

Andhra Pradesh Tax Case

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

f) SONY.SAMBANDH.COM CASE

India saw its 1st cybercrime conviction. This is the case where Sony India Private Limited filed a complaint that runs a website referred to as www.sony-sambandh.com targeting the NRIs. The website allows NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the involved recipients. In May 2002, somebody logged onto the web site underneath the identity of Barbara Campa and ordered a Sony colour television set and a cordless head phone. She requested to deliver the product to Arif Azim in Noida and gave the number of her credit card for payment. The payment was accordingly cleared by the credit card agency and the transaction processed. After the related procedures of dues diligence and checking, the items were delivered to Arif Azim by the company. When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized

transaction as the real owner had denied having made the purchase. The company had filed a complaint for online cheating at the CBI that registered a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code). Arif Azim was arrested after the matter was investigated. Investigations discovered that Arif Azim, whereas acting at a call centre in Noida did gain access to the number of the credit card of an American national which he misused on the company's site. The CBI recovered the color television along with the cordless head phone. In this matter, the CBI had proof to prove their case so the accused admitted his guilt. The court had convicted Arif Azim under the Section 418, Section 419 and Section 420 of the IPC, this being the first time that a cybercrime has been convicted. The court, felt that since the defendant was a boy of 24 years and a first-time convict, a compassionate view needed to be taken. Thus, the court discharged the defendant on the probation for one year.

3.2 2 CYBER LAW

Cyber Law took birth in order to take control over the crimes committed through the internet or the cyberspace or through the uses of computer resources.

Description of the lawful issues that are related to the uses of communication or computer technology can be termed as Cyber Law.

3.2.1 What is the importance of Cyber Law?

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views.

3.2.2 Cyber Law awareness program

Once should have the following knowledge in order to stay aware about the cyber crime:

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.

- Read cyber crime's cases. By reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime.

3.2.3 The Information Technology Act of India, 2000

According to Wikipedia "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), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes 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".

Some key points of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company.

3.2.4 Cyber Law in India

Following are the sections under IT Act, 2000

1. **Section 65- Temping with the computers source documents**

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment:

Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

2. Section 66- Hacking with computer system, data alteration etc

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment:

Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.

Section 66A- Sending offensive messages through any communication services

- Any information or message sent through any communication services this is offensive or has threatening characters.
- Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.
- Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.

Punishment:

Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine.

4. Section 66B- Receiving stolen computer's resources or communication devices dishonestly

Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment:

Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

5. Section 66C- Identify theft

Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment:

Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

CONCLUSIONS

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. The Act further revise the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber crime could be originated passing national boundaries over the internet creating both technical and legal

complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to take action towards the cyber crimes.

Our main purpose of writing this paper is to spread the content of cyber crime among the common people. At the end of this paper "A brief study on Cyber Crime and Cyber Law's of India" we want to say cyber crimes can never be acknowledged. If anyone falls in the prey of cyber attack, please come forward and register a case in your nearest police station. If the criminals won't get punishment for their deed, they will never stop.