Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(11s):63-70

Research Article ISSN: 2394 - 658X

A Short Study of Cyber Crime and Cyber Law's in India

Neeraj Singh Yadav[1], Dr Kaushal Kumar[2]

[1]Research Scholar, Raffles University Neemrana
[2]Associate Professor, Rao Sohan Lal College Neemrana
neerajkumar318@gmail.com, kaushalyadav54@yahoo.com
Received: 30/07/2023; Accepted 25/08/2023; Published 25/10/2023

ABSTRACT

As you know, this is an era when most things, from online commerce to online transactions, are usually done through the internet. The Web is viewed as a global arena, allowing anyone, anywhere to access Internet resources. Internet technology is used by very few people for criminal activities such as unauthorized access to other people's networks and fraudulent activities. These criminal activities or crimes/offenses related to the Internet are known as cybercrime. The term "cyber law" was introduced to stop and punish cybercriminals. Cyberlaw can be defined as the part of the legal system that deals with the Internet, cyberspace, and legal matters. It covers a wide area and includes many sub-topics such as freedom of expression, internet access and use, online safety and online privacy, etc. These are commonly referred to as the Laws of the Internet. . We may define "cybercrime" as a criminal or other criminal activity involving any electronic communication or information system, including any device and/or the Internet, or combination of both.

Key words: : Internet, unauthorized access, cybercrime, cyberlaw, cyberspace, punishment, network.

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 [1]. 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 [2]. 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 [3]. 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 [4].

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.

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 [5].

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 [6].

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.

There is a myth among the people that cyber crimes can only be committed over the cyberspace or the internet. In fact cyber crimes can also be committed without ones involvement in the cyber space, it is not necessary that the cyber criminal should remain present online. Software privacy can be taken as an example.

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 [7].

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.

Table-1 Evolution of Cyber Crime

Years	Types of Attacks
1997	Cyber crimes and viruses initiated, thatincludes Morris Code worm and other.
2004	Malicious code, Torjan, Advancedworm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack,Cyber warfare etc.

Classifications of Cyber Crime

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:

• 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 [8].

• **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.

• **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 [9]. The purpose of making defamatory statement is to bring down the reputation of the individual.

• **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.

- Cyber Criminals basically uses it for meeting.
- Hacker uses it for discussing their techniques.
- Paedophiles use it to allure small children. A few reasons behind IRC Crime:
- Chat to win ones confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts threatening to upload victim's nude photographs or video on the internet.
- A few are paedophiles, they harass children for their own benefits.
- A few uses IRC by offering fake jobs and sometime fake lottery and earns money [10].

• **Phishing:** In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity in various communication channels or in email.

Some other cyber crimes against individuals includes- Net extortion, Hacking, Indecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc. The potential harm of such a malefaction to an individual person can scarcely be bigger.

b) Cyber Crime against property: These types of crimes includes vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes,
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.

c) 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 [11].
- 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 cyber crimes against organization includes- Logical bomb, Torjan horse, Data diddling etc.

d) Cyber Crime against society: Cyber Crime against society includes:

- Forgery: Forgery means making of false document, signature, currency, revenue stamp etc.
- Web jacking: The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page. These types of attacks are done to get entrance or to get access and controls the site of another. The attacker may also change the information of the victim's webpage.

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 you webmail or your social media account secured.

Guideline of strong password:

- Password should be of minimum eight characters.
- One or more than one of lower case letter, upper case letter, number, and symbol should be included.
- 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 tha 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 .

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.

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 [13].

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.

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" [14].

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 [15].

Cyber Law in India

Following are the sections under IT Act, 2000

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.

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 [16].

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.

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.

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.

Section 66D- Cheating by personation by the use of computer's resources

Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

Section 66E- Privacy or violation

Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

Section 66F- Cyber terrorism

Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people by-

- Deny to any people to access computer's resources.
- Attempting to break in or access a computer resource without any authorization or to exceed authorized access.
- Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavorably affect the critical information's infrastructure specified under the section 70 of the IT Act.

By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of our country India.

Punishment:

Whoever conspires or commits such cyber crime or cyber terrorism shall be sentenced to life time imprisonment.

Section 67- Transmitting or publishing obscene materials in electronic form

Whoever transmits or publishes or cause to publish any obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend upto five years of imprisonment along with a fine which may extend upto 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend upto ten years along with a fine that may perhaps extend to two lakhs rupees.

Section 67A- Transmitting or publishing of materials that contains sexually explicit contents, acts etc in electronics form

Whoever transmits or publishes materials that contains sexually explicit contents or acts shall be sentences for either description for a term which may extend upto 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees in the first convict. And in the event of the second convict criminal could be sentenced for

either description for a term that could extend upto 7 years of imprisonment along with a fine that may extend upto 20 lakhs rupees.

Section 67B- Transmitting or publishing of materials that depicts children in sexually explicit act etc in electronics form

Whoever transmits or publishes any materials that depict children in sexually explicit act or conduct in any electronics form shall be sentenced for either description for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees 10 lakhs on the first conviction. And in the event of second conviction criminals could be sentenced for either description for a term that could extend to 7 years along with a fine that could extend to rupees 10 lakhs.

Section 67C- Retention and preservation of information by intermediaries

- Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the Central Government may prescribe.
- Any intermediaries knowingly or intentionally contravene the provision of the sub-section.

Punishment:

Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

Section 69- Power to issue direction for monitor, decryption or interception of any information through computer's resources

Where the Central government's or State government's authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of our country India, state's security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section (II). For reasons to be recorded writing, direct any agency of the appropriate government, by order, decrypt or monitor or cause to be intercept any information that is generated or received or transmitted or is stored in any computer's resources.

The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carried out, shall be such as may be prescribed.

The intermediaries, the subscribers or any individual who is in the charge of the computer's resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access or access to computer's resources receiving, transmitting, generating or to store such information or
b) Decrypting, intercepting or monitoring the information, as the case might be or
c) Providing information that is stored in computer.

The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section (III), shall be sentenced for a term that could extend to 7 years of imprisonment and also could be legally responsible to fine [17].

There are many other sections in the IT Act, 2000 among them a few important sections one should know are as follows:

Table-2: A few important sections one should know

Offences	Sec. under IT Act, 2000
Damage to Computer, ComputerSystem etc.	Section 43
Power to issue direction for blocking from public access of any information through any computer's resources.	Section 69A
Power to authorize to collect traffic information or data and to monitor through any computer's resources for cyber security.	Section 69B
Un-authorized access toprotected system.	Section 70
Penalty for misrepresentation.	Section 71
Breach of confidentiality andprivacy.	Section 72
Publishing False digitalsignature certificates.	Section 73
Publication for fraudulentpurpose.	Section 74

Act to apply for contraventionor offence that is committedoutside India.	Section 75
Compensation, confiscation orpenalties for not to interfere with other punishment.	Section 77
Compounding of Offences.	Section 77A
Offences by Companies.	Section 85
Sending threatening messagesby e-mail.	Section 503 IPC
Sending defamatory messagesby e-mail.	Section 499 IPC
Bogus websites, Cyber Frauds.	Section 420 IPC
E-mail Spoofing.	Section 463 IPC
Web Jacking.	Section 383 IPC
E-mail Abuse.	Section 500 IPC
Criminal intimidation byanonymous communications.	Section 507 IPC
Online sale of Drugs.	NDPS Act
Online sale of Arms	Arm Act

CONCLUSIONS

The rise 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.

ACKNOWLEDGEMENT

We express our sincere gratitude and thanks to Mr. Amlan Jyoti Baruah (Assistant Professor, Computer Science and Engineering) of The Assam Kaziranga University for his valuable guidance, and support and kind co-operation during preparation of this paper and helping us in writing this review paper successfully.

REFERENCES

[1]. www.tigweb.org/action-tools/projects/download/4926.doc
[2]. https://www.tutorialspoint.com/information_security_ cyber_law/introduction.htm
[3]. https://www.slideshare.net/bharadwajchetan/an- introduction-to-cyber-law-it-act-2000-india
[4]. https://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW
[5]. https://cybercrime.org.za/definition
[6]. https://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws
[7]. https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf