A STUDY ON THE CYBER CRIMES COMMITTED IN INDIA AND THE CYBER LAWS

Mohammad Istekhar
Research Scholar
Department of Computer Science
Sunrise University
alam2611985@gmail.com

Dr. Amit Jain
Research Guide
Department of Computer Science
Sunrise University

Abstract *-As is common knowledge, most activities in this day and agefrom online business to online transactions are conducted over the internet. Anyone can access internet materials from anywhere since the web is thought of as a global stage. A small number of individuals have been leveraging internet technology for illegal activities including frauds and unauthorized access to other people's networks. Cybercrime is the word used to describe these illicit actions or the offense/crime connected to the internet. The phrase "Cyber Law" was first used to describe measures taken to deter or punish online crimes. Cyber law may be characterized as the area of the legal framework that deals with the Internet, cyberspace, and legal matters. It includes a wide range of subjects, including freedom of speech, access to and use of the Internet, as well as online safety or privacy. It is often referred to as the web's governing law.*

Key Words*: Cybercrime, Cyberspace, Cyber law, Internet*

INTRODUCTION

The creation of the computer has improved human lives; it is being used for a variety of global purposes by both small and big companies. Computers may be simply defined as devices that can store, modify, and carry out user-inputted information or instructions. Since decades, the majority of computer users have been misusing the technology for either their own or other people's profit [1]. As a result, "Cyber Crime" was born. This has caused people to indulge in socially unacceptable behaviour. Cybercrime is defined as a kind of criminal activity that often takes place online, particularly on the Internet, and involves the use of computers or computer networks [2]. The phrase "Cyber Law" is now used. Although it has no set definition, we may sum it up by saying that it is the law that controls the internet. Laws governing the cyberspace are known as cyber laws. The Cyber Law encompasses cybercrimes, digital and electronic signatures, data safeguards and privacy, among other things [3]. The first Information Technology Act of India was suggested by the UN General Assembly and was based on the "United Nations Model Law on Electronic Commerce" Model [4].

CYBER CRIME AND CYBER LAW

Any criminal activity or other offences involving electronic communications, information systems, including any device or the Internet, both of them, or both and more, are referred to as "cybercrimes" [5]. "Cyber law" may be defined as the legal concerns associated with the use of communications technology, namely "cyberspace," which is the Internet. The goal is to reconcile the difficulties posed by online behaviour with the established legal framework that governs the real world [6].

Cyber Crime

In 1995, Sussman and Heuston initially suggested the phrase "cybercrime." Cybercrime is best understood as a group of activities or conducts; there is no one term that adequately captures it. These

actions are based on the tangible offence item that has an impact on computer systems or data. These are illicit activities when a digital device or information system is a tool, a target, or both. Other names for cybercrime include electronic crime, crime involving computers, e-crime, high-tech crime, information age crime, etc.

Cybercrime, to put it simply, is any offence or crime committed through electronic communications or information networks. These sorts of crimes are essentially any unlawful actions that involve a computer or network. The amount of cybercrime activities is growing as a result of internet growth since it is no longer necessary for the criminal to be physically present to conduct a crime.

The peculiar aspect of cybercrime is that it's possible for the victim and the perpetrator to never have a face-to-face encounter. In order to decrease the likelihood of being discovered and prosecuted, cybercriminals often choose to operate from nations with nonexistent or lax cybercrime legislation.

There is a misconception that cybercrimes may only be done online or in cyberspace. In truth, committing a cybercrime doesn't need being present online; it may be done without one being involved in the internet world. You may use software privacy as an example.

History of Cyber Crime

Cybercrime began in 1820. Charles Babbage's analytical engine was the first modern computer, however Japan, China, and India had primitive computers from 3500 B.C. Joseph-Marie Jacquard invented the loom in 1820. This equipment made weaving specific textiles or materials continuous. This caused Jacquard's employees to fear for their jobs and livelihoods and try to prevent the company from using the new technology [7].

Evolution of Cyber Crime

Morris Worm was the first cyber-attack, and ransom ware is the next evolution. While many nations, including India, are attempting to put an end to these crimes or assaults, they are always evolving and have an impact on our country.

Table-1: Evolution of Cyber Crime

Year	Types of Attacks
1997	Cybercrimes and viruses initiated, that inclu other
2004	Identifying thief, Phishing etc
2007	DNS Attack, Rise of Botnets, SQLattack
2010	Social Engineering, DOS Attack, BotN Ransomware attack etc.
2013	Social Engineering, DOS Attack,BotNets, Emails,Ransomwareattacketc.
Present	Banking Malware, Keylogger, Bitcoin walle hack, Cyber warfare etc.

Classifications of Cyber Crime

Cyber Crime can be classified into four major categories. They are as follows:

- **Cyber Crime against individuals:**crimes that are perpetrated against a person or a person by cybercriminals. Among the cybercrimes committed against people:
- **Email spoofing**: This tactic impersonates an email header. This indicates that the communication looks to have come from a different source than the real or authentic one. These strategies are often used in phishing or spam operations because consumers are more likely to open an email or electronic message when they believe it has been issued from a reliable source [8].
- **Cyber defamation:**Cyberdefamation is the term used to describe the damage done to a

person's reputation in the eyes of other people through the internet [9]. Making false statements has the intention of damaging a person's reputation.

- **Phishing:**Through these types of crimes or fraud, the perpetrators pretend to be a reliable person or Organisation in different communication channels or via email in an effort to get information such as login credentials or account information.

Other online crimes committed against people include credit card fraud, net extortion, hacking, indecent exposure, trafficking, distribution, posting, and malicious code. There is hardly any other damage that such a malefaction to an individual could possibly do.

❖ **Software piracy:** It can be describes as the copying of software unauthorized.

❖ **Trademark infringement:**It may be characterized as the unlawful use of a service mark or trademark.

- **Cyber Crime against organization:** Cyber Crimes against organization are as follows:

Unauthorized changing or deleting of data

Unauthorized reading or copying of private information that is neither changed nor erased.

➢ **DOS attack:** The goal of this assault is to overload the victim's resources and make it impossible or challenging for the users to utilize them by flooding the servers, systems, or networks with traffic. [11].

➢ **Email bombing:**Huge volumes of emails are sent to an email address in an effort to overwhelm or flood the mailbox with messages or the server that hosts the email address. This is an example of net abuse.

➢ **Salami attack:**Salami slicing is another term for salami attack. In this assault, the perpetrators steal consumer information, including bank and credit card information, using an internet database. Over time, the attacker takes extremely little sums from each account. In this assault, no complaints are made, and the hackers escape discovery since the customers are unaware that they are being sliced.

Logical bombs, Torjan horses, data manipulation, and other cybercrimes against organizations are only a few examples.

Cyber Crime against society: Cyber Crime against society includes:

➢ **Forgery:** Forgery means making of false document, signature, currency, revenue stamp etc.

➢ **Web jacking:**Hi-jacking is the root of the word "web jacking." When the victim clicks on the link to the phoney website created by the attacker, a new page with the message appears, prompting them to click another link. The victim will be sent to a false website if he clicks on the link that seems authentic. These kinds of assaults are carried out to get access to another person's property or to gain entry and take control. The victim's website's information may potentially be altered by the attacker.

Safety in cyberspace

Following is a list of things to consider during online browsing:

Use a strong password whenever you can, and activate two-step authentication or 2FA in webmail. Making sure that your social networking or webmail accounts are safe is crucial.

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: Thing need to avoid while setting the password:

• Avoid using weak passwords that are easy to crack. Instance: password

• A password should never include personal information.

• Character repetition should be avoided. Instance: aaaacc

• It's best to avoid using the same password across several websites.

What is two-step authentication?

• Your user name, password, and a verification code that is provided by SMS to the registered phone number are all required for this extra layer of protection. Even if a hacker manages to guess your password, they won't be able to access your account without the temporary and distinctive verification code.

• Keep your password private at all times.

• Never transmit or disclose any personal information, including your bank account number, ATM pin, password, or email address, over an unencrypted connection. Unencrypted websites are those that lack the lock symbol and https in the browser's address bar. The website is secure if it has a "s" after it, which stands for secure.

• If you are not of legal age, wait to join up for any social networking site.

• Be sure to keep your operating system updated.

• One should install and maintain anti-virus, anti-spyware, and firewall software on their computer.

• It is best to avoid visiting unreliable websites or clicking on links sent to you by unknown or suspect websites.

• Avoid retweeting spam.

• Ensure that sensitive data is encrypted before putting it in the cloud.

• Try to avoid pop-up windows since they sometimes contain harmful software. When we click on or accept the pop-ups, a background download is initiated that includes malware or other hazardous software. Drive-by download is the term used for this. Avoid clicking on pop-ups that offer site surveys on e-commerce websites or other similar websites since they can be infected with malware.

Cyber Crime's scenario in India

Parliament Attack Case

This case was handled by the Bureau of Police Research and Development, Hyderabad. The terrorist who assaulted the Parliament had a laptop that was found. The laptop that belonged to the two terrorists who were shot dead on December 13, 2001, when the Parliament was under siege, was taken into custody and handed to the BPRD's Computer Forensics Division.

The laptop contained several pieces of evidence that supported the two terrorists' goals, most notably the fake ID card that one of the two terrorists was carrying and the sticker of the Ministry of Home that they had created on the laptop and placed on their ambassador car to gain entry into Parliament. The three lions' symbols were meticulously scanned, and a seal with Jammu and Kashmir's residence address was also skillfully made. But close examination revealed that everything was fake and created on the laptop.

The Bank NSP Case

In this instance, a bank management trainee became engaged to be married. Using the company's computers, the pair used to send and receive a lot of emails. After some time, they separated, and the

young woman sent emails to the boy's international customers using fictitious email addresses like "Indian bar associations." She accomplished this using the bank's computer. The boy's business lost a tonne of customers and sued the bank. The emails sent utilizing the bank's technology were held accountable by the bank.

Cyber Pornography

Pornography is the biggest online industry, even though some governments restrict it. IT Act Sections 67, 64A, and 67B apply to such offences.

CYBER LAW

Cyber Law was created to regulate cybercrime.

Cyber law describes legal concerns using communication or computer technology.

What is the importance of Cyber Law?

In this modern technological era, cyber law is very significant. It is significant because it affects practically all elements of activities and transactions that happen online or via other forms of communication. Whether we realize it or not, every action and every response taken in cyberspace is subject to certain legal and ethical standards [13].

Cyber Law awareness program

• In order to be informed about cybercrime, one needs be knowledgeable about the following:

• The cyber legislation should be carefully studied.

• A working understanding of internet security.

• Read about instances of cybercrime. One may learn about such crimes by reading about such instances.

• Sensitive information or data may be protected by using a trustworthy application from a trusted website.

• The effect of technology on crime.

The Information Technology Act of India, 2000

The Information Technology Act, 2000, sometimes referred to as ITA-2000 or the IT Act, is an act of the Indian Parliament (No. 21 of 2000), which was announced on October 17, 2000, according to Wikipedia. It is the most significant legislation in India that addresses internet commerce, cybercrime, and other forms of digital crime. Based on a decision passed by the United Nations General Assembly on January 30, 1997, the UNCITRAL Model Law on Electronic Commerce from 1996 serves as its foundation [14].

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

• The Act now recognizes electronic mail as a legitimate means of communication, and it gives legal standing to digital signatures.

• The Act has spawned new economic opportunities for organizations that want to issue digital certificates by acting as Certifying Authorities.

• This Act permits e-governance, which enables the government to publish notifications online, as well as internet communication between businesses or between businesses and the government.

• The primary goal of this Act is to address the problem of security. • In case of any injury or loss done to the firm by criminals, the Act gives a remedy in the form of money to the company [15].

• It created the concept of digital signatures that certifies a person's identification of an individual on the internet.

Cyber Law in India

Following are the sections under IT Act, 2000

Section 65- Temping with the computers

source documents

Anyone alters the source code for any computer utilized in a computer, computer programme, computer system, or computer network with the purpose to do so.

Punishment:

Anyone who participates in such activities faces a term of up to 3 years in jail, a fine of Rs. 2 lakh, or both.

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

Whoever intends to harm another person's computer, cause loss or damage, or delete, change, or otherwise dispose of any information that is stored there. Hacking is any action that reduces the value, diminishes its usefulness, or negatively impacts it.

Punishment:

Any individual involved in such offences faces a penalty of up to 3 years in jail, a fine of up to 2 lakh rupees, or both [16].

Section 66A- Sending offensive messages through any communication services

• Any information that is false or invalid and is provided with the objective of disturbing, inconveniencing, danger, insult, obstruction, harm, criminal intention, animosity, hate, or ill will;

• Any information that is offensive or contains threatening characteristics.

• Any electronic mail or email sent with the intent to irritate, trouble, deceive, or mislead the recipient regarding the source of the contents.

Punishment:

Any person found guilty of such offences under this provision faces a maximum penalty of three years in jail and a fine.

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

Receiving or holding onto a computer, its resources, or any communication equipment that has been taken with knowledge or suspicion of having been stolen.

Punishment:

Any individual who participates in such activities may get a sentence of up to three years in jail, a fine of one lakh rupees, or both.

Section 66C- Identify theft

It is illegal to use someone else's password, digital or electronic signature, or any other kind of unique identification.

Punishment:

Any individual who participates in such activities may get a sentence of up to three years in jail and/or a fine of up to one lakh rupees.

Section 66D: Personation-based cheating via the use of computer resources

Anyone who attempts to defraud someone by impersonating another person using communication devices or computer resources may be punished to up to three years in jail and/or a fine of up to one lakh rupees.

Section 66E- Privacy or violation

Any person who violates another person's privacy by knowingly or intentionally publishing, sending, or taking pictures of their private spaces or private parts without that person's agreement faces a three-year jail term, a fine of up to two lakh rupees, or both.

Section 66F- Cyber terrorism

Those who purposefully put integrity, unity, sovereignty, or security in jeopardy or cause dread among the general public or any portion of the general public via -

I. Prevent anybody from using the resources of the computer.

II. Making an attempt to gain unauthorized access to, break into, or use a computer resource.

III. Introducing any computer

contaminant, and through such conducts causes or is probable to cause any death or injury to any individual, damage to any property, or destruction of any property, or disrupts or it is known that by such conduct it is probable to cause damage to the infrastructure for critical information as specified in section 70 of the IT Act, or poses a threat to such infrastructure.

By doing things like this, one can gain access to data, information, or computer databases that are restricted or limited for a variety of reasons related to the security of the state or of other countries, or to any restricted database, data, or information with the reason to believe that those data, information, or the computer's resources are in some way, shape, or form, not authorized.

Punishment:

Anyone who participates in a conspiracy or engages in such cybercrime or cyberterrorism will get a life sentence.

Section 67- Transmitting or publishing obscene materials in electronic form

Those who transmit, publish, or encourage the publication of any pornographic content in electronic form. Any content that is vulgar or appealing to be lubricious, or if it has the effect of, for example, tending to corrupt any person who is likely, taking into account all relevant circumstances, to read, see, or hear the matter that is contained in it, shall be sentenced on the first convict with either description for a term that may extend up to five years of imprisonment along with a fine that may extend up to one lakh rupees, and on the second or subsequent convict it can be sent

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

Anyone who distributes or publishes anything that involves explicit sexual content or activities faces a punishment of up to 5 years in prison or 10 lakh rupees in fines and/or additional years in jail for the first offender. And in the case of a second conviction, the offender might get a sentence for any classification that included up to 7 years in jail and a fine of up to 20 lakh rupees.

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

On the first offence, anybody found guilty of transmitting or publishing any materials that show youngsters engaging in sexually explicit behaviour may face a punishment that could include up to five years in jail and a fine of Rs. 10 lakh. And in the case of a second conviction, offenders might get a sentence for each category that could last up to 7 years and a fine up to Rs. 10 lakh.

Section 67C- Retention and preservation of information by intermediaries

The Central Government may stipulate the length of time, format, and method in which information must be retained and preserved by intermediaries.

Any middlemen who deliberately or knowingly violate the sub-clause. section's

Punishment:

Any person who commits one of these offences faces a term of up to three years in jail as well as a fine.

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

When the authorized officers of the Central or State governments, as applicable, determine that doing so is

necessary or advantageous for maintaining the integrity or sovereignty, the security of India, the security of the state, or friendly relations with other nations, or for preventing any incident that might lead to the commission of any cognizable offences related to the foregoing, or for investigating any offences that are subject to the p (II). Direct any agency of the relevant government, by order, to decrypt, monitor, or cause to be intercepted any information that is created, received, transferred, or stored in any computer's resources, for reasons that will be documented in writing.

I. I. Any decryption, monitoring, or interception that is done must follow the safeguards and procedures that may be mandated.

II. II. Any agency referred to in subparagraph (I) may contact intermediaries, subscribers, or any person in control of the computer's resources, who offer all services and technical help to:

VI. The failure to assist the agency referred to in sub-section (III) by intermediaries, subscribers, or any other person will result in a penalty of up to 7 years in jail as well as the possibility of a fine [17].There are several additional parts in the IT Act, 2000.

4. CONCLUSIONS

The emergence and spread of newly created cybercrimes. The IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934 are all further revised by the Act. Cybercrime may begin from anywhere in the globe and spread across national borders through the internet, making it difficult to investigate and prosecute these crimes on both a technological and legal level. To combat cybercrimes, worldwide harmonization efforts, coordination, and cooperation amongst diverse states are necessary.

Our primary goal in producing this essay was to inform the general public about cybercrime. This paper concludes by stating that cybercrimes would never be accepted. Please come forward and file a report at the closest police station if you or someone you know becomes the target of a cyber-attack. The criminals will never cease if they don't get punished for their actions.

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] http://www.academia.edu/7781826/IMPACT OF SOCIAL MEDIA ON SOCIETY and CYBER LAW

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

[7]https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

[8] http://searchsecurity.techtarget.com/definition/email- spoofing

[9] http://www.helplinelaw.com/employment-criminal-and-labour/CDII/cyber-defamation-in-india.html

[10] http://ccasociety.com/what-is-irc-crime/

[11]http://searchsecurity.techtarget.com/definition/denial- of-service

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

[13] http://www.cyberlawsindia.net/cyber-india.htmltechnologies begin star to operate many cybercrimes in recent years. The Government of India has enacted IT Act, 2000 to deal with https://en.wikipedia.org/wiki/Information_Technolo gy_Act,_2000

[14]https://www.ijarcsse.com/docs/papers/Volume_5/8_ August2015/V5I8-0156.pdf

https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/https://indiankanoon.org/doc/1439440/

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

[16]

http://www.lawyersclubindia.com/articles/*Classification-Of-Cyber Crimes1484.asp*