A HYPOTHETICAL ALALYSIS OF CYBER CRIME AND IT'S IMPACT

Sarthak Sampad Roy[1], Mainak Pal[2], Anirban Bhar[3], Suchismita Maiti[4]

[1,2] *B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[3]*Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[4]*Associate Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*

ABSTRACT

Today's cybercrime has harmed many people, businesses, and even the government. Methods for detecting and categorizing cybercrime have been developed, with various degrees of success for preventing and safeguarding data from such attacks. Cybercriminals are subject to sanctions under a number of laws and measures that have been put in place to prevent it. As is common knowledge, most activities in this day and age—from online business to online transactions—are conducted via the internet. Anyone can access internet materials from anywhere since the web is thought of as a global stage. A small number of people have been leveraging internet technology for illegal activities like frauds and unauthorized access to other people's networks. Cybercrime is the term 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 can 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 generally referred to as the web's governing law.

Keyword: - *Cyber Crime, Cyber Law, Cyber Space, Unauthorized Access.*

---

1. INTRODUCTION

The creation of the computer has improved human lives; it is being used for a variety of global purposes by both small and large companies. Computers can be simply defined as devices that can store, manipulate, 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 had caused people to indulge in socially unacceptable behavior. Cybercrime is defined as a type of criminal activity that typically 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 protections 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" (UNCITRAL) Model [4].

Crime is defined as [5] a criminal conduct that carries a state-imposed penalty. However, there is no formal definition given for some reasons. Other names for crime include offence and criminal offence. It is destructive to the community or the state as well as to some specific individuals. [6] The enforcement of the law has nothing to do with cybercrime. The term "cyber" is a prefix used to identify a person, object, or idea as being in the computer and information age, according to the authors of [7]. Computers or computer networks are involved [8]. A computer network is essentially a group of interconnected nodes that facilitates data flow. Computers, laptops, smartphones, and other nodes could all be considered nodes at any one time. [8] Cybercrime includes all illegal activities involving networks and computers. [9] It involves criminal activity committed online. The Internet is essentially a network of networks used for data sharing and communication. The use of a tool for illicit purposes, such as [9] perpetrating fraud, trafficking in child pornography and

stolen intellectual property, stealing identities, or violating privacy, is known as cybercrime, also known as computer crime. The development of Internet technologies like the 2G and 3G has made it possible for the global village to share and communicate important data across the network in an efficient manner. However, some people deliberately attempt to seek down and illegally obtain sensitive information for their own use, financial gain, and a variety of other reasons.

2. CYBER CRIME

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 "cyber crimes".

"Cyber law" can 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 behavior with the established legal framework that governs the real world.

In 1995, Sussman and Heuston initially suggested the phrase "cyber crime." Cybercrime is best understood as a group of acts or conducts; there is no single 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 either 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 types of crimes are essentially any unlawful actions that involve a computer or network. The volume of cybercrime activities is growing as a result of internet development because 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 frequently 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 require being present online; it can be done without one being involved in the internet world. You may use software privacy as an illustration.

3. EVOLUTION OF CYBER CRIME

Within the year 1820, the first cybercrime was noted. Japan, China, and India have had primitive computers since 3500 B.C., but Charles Babbage's analytical engine is regarded as the beginning of modern computers. A French textile manufacturer by the name of Joseph-Marie Jacquard invented the loom in the year 1820. The weaving of unique fabrics or materials was made possible by this instrument through a series of ongoing steps. Due to their extreme fear that both their livelihoods and their established jobs were in danger, the Jacquard employees chose to damage the company in order to deter them from using the new technology in the future.

From Morris Worm to ransomware, cybercrime has progressed. While efforts are being made to curb these crimes and attacks by many nations, including India, these attacks are evolving and have an impact on our country.

In India, although there had been some cybercrime before to that in the late 1980s, the growth of email coincided with the first significant spike in cybercrime. It has made it simple to send your inbox a variety of scams and/or malware.

The subsequent wave in the history of cybercrime emerged in the 1990s as a result of developments in web browser technology. There were considerably more users available back then than there are now, and the majority of them were susceptible to infections. Virens were transmitted via Internet connections whenever questionable websites were browsed.

Cybercrime began to seriously take off in the early 2000s as social media started to take off. The rush of people dumping all the information they could into a profile folder led to an influx of personal data and the rise of ID fraud. The data was utilized by thieves to open bank accounts, create credit cards, and commit other types of financial theft.

The creation of an annual, multi-national criminal organization with a value of close to half a trillion dollars is the new wave. These criminals operate in groups, employ tried-and-true strategies, and target everyone with a digital presence.

4. CLASSIFICATION OF CYBER CRIME

There are four main categories into which cybercrime can be divided:

4.1 Cybercrimes against individuals

Crimes done by online criminals against a person or an individual or a person are classified as:

Email spoofing: This tactic involves fabricating an email header. This indicates that the communication doesn't seem to have come from the real or authentic source, but rather from someone else or someplace else. Because consumers are likely to open an email or electronic mail when they believe it has been provided by a reliable source, these techniques are frequently employed in spam campaigns and phishing.

Spamming: Email spam, also known as junk email, is considered to be spam. Email was used to send the unwanted bulk communication. Most email users today deal with the issue of spam because it first gained popularity in the middle of the 1990s. Spam bots are automated programmes that scour the internet for email addresses and collect recipients' email addresses. To establish email distribution lists, spammers utilize spam bots. Spammers often send emails to millions of addresses with the hope of getting a small number of responses.

Cyber defamation: The harm done to a person's reputation in the eyes of other people through the internet is referred to as cyberdefamation. It is intended to damage a person's reputation by making defamatory statements.

IRC crime (Internet Relay Chat): IRC servers let users from all over the world congregate in one area, also referred to as a room, where they may communicate with one another.

- It is primarily used for meetings by cybercriminals.
- Hackers use it to discuss their methodologies.
- To entice young children, pedophiles utilize it.

Phishing: Through these types of crimes or fraud, the perpetrators pretend to be a reliable person or organization in various 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 harm that such a malefaction to an individual could possibly cause.

4.2 Cybercrimes against property

Computer vandalism, crimes involving intellectual property (such as Copyright, patents, trademarks etc.), and cyberthreats are some examples of these crimes. crimes involving intellectual property include:

- **Software piracy:** The unauthorized copying of software is known as software piracy.
- **Copyright infringement:** Infringements on a person's or an organization's copyright are referred to as copyright infringements. It can also be summed up simply as the unauthorized use of copyright materials like music, software, writing, etc.
- **Trademark infringement:** Using a service mark or trademark without authorization is known as trademark infringement.

4.3 Cybercrimes against property

The following list of cybercrimes against organizations:

- Unauthorized reading or copying of private information, unauthorized changing or deleting of data.
- Reading or copying of confidential information unauthorizedly, but the data are neither being change nor deleted.
- The purpose of a denial-of-service (DoS) assault is to overwhelm the victim's resources and make it impossible or challenging for users to utilize them by flooding the victim's servers, systems, or networks with traffic.
- Email bombing is a form of online abuse in which a large volume of emails is sent to a single address to overwhelm the mailbox, flood the server hosting the address, or both.
- Salami assault is often referred to as "salami slicing." In this attack, the perpetrators steal consumer information, including bank and credit card information, using an internet database. Over time, the attacker takes extremely small amounts from each account. In this assault, no complaints are made, and the hackers escape discovery because 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.

4.4 Cybercrimes against society

Cyber Crime against society includes:

- **Forgery:** Forgery is the creation of a fake document, signature, piece of money, revenue stamp, etc.

- **Web jacking:** Hi-jacking is a phrase that has been used to describe 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 page if he clicks on the link that appears authentic. These kinds of attacks 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.

5. STUDY ON CYBER CRIMINALS

Cyber criminals range from a wide variety of age groups:
Kids (age group 9-16): It may be difficult to believe, but children can also engage in cybercrime, whether consciously or unknowingly. Teenagers make up the majority of inexperienced hackers. Being able to hack into a computer system or a website seems to be a source of pride for these kids. They could also carry out the offences without being aware that they are breaking the law.
Organized Hacktivists: Hacktivists are a collective of hackers who share a common goal. These organisations mostly pursue political goals. While in other instances, they might be motivated by social activism, religious activism, or something else entirely.
Disgruntled Employees: It is difficult to fathom how bitter disgruntled employees might turn. To date, these disgruntled workers have had the option of going on strike against their bosses. Disgruntled employees can now cause a lot more harm to their companies by committing crimes using computers, which can bring their entire system to a halt, thanks to the growing reliance on computers and the automation of procedures.
Professional Hackers: Information is now stored in electronic form in commercial organizations as a result of extensive computerization. Rival organizations hire hackers to steal additional commercial secrets and information that could be useful to them. It is seen redundant to require physical presence to gain access if hacking can retrieve the relevant information from competitors' businesses. This increases the incentive for businesses to employ skilled hackers to perform their dirty work.

6. INDIAN CASE STUDY

Recently, there have been several cybercrimes reported in India. Here are some examples of these:

CASE 1: In April 2014, two undergraduate students, Vivek Kumar alias Kishan Dubey and Anand Mishra, were detained for engaging in internet fraud in Allahabad, India. These two students committed credit card theft of Rs. 1.20 lakhs INR after obtaining the ATM password of a man by the name of Mahmood. After being detained, the students admitted to some of their frauds. The two students would supply Delhi-based addresses for the delivery of items they had ordered online, according to the Police. When the goods arrived, they would sell them to duplicitous customers. This case had been filed in accordance with sections 419 and 420 of the IPC Act and section 66 of the IT Act.

CASE 2: In the context of cyberstalking, police in Hyderabad detained a young man from Bangalore named N Santosh Kumar alias Kiran in 2013 after he was accused of constructing a false Facebook profile for a woman. Additionally, after the woman declined his romantic proposal, the young man threatened her. Dejected, he created a phony profile and started chatting with others using her name. Additionally, he called and texted the victim's relatives with threats. The perpetrator was taken into custody after the victim's brother filed a complaint with the Cyber Crime Police in August 2013.

CASE 3: Email is at issue in this case. One of the Global Trust Bank's branch offices has recently struggled due to spoofing. Many clients abruptly made the decision to withdraw their funds and further cancel their individual bank accounts. Investigation revealed that someone had sent these customers and other recipients fraudulent emails claiming the bank would soon be shut down due to financial difficulties.

CASE 4: This case involves an E-mail bombing (Denial of Service) and involves a foreign national who spent over thirty years living in Simla, India. He wished to take advantage of a plan put up by the Simla Housing Board to purchase land for less money. His application, however, was rejected since they stated that the programme is only for Indian citizens. This man decided to strike back in response. He then bombarded the Simla Housing Board with hundreds of emails, sending them nonstop until their email systems broke.

7. CONCLUSIONS

According to the findings of this study, there are numerous different channels via which one can conduct crimes online. Cybercrimes are offences that carry legal repercussions. We have seen a quick description of the expanding domains of cybercrime in section 4. It can be easily understandable that how cybercrime has devastating financial repercussions for many nations, particularly in the trade and investment sectors. For this type of offence, various fines and penalties have been set down. The various online crimes involving electronic mail are covered in Section 3 as well. These crimes include email bombing, mail spoofing, and the distribution of malicious software through emails. Additionally, we have observed a variety of cybercriminals, from novice teenage hackers to experienced hackers who are frequently hired by competing firms to break into another company's system. Therefore, it is crucial that everyone is aware of these crimes and vigilant at all times to prevent any loss. The judiciary has developed various laws known as "Cyber Laws" in order to secure justice for the victims and punish the offenders. Therefore, it is advisable for everyone to be aware of these rules. Additionally, the issue of cybercrime cannot be reduced to a technological one. Instead, it is an approach-based issue because it is people, not computers, who are injuring and assaulting businesses. People are using technology to their own advantage to do evil. Therefore, it is up to us to be vigilant and identify the many strategies that these crooks may employ. To recognize situations that could result in such harm, one must have an intellectual attitude. Such crimes cannot be solved solely through technological means. Technologies may only be one tool in the arsenal used to disrupt and, to some extent, stop such actions.

7. 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
[5]. en.wikipedia.org/wiki/Crime
[6] David Wall, “Cyber crimes and Internet”, Crime and the Internet, by David S. Wall. ISBN 0-203-164504 ISBN 0-203-164504, Page no.1
[7] searchsoa.techtarget.com/definition/cyber
[8] www.merriamwebster.com/dictionary/cyber
[9] Bela Bonita Chatterjee, “Last of the rainmacs? Thinking about pornography in cyber space”, Crime and the Internet, by David S. Wall. ISBN 0-203-164504, Page no.- 74.