THE SCANDALOUS ASPECT OF THE DIGITAL WORLD: CYBER CRIME

Kashish Khanna IILM University, Gurugram, Haryana

I. ABSTRACT

The advancement of information technology has brought along its own boons and banes. Cybercrimes are evil scandals which have emerged after the advancement of the IT Sector in India and abroad. Beginning in the 1970s, telephone connections were frequently used by criminals to perpetrate crimes. These criminals were known as Phreakers. In reality, cybercrime didn't really exist until the 1980s. To search, copy, or change personal data and information, one person had access to another person's computer. Lan Murphy Captain Zap, was the first person to be convicted of a cybercrime, and this occurred in 1981.He had manipulated the American telephone company's internal clock through hacking in order to allow users to make free calls during busy hours.[1]On the other hand, in today's scenario it is a huge income generating crime. People try to make easy money out of such crimes. But why is so much attention given on Cyber-Crimes these days, there are various other crimes as well? What are they? Who commits such crimes? And what is the impact of cyber-attacks on our country and abroad? What is the implementation status of the Cyber Laws in India? How any people are affected? The answers to all these questions shall be given by the end of the research paper and the concept of cyber-crime shall appear clear and simple.

Keywords: Cyber-crimes, Phreakers, advancement, technology, income, hacking, data.

[1] Nidhi Narnolia, Cyber Crime In India; An Overview, Legal Services India, https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html, Lat Accessed on 18th June,2023 - 4:03 PM

II. RESEARCH METHODOLOGY

Doctrinal research is the methodology that will be used for this study. Glimpses of comparative research shall also be observable. Comparative research is used when there is involvement of situational or objective comparison. Published books, journals, scholarly articles, online journals, research reports, and others will be employed as secondary sources of data for the purpose of this research. The scope of research is analyzing laws on cybercrime and incidents (experiences). If the paper is subject to any limitation, with regards to scope, it shall be due to time and geographical constraints.

III. INTRODUCTION

Any person who commits an act punishable by the law comes under the category of a criminal and any person who commits a cyber-crime comes under the sub category of a cyber- criminal.[2] Anyone could be a cybercriminal; an unhappy employee, a child, a teenager, a professional hacker etc.

The criminal activities of gaining unauthorized access to computer systems are known as cybercrime. They pose a threat economically, politically and even socially in any society. Such crimes do not involve any violence and thus are sometimes called 'White Collar Crimes'.[3] They affect 500 million people all over the Internet. New forms and developed criminals activities enter cyberspace with advancing technologies. These crimes could take place against against a particular person, a business, or a property or even the government.

Businesses can be directly affected by them. Sensitive customer data may get leaked which may result that business to get sued and shut down later due to its failure to protect the data of its customers. A single attack costs an average of $200,000 loss to affected companies. Such crimes not just lead to financial loss but also accompany loss of reputation, trust, social standing in the society.[4]

The foundation of network and information security is cyber security. To protect data from data breaches, several strategies are used in cyber security. Cybersecurity is becoming more

[2] Ashish Pandey, Cyber Crimes Detention and Prevention,2006, Pg.3.1
[3] Ranbir Singh, Ghanshyam Singh, Cyber Space and The Law,2015, Pg.1
[4] What is Cyber-crime? , Kaspersky, https://www.kaspersky.com/resource-centre/threats/what-is-cybercrime Last Accessed on 18th June 2023 – 4:37 PM.

and more important as businesses go online to protect data from harmful activity.[5]

Similarly, the effect of cybercrimes on the defence and the government may also prove very hazardous.

The working of cyber criminals is pretty simple. Such crimes can start wherever there is digital data, opportunity and motive. They use malware and various other softwares. The causes of such a crime could be a money deprived person, a job deprived person, one who wishes to seek revenge etc.

Cybercrime is distinct from other types of crime that take place in society. The reason is because it has no geographical limits and that no one knows who the cybercriminals are.[6] varied countries may have varied rules and regulations regarding cybercrime, and like with real crimes, it is far simpler to hide your tracks when conducting a cybercrime.

Cyber-crimes bring along various challenges with them for the governments worldwide. Some of them could be; Critical Infrastructure Vulnerability, Under-Preparedness, Limited Private Sector Participation, Added Complexity etc.[7]

Various cybercrimes like hacking, phishing, cyberstalking, cyberbullying, cybersquatting were registered in India every day in the year 2020 (136 per day approximately) according to the National Crime Records Bureau.[8]

These crimes have increased four times that is three hundred and six percent in the past four years in India. An average of two thousand cyber-crimes occurs globally every day. These numbers are alarming.

Cyber-crimes could be prevented by not sharing sensitive information online or on social media, by enforcing a concrete security setup and maintenance thereof, by using anti-virus softwares and various other similar measures. Online courses offer guidance on how to avoid, safeguard against, and recover from cybercrime risks.

[5] What is Cyber –Crime? , Intellipat, https://intellipaat.com/blog/what-is-cybercrime/, Last Accessed on 18th June 2023 – 4: 45 PM.
[6] Supra note 2.
[7] Rising Up to Cyber Security Challenges, Drishti IAS, https://www.drishtiias.com/daily-updates/daily-news-editorials/rising-up-to-cyber-security-challenges Last Accessed on 18th June 2023 – 4:32 PM.
[8] Cyber Crimes, Getastra ,https://www.getastra.com, Last Accessed on 18th June 2023 – 5:09 PM.

The numbers of the workforce dealing with cyber-crimes in cyber cells has been increased. But, this does not give a permanent solution to the problem. A permanent solution shall involve better implementation of laws and treaties and preventing the emergence of any new cyber-criminal along with the spread of awareness in common people and reaching out to the masses so that they stay alert and don't fall prey to such frauds.

IV. POTENTIAL CYBER CRIMINALS

The categorization done below is regardless of physical, geographical or social barriers.

1. Children Between 6-18 years of age: This category indulges into the world of cyber-crime mostly because of uncontrolled curiosity and eagerness. They might wish to stand out from others of their age group.

2. Revenge seekers: People who experience the fire inside them lighting up against somebody, wish to seek revenge, may go to the extent of committing a cyber crime against the person they are revengeful of.

3. Psychopaths: Sadist psychopaths are those who would feel pleasure seeing other people to lose on their assets and might also tend to involve in the commission of a cyber crime just for mental satisfaction.

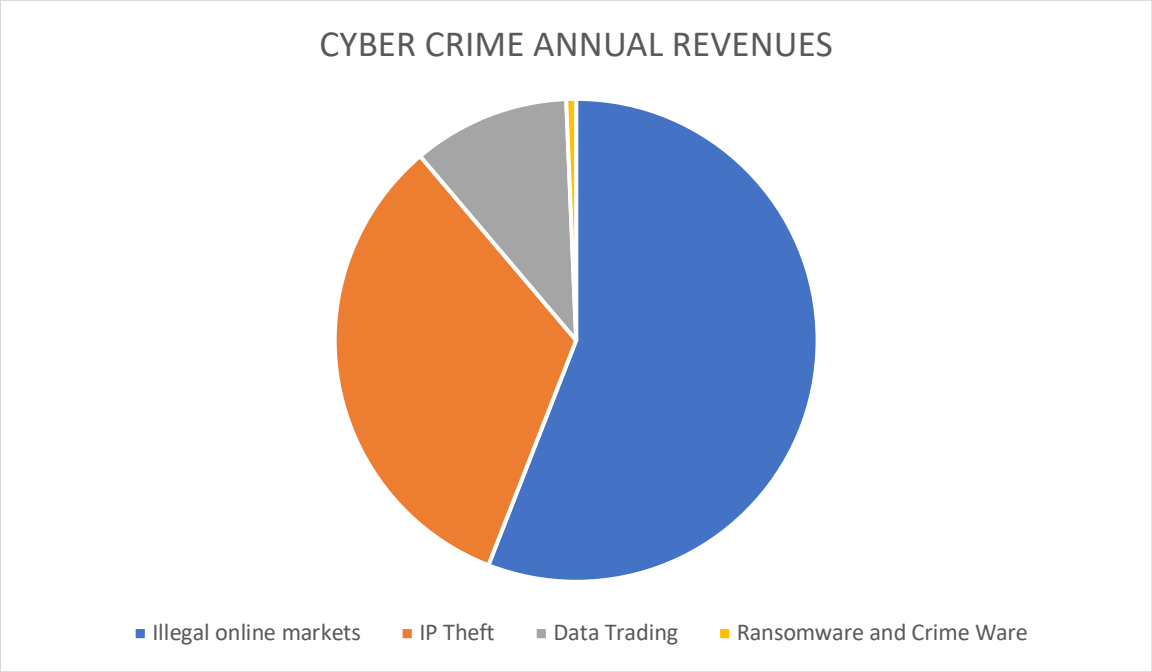
4. Unsatisfied Employees: To seek financial support through hacking or to avenge from their employer, they might commit a cyber-crime.[9]

5. People who want easy money: Many people would indulge in cyber crimes to make money easily.

These categories were meant to show how vastly can the backgrounds a various cyber criminals differ.

[9] Ashish Pandey, Cyber Crimes; Prevention and Detention,2006, Pg.3.1-3.2

V. REVENUE GENERATION FROM CYBER CRIMES



Areas Of Crimes	**Revenue (In Billion Dollars)**
Illegal Online Markets	**$850**
IP Theft	**$500**
Data Trading	**$160**[10]
Ransomware and Cybercrimeware	**$10**

VI. VARIOUS CYBER CRIMES IN THE INFORMATION ERA

1. Hacking: It has been defined in S.66 Of the Information Technology Act. Hackers could be wizards, dark side hackers, crackers, cyberpunks or traditional hackers. It implies taking unauthorized access of someone else's devices.

2. IP Spoofing: It happens when a hacker from outside the network poses as a reliable machine. It occurs when an IP address is used.

[10] Statistics Of Cyber Crime, SSL Store, https://www.thesslstore.com/blog/2018-cybercrime-statistics/, Last Accessed on 20th June 2023.

3. Frauds: People with fraudulent intention act to be reliable and credible. Innumerable scams and frauds take place. It is the most common type of crime.

4. Phishing: Phishing (pronounced as "fishing") is an attack that tries to steal your money or your identity by tricking you into disclosing personal information on websites that look official but are actually fake, such as credit card numbers, bank information, or passwords.

VII. CYBER LAWS; IMPLEMENTATION AND IMPORTANCE

The Information Technology Act,2000 encompasses policing online transactions and protecting private information. A few important provisions are:

- Unauthorized access: Section 43 of The Information Technology Act, talks about the illegality of trespassing someone's data privacy on his computer.
- Bodily Privacy: According to S.66E, if one transits someone else's image of his private area without his consent, then such a person violates the privacy of the other. He may be subject to three years in jail and a fine up to 2 lakh Indian rupees or both.
- Tampering of Computer Source: According to S.65, the privacy of a person will be disrespected if the computer source documents are interfered with.[11]
- The Servers of Banks and other virtual platforms via which the Banks provide us with E-Banking Services are specifically mentioned in Section 3(2) of the Information and Technology Act, 2000, as a method of verifying the records.
- In addition, Section 4 of the Information and Technology Act of 2000 states that any requirement pertaining to the security and privacy of a customer's information that is in writing or in a typewritten or printed form shall be deemed to have been satisfied as true, if such information is rendered and certified in an electronic form and is usable for the subsequent references.[12]

SEBI has suggested some guidelines in the year 2000, for brokers offering security trading services by using WAP (Wireless Application Protocol).[13]

[11] G.P. Sahoo, New Legal Dimensions of Cyber Crime, 2017, Pg. 149-150
[12] Major Issues in Indian Banking System, IP Leaders, https://blog.ipleaders.in/major-legal-issues-indian-e-banking-system/ Last Accessed on 22nd June 2023.
[13] Rodney D. Ryder, Guide to Cyber Laws,2000, Pg.33

The Data Protection Bill 2022's goal is to "ensure that digital personal data is processed in a way that recognizes both the right of individuals to protect their personal data and the necessity of processing personal data for lawful purposes."

Implementation of cyber laws is of primary importance in India. Cyber-crimes have become a major threat today. This has happened due to poor implementation and lack of adequate resources with the Indian government to implement these laws in India. None of the laws gave a legal sanction to the essential activities in cyber space. For instance, the vast majority of people utilize the Internet for email. Email, however, has not yet taken off in our nation. There is no law in the nation that recognizes email as legitimate or sanctioned. In our country, courts and the judges have been hesitant to uphold the legitimacy of email because no explicit legislation has been passed by the Parliament. As a result, cyber laws are now necessary. In the case of **Shreya Singhal VS Union of India:**[14]

- Two ladies were detained by the police without any warrant as said under Section 66A. for reportedly making inappropriate and disrespectful remarks on Facebook over the morality of closing Mumbai following the passing of a political leader.
- The information was sent through a computer resource or communication device with the intent to cause annoyance, inconvenience, danger, insult, injury, hatred, or ill will. The information was false and was sent with knowledge of its falsity, according to Section 66A of the Information Technology Act of 2000 (ITA), under which the police made the arrests.
- Although the women were eventually freed by the police, who dropped their charges, the incident received a lot of media attention and backlash.
- The ladies then submitted a petition, arguing that Section 66A is unconstitutional since it interferes with their freedom of expression.
- In Singhal v. Union of India, the Supreme Court of India first ordered an interim measure that forbade any arrest made in accordance with Section 66A unless it was authorized by top police authorities. The Court reviewed the legality of the clause in the current case.[15]

[14] (2013) 12 S.C.C. 73

[15] Shreya Singhal VS Union of India, Columbia, https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/ Last Accessed on 4th July 2023.

The major question was whether the right to freedom of expression protected by Article 19(1)(a) of the Indian Constitution was breached by Section 66A of the Indian Tax Act. The government may impose "reasonable restrictions. in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence" as an exception to the right, according to Article 19(2) of the Constitution.

The Hon'ble supreme court first held that such an arrest could now only be made after the permission of senior police officers.

As to petitioners' challenge of vagueness, the Court followed the U.S. judicial precedent, which holds that "where no reasonable standards are laid down to define guilt in a Section which creates an offense, and where no clear guidance is given to either law abiding citizens or to authorities and courts, a Section which creates an offense and which is vague must be struck down as being arbitrary and unreasonable." [para. 52] The Court found that Section 66A leaves many terms open-ended and undefined, therefore making the statute void for vagueness.

The section 66A of the Information Act, 2000 was completely invalidated by the two-judge panel of Justice Chelameshwar and Justice R.F. Nariman on the grounds that it contravenes the terms of Article 19, which guarantees the right to freedom of speech and expression.

Even after seven years of this judgement, the police officers, still arrest people on this ground. This depicts lack of proper implementation of laws in our country.

IX. SHOULD MORE EFFORTS BE DONE TO PROTECT PRIVACY RIGHTS GLOBALLY?

Whether the government should intervene and enact legislation to safeguard customers' rights to online privacy is one of the issues that both consumers and internet marketers are now grappling with. The Consumer Federation of America and the Electronic Privacy Information Centre are two organizations that were lobbying Congress to establish legislation to safeguard online privacy rights.

The American Electronics organization (AEA), has modified its antiregulatory attitude and announced "principles" for nations to take into account while drafting new Internet privacy laws.

According to AEA principles, there should be new regulations regulating e-commerce. Web

sites to tell users about the type of information being gathered and provide them the option to decline to provide it. The Information Technology Association of America and the Information Technology Industry Council, among other internet industry groups, continue to promote the self-regulation approach. The AEA's shift in position on regulation, however, shows a rising worry about the pressure being placed on state governments to control internet businesses. There is a concern that if the federal government does nothing to safeguard online privacy, different state laws may apply to internet marketers, which would hurt e-commerce. A variety of laws that deal with concerns related to internet privacy, consumers, were debated and now even certain groups inside the online sector are suspicious.[16]

X. International and National Incidents of Cyber Crime

1. How moral hackers seized control of her PC

The Daily Telegraph's Sophie is a technology reporter. She agreed to take part in an experiment on ethical hacking as part of a task. In essence, a team of moral hackers would attempt to attack her system without her knowledge of the where, when, or how. Sophie merely anticipated that it would occur eventually. The hackers conducted thorough research on Sophie for a whole month, poring over her Twitter and Facebook accounts, Daily Telegraph articles, and even learning her birthdate from a family tree website. Social-engineering-tactics. The hackers started their attack about two months after the experiment started. They sent her an email with some of the files attached while posing as whistleblowers in charge of private government data. The instant she opened the file, she became infected with malware, giving the attackers access to her webcam and email address among other things. And completing it wasn't even that challenging.[17]

2. Uber experiences a serious cyberattack

Service that shares rides Uber was allegedly the target of a social engineering assault on an employee by a young hacktivist in September, who apparently wanted the firm to pay its drivers more. This incident made headlines and made Uber one of 2022's high-profile cyber attack victims. Multiple Uber systems were interfered with during the event, for which the Lapsus$

[16] Roger LeRoy Miller, Gaylord A. Jentz, Law for E-Commerce, 2002, Pg. 247

[17] Stories That Wil Make You Care About Cyber Security, Heimdal Security, https://heimdalsecurity.com/blog/12-true-stories-that-will-make-you-care-about-cyber-security/, Last Accessed on 7th July 2023.

group was later held responsible.[18]

3. A Dog of Lakhs of Rupees

A little girl who requested her mom for a new puppy could have never anticipated the fate of her family post this demand. The puppy they wished to buy was supposed to be shipped from some other city. They had placed their demand online. The dealers asked them for advance payment of the puppy, which they made. Gradually, the dealers began to ask them for security payments which will be returned to them after the puppy is delivered. The sum reached to some lakh rupees. The puppy never reached them.

4. Fraudsters Never Age

This incident happened in Hyderabad in India. A girl aged 25 met a man on a social media platform who pretended to be of 27 years. They became good friends. The man asked her to lend some money, because he was in a big problem, to which the girl agreed and which he returned later. This happened once again. The third time, the man asked her for one lakh rupees and did not return them. Later when he was caught, it was found that he was 40 years old and had done the same fraud with various other people who became the victims to this cyber-crime.

5. In the largest-ever cyber fraud sweep, UK police make 120 arrests.

Due to the rarity of ransomware gangs attacking customers directly, digitally enabled fraud is undoubtedly the most common way for the typical individual to become a victim of cybercrime. In November 2022, the Metropolitan Police announced details of its involvement in a significant investigation that brought down a cybercriminal website and resulted in more than 100 arrests.[19]

6. AIIMS Cyber Attack

Lately, in India many cyber-attacks have been observed on the Indian health sector by hackers from China, Pakistan and Vietnam etc. A major example of this is the repeated cyber-attacks on All India Institute of Medical Research (AIIMS). The first attack was done on 23rd November 2022. 4.5 million cases were recorded as this point. A case of extortion and cyber terrorism was registered. All computer services got incapacitated. This news got everyone

[18] Top 10 Cyber Crime Stories, Computers Weekly, https://www.computerweekly.com/news/252528238/Top-10-cyber-crime-stories-of-2022 Last Accessed on 9th July 2023.
[19] Supra Note 18.

panicked. The second attack was done on June 2023. This was a little different from the previous one. Data could be secured this time.

XI. THE DILEMMA: Is it the Victim's fault too?

Yes, to some extent victims of cyber crimes are also at fault. In many cases they become a victim because They were careless, negligent and inconsiderate at many places before typing in their personal details even after hundreds of government advertisements spreading awareness about the same. The victims sometimes make the work of cyber criminals easier by trusting everything very easily and giving them their OTP's or Bank Account Passwords and other confidential information.

In this era, it has been observed that youngsters are more prone to cyber crime than the older adults due to them being more exposed to the world of Internet. Only 4.8% older adults (65-74 years old) are prone to such crime whereas all other major groups being at 6.5% in India.[20]The criminal is wrong by indulging in such crimes but such victims are even worse who promote cyber criminals by their carelessness.

XII. COMPARING CYBER CRIMES; India and Abroad

The US holds the top spot in the study, with 4,66,501 victims of cybercrime. The United Kingdom came in second with 3,03,949 casualties. 3,131 Indians were victims of cybercrime. Just 25,000 of these crimes occurred in all other nations save the top 5.

More than 70% organizations in countries like USA, UK, Saudi Arabia, China and Mexico were affected by ransomware attacks. Whereas, organizations in countries like Singapore, UK, Japan suffered up to 60% ransomware attacks. In India, 73% of the organizations have suffered cyber-attacks. The cyber crime revenue is estimated 23.8 trillion dollars in the year 2027.[21]

Russian-speaking cyber teams constitute a significant threat to UK interests, but domestic cybercriminals are also a growing menace due to their increased sophistication. Young offenders frequently choose peer approval above monetary gain, while structured UK cyber-

[20] Dr. Annie Kirby, Science direct, https://www.sciencedirect.com/science/article/abs/pii/S0267364921000881#:~:text=In%20terms%20of%20levels%20of,groups)%2C%20although%20this%20may%20be Last Accessed On 10th July 2023.
[21] Cost Of Cyber Crime, Statista, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/, Last Accessed on 11th July 2023.

crime teams are profit-driven.[22] Whereas, in this context, countries like Pakistan and China pose a threat to India.

XIII. UN Model Law on Digital Intricacies

UN adopted a model law in 2019 on digital intricacies (to be implemented). It also made it compulsory for each nation state to have its own laws on cyber-crimes.

Making it simpler for law enforcement to obtain data, including data outside of the country, where the law enforcement agencies seeking it are located, is a common goal of efforts to strengthen international cooperation against cybercrime. While accelerating cross-border access to data for criminal investigations may be necessary to ensure accountability, doing so frequently entails taking steps that circumvent or weaken due process safeguards or violate the right to privacy sometimes with the backing of influential businesses.[23]

The international treaty's drafting sessions are anticipated to last three years. The initial gathering happened in March 2022. A resolution on "countering the use of information and communications technologies for criminal purposes" was adopted by the UN General Assembly in December 2019, along with the creation of an Ad Hoc Committee. It was revealed that a committee will be formed to design an extensive international convention. working to design a fresh international cybercrime agreement.[24]

XIV. Conclusion

Due to increasing cases of cyber-crimes, it has become very important to curb such crimes. It is suggested that scope of existing law can be extended. The Ministry of Home Affairs has issued a Cyber Crime Advisory to State Governments and Union Territories. In order to detect, register, investigate, and prosecute cybercrime, the State Government is also encouraged to create strategies like cyber police stations, technical infrastructure, and trained personnel. Indian Computer Emergency Response Team (CERT-In) and the Centre for Development of Advanced Computing (CDAC) are offering advanced and fundamental training to Law Enforcement Agencies, forensic Labs, and the Judiciary regarding the procedures and methods

[22] Cyber Threats, National Crime Agency, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime, Last Accessed on 11th July 2023.
[23] Cybercrime new UN Treaty, HRW, https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights Last Accessed on 12th July 2023.
[24] A UN Treaty on Cybercrime en Route, United Nations Regional Information Centre for Western Europe https://unric.org/en/a-un-treaty-on-cybercrime-en-route/

to gather, analyze, and present digital evidence. Forensic Lab training has been established at the Central Bureau of Investigation (CBI) to provide training for Cyber Crime Police Officers. Arunachal Pradesh, Kerala, Assam, Mizoram, Nagaland, Tripura, Meghalaya, Manipur, and the government of Jammu and Kashmir has established forensic training labs. For the purpose of raising awareness of cybercrime, DSCI (Data Security Council of India) have been established in Mumbai, Bengaluru, Pune, and Kolkata. People should be made aware that they should use strong passwords and should not disclose any OTP to anyone. A meeting held on July 4th 2023 joined by representatives of several banks and Google, Paytm and Apple talked on Cyber security and rising cyber-crimes.[25]

To conclude, it can be said that judiciary combined with increased awareness in people can be efficient in cyber law implantation.

[25] Cyber Security Panel Meeting, Gadgets 360, https://www.gadgets360.com/internet/news/google-apple-paytm-banks-parliamentary-panel-meeting-discuss-cyber-security-4166782, Last Accessed on 12th July 2023.