International Research Journal of Commerce and Law
Volume 11 Issue 04, April 2023 ISSN: 2349-705X Impact Factor: 6.893
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Cybercrime in India- A Critical Study in Morden Prospective

Aekansh Yadav, Research Scholar
Department of law
Bishamber Sahai (PG) Institute, Roorkee
Dr Amit Choudhary, Assistant professor
Department of law
Bishamber Sahai (PG) Institute, Roorkee

Abstract

To commit a cybercrime requires using a computer, network, or other device to communicate via the internet. It's not always about the money when it comes to hacking and other forms of cybercrime. Different types of cybercrime have different goals; some attempt to disable or destroy particular computers, while others exploit the internet to spread malware or illegal content. Some forms of cybercrime aim to infect computers with a virus so that it may spread to other machines and even whole networks. Any place with digital data, the ability to conduct the crime, and the motivation to do so is a potential starting point for cybercrime. Cybercriminals may vary in size and shape, from a single user engaging in cyberbullying to a nation-state orchestrating a massive attack. Cybercrime is not an isolated event but rather a widespread phenomenon. Hackers often enlist the aid of others to carry out their schemes. The same principles apply, whether it's a malware developer secretly trading source code, a drug dealer utilising Bitcoin brokers as escrow services, or a nation-state stealing IP via its technology contractors. Cybercriminals use a wide variety of attack vectors to carry out their assaults, and they are always on the lookout for new ways to achieve their aims without being discovered or facing the legal ramifications that may ensue from doing so. While cybercriminals often use malware and other kinds of technology, social engineering remains an integral aspect of the execution of the great majority of the different types of cybercrime. While email phishing is a typical cybercrime in and of itself, it also forms an integral part of more sophisticated operations like those that aim to get access to corporate email servers. In this phishing attack, the attacker contacts the target's workers pretending to be the company's owner and demanding immediate payment of bogus bills.

Keywords: *Cybercrime, Cyber Laws, Social Engineering, Identity theft, Cyberstalking, Online Criminal*

Introduction

Crimes done by computers, networks, or other networked devices are collectively referred to as "cybercrime." While financial gain is a common motivation for hackers and other cybercriminals, it is not always the case. Some forms of cybercrime aim to harm or turn off individual computers or other devices; others desire to transmit harmful software, unlawful information, photos, or other material forms across networks. Specific forms of cybercrime aim to spread a computer virus from one system to another and even across networks. Wherever there is digital information, the tools to commit a crime, and the intent to do so, the seeds of cybercrime may be sown. Cybercriminals range in size and sophistication, from the isolated user who engages in cyberbullying to the nation-state that orchestrates large assaults. Cybercrime is not a rare occurrence but rather takes many shapes and forms. Hackers often use the services of other parties to help them carry out their plans. This is true whether the perpetrator is a malicious software developer selling source code online, a drug dealer utilising Bitcoin brokers as an escrow service for virtual cash, or a state threat actor stealing intellectual property via technology contractors. Even though cybercriminals often use malware and other technologies, social engineering is a vital aspect of the execution of the great majority of the many types of cybercrime. Although phishing emails are employed in many types of cybercrime, they are essential in targeted attacks such as corporate email intrusion. Email impersonation attacks occur when a malicious actor pretends to be a company's legitimate owner to trick workers into paying fake invoices. **(Sujata and Yogesh)**

Objective of Paper

1. Discuss cyberlaw and crimes
2. Discuss various landmark judgements
3. Discuss various impacts of cybercrimes
4. Discuss various laws & implementation

The Roots Of Online Criminality

At the beginning of the 1970s, it was common practice for criminals to carry out their nefarious endeavours via telephone. The individuals who were involved were given the appellation "Phreakers." The word "cybercrime" was not coined until the 1980s after it had been used for years. Someone could examine private files and information on another person's computer, copy those files, or manipulate the material differently. Lan Murphy, better known by his alias Captain Zap, was the first person ever to be found guilty of conducting a cybercrime and sentenced to prison in 1981. This incident indeed took happened. He had compromised the security of the American telephone company's computer network and tampered with the system's internal clock to make it possible for consumers to make free calls even at the busiest times of the day. **(Trout)**

Cyber Laws

The widespread use of the Internet in today's society has led to a rise in a new category of criminal activity known as cybercrime, which is on the rise. When the Information Technology Act of 2000 was passed into law to fight the crimes associated with the Internet, its primary purpose was to facilitate the use of information and communications technology in business settings. The IT Act details the transgressions that may now result in a criminal charge. In addition, the Indian Penal Code from 1860 has been updated to include provisions for prosecuting cybercrimes. **(Zittrain)**

1) *Types of cybercrimes*

There is a wide variety of cybercrimes since criminals may choose to attack almost anything of value to an individual, a group, or a nation. Let's analyse these categories as appropriate. **(Gibson)**

Identity theft

If a criminal can access a user's personal information, they may conduct tax or health insurance fraud, steal money, or get access to sensitive information. Someone with access to your personal information may open a bank account, apply for a driver's licence, apply for welfare, or commit crimes in your name. They might send phishing emails, hack into users' accounts, or steal their personal information from social media. **(Myers)**

Phishing

In these assaults, hackers trick victims into opening infected attachments or visiting compromised websites. As hackers grow in prominence, more and more emails aren't being flagged as spam. Accounts are compromised when users fall for phishing emails claiming they must reset their password or update their payment information. **(Solove and Schwartz)**

Social Engineering

Criminals will employ social engineering to contact you, generally over the phone or online.In most cases, they will pretend to be a helpful staff member to get the information they need from you. Your passwords, your employer's name, and your bank account number are all examples of sensitive data. Cybercriminals will do extensive online research on you before they even consider adding you as a friend on social networking networks. If a hacker gains access to your account, they may use it to steal money or commit identity theft. **(Bowker)**

Cyberstalking

Criminals engage in cyberstalking when they monitor your online activity to steal your personal information and use it to commit fraud or identity theft. There are several entry points for data collection. They could accomplish this by sending phishing emails, hacking into users' accounts, or collecting users' personal

information through social media. Examples of controlling, influencing, or intimidating behaviour include making threats, spreading false information, or engaging in sexual harassment. **(Broadhurst and Chang)**

Botnets

Botnets are networks of infected computers that may be controlled remotely by cybercriminals. Hackers in remote locations utilise these botnets to launch DDoS attacks or send spam. However, botnets may also be used maliciously, making them potential malware.

Prohibited content

The table above shows that the number of reported cybercrime cases in India is rising. Phishing scams, identity theft schemes, online harassment, cyberstalking, and breach of privacy are the five most common types of cyber crimes. **(Chang and Grabosky)**

The following is a list of some of the internet-related crimes that carry penalties under the IT Act and the IPC:

1. **Cybercrimes under the IT Act:**

- Modifying original computer-generated paperwork - Section 65
- Data Tampering and Computer Hacking - Sec.66
- Indecent Publication Act, Section 67
- Abuse of a Protected System in Violation of Section 70
- Security and Privacy Breach, in Violation of Section 72
- Distributing forged certificates for use in digital signatures - Section73
-

2 The International Penal Code and Other Cybercrime Laws:

- Sec. 503 IPC: Threatening others through electronic mail

- Emailing slanderous statements (Section 499 IPC)
- IPC 463 Forgery of Electronic Records
- Online fraud and impersonation: in violation of Section 420 of the Indian Penal Code
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- Email Abuse - Sec.500 IPC

2. **Acts of Special Concern Regarding Cybercrime:**

- Online sales of weapons violate the Gun Control Act; online distribution of psychoactive drugs in violation of the Controlled Substances Act; online distribution of controlled substances. According to the data in the table above, the amount of cybercrime recorded in India is increasing. The five most prevalent cyber crimes are phishing scams, identity theft schemes, online harassment, and cyberstalking. Invasions of privacy are the fifth most common type of cybercrime.

The Rising Tide of Cybercrime

2018	27,248
2017	21,796
2016	12,317
2015	11,592
2014	9,622
2013	5,693
2012	3,377

The number of instances involving cybercrime in India is undoubtedly rising, as seen in the table above. Phishing scams, identity theft schemes, online harassment, cyberstalking, and breach of privacy are the top five most common types of cyber crimes. **(Glenny)**

2) Analysis of Cybercrimes In India:

With more than 560 million people already online, India has overtaken Japan as the world's second-largest Internet market. Furthermore, by 2023, it is anticipated that more than 650 million individuals in the nation will utilise the Internet. According to the most current figures that are available from the National Crime Records Bureau (NCRB), in 2018, there were a total of 27,248 instances of cybercrime that were recorded in India. During the same year, there were a total of 1205 instances of cybercrime that were documented in the state of Telangana. The FBI conducted a poll to determine which nations suffer the most from the effects of cybercrime and found that India rated third among the top 20. The national cybercrime reporting portal, cybercrime.gov.in, has been operational for one year and has received 33,152 complaints since its establishment by the federal government. These complaints have resulted in the submission of 790 first information reports (FIRs). **(Grabosky)**

Crime as an Evil Factor in Society

Even though the idea of a community that never engages in illicit activity can only be discovered in the domain of fiction, criminal activity can be found in every facet of human civilisation. Some individuals can see it annoying when you ask a question like "Why is there so much ado about crime?" since it raises an important topic that deserves more attention. It is impossible to deny the existence of crime as a social phenomenon; it is endemic to every society and has existed for a long time. Criminal behaviour is present in every human culture, regardless of how advanced or primitive it may be. This is the case even in places like ancient Egypt. It is appropriate to express worry about high crime rates; however, this should not be done because of the nature of the crimes in and of themselves; instead, this should be done because of the possibility of social unrest. In addition, the impact of criminal activity may be far more severe for certain victims than others. It is not unheard of for victims of crime to wind up with nothing due to what happened to them. The values that assist in satisfying human demands, such as the right to one's property, safety, and wealth, are

among the most significant, if not the most critical, values. Other examples of such matters are safety and peace. **(Halder and Jaishankar)**

Impact of Cyber Crime on Teenagers

Teenagers in today's culture are understandably anxious about becoming the target of cyberbullying, sometimes called online bullying. The study's findings indicate that the practice has been more widespread over the last five years and that children and teens under eighteen are more likely to be victims of cyberbullying and more afraid of it. Additionally, adults have a much-increased risk of being victims of cyberbullying. Because of this inclination, our civilisation is going through an unfavourable metamorphosis, and it's unsettling to see it occur. The results of several studies indicate that young women in their teens are the segment of the population that is most often targeted by criminals online. When a person gets threats, harsh negative remarks, or horrible photos or comments from another person, the possibility of becoming the victim of cyberbullying becomes a source of concern for that individual. This is because cyberbullying may take many different forms. This is primarily achieved using the core technologies covered before; most of these technologies may be obtained via the Internet. It is possible to harass someone online via chatting, instant messaging, and other types of behaviour that come under the umbrella of cyberbullying. This is referred to as cyberbullying. It is more probable that those who use social networking sites like Facebook, Orkut, and Twitter will participate in bullying behaviour when they are online (cyberbullying). In my view, people who are generally feared may reach a point where they are depressed, embarrassed, and frightened simultaneously. These statistics lead us to the probable conclusion that if a person is the target of cyberbullying, they may get sad to the point where they hurt themselves, which might be a direct result of the bullying. **(McQuade)**

Influence of Online Criminal Activity on Consumer Behavior

As a result of the information revolution and strategic use of the Internet, cybercriminals and cyber terrorists can now target the online operations of commercial firms. This has made many societies that were previously safe susceptible to assault. This holds in every aspect of life, especially in the professional world. Cybercrime is the label given to this murky aspect of business, and it has developed in various forms that question our preconceptions about how we should purchase safely and securely online. The strategic consequences that any threats to an organisation's online operations may have on the organisation's long-term performance are something that organisations should consider. Internet retailers risk losing customers if they don't do what needs to be done to eliminate or significantly mitigate these risks. These safety measures, commonly referred to as "cyber security," were developed to protect customers' financial and identification information of customers while also making it easier for them to do business online. The development of models that will allow companies to assess the impacts of cybercrime on online customer trust and to react by capitalising on the advantages of recent improvements in online security is a need. These models need to be created so that businesses can meet this demand. For firms to be able to meet this demand, they need to build models along these lines. Because of the influence these two facets of e-commerce have on online shoppers, companies are responsible for guaranteeing that the security measures they now have in place will be successful. Because of this, there is an increased likelihood that customers will continue to utilise the Internet to finish their purchases. **(Taylor)**

Landmark judgments

The following verdicts are widely regarded as landmark decisions on cybercrime in India. The first polymorphic virus was released to the public in 1992, and this event is often considered the starting point of the very first incidence of cybercrime. The case of Yahoo v. Akash Arora (1999), which took place in India, is considered to be one of the first instances of cybercrime to occur in that nation. In this particular case,

the plaintiff sought a permanent injunction against the defendant, Akash Arora, because he was accused of making unauthorised use of the trademark or domain name "yahooindia.com." In addition, the plaintiff requested an injunction against Akash Arora. The second instance is the lawsuit that Vinod Kaushik and others filed against Madhvika Joshi (2012). In this case, the court ruled that by Section 43 of the Information Technology Act of 2000, it is illegal to access a spouse's or father-in-law's email accounts without obtaining their consent. This ruling was made because it is unlawful to access the email accounts of a spouse or father-in-law without first obtaining their permission. In 2011, an agreement was made that was accepted by all parties. The evolution of cybercrime is at the centre of this litigation, with India as the primary focus.

3) *Case number: CBI v. Arif Azim (Sony Sambandh) (2013)*

In 2013, India had its first individual convicted of a cybercrime. The chain of events started with a complaint from Sony India Private Ltd. Sony India Private Ltd. operates the Non-Resident Indian-centric website www.sony-sambandh.com (NRI). This service allows NRIs to ship Sony things they've purchased online inside India to friends and family who live there. The items will be delivered to the right persons, or the firm will refund your money. Somebody in May of 2002 used the alias Barbara Campa bought a cordless headset and a Sony colour television on the Internet. She authorised us to charge her credit card and provided Arif Azim's address in Noida so we could send the goods to him. The credit card company confirmed the payment, and the sale was completed. After doing all appropriate checks and balances, the company sent the goods to Arif Azim.

Photographs of Arif Azim receiving the package at delivery were taken. A valid cardholder who first approved the sale subsequently denied doing so, causing the credit card company to alert the store that the purchase was fraudulent. A CBI investigation into charges of internet cheating was launched under Sections 418, 419, and 420 of the Indian Penal Code after the company informed the agency of the allegations. As a result of the inquiry, Arif Azim was taken into custody. According

to the findings of the investigations, Arif Azim, while working at a contact centre in Noida, stole the credit card information of a U.S. citizen. He then made fraudulent use of the organisation's domain name.

IN THIS ONE-OF-A-KIND CYBERCRIME INVESTIGATION, the FBI tracked down a stolen colour TV and a pair of wireless headphones. Given the weight of the CBI's evidence, the accused has conceded guilt. As far as we know, Arif Azim is the first cybercriminal to be found guilty of a crime; he was found guilty of violating Articles 418, 419, and 420 of the Indian Penal Code. The judge, however, decided that the 24-year-old defendant, a first-time criminal who deserved sympathy, should be given a lighter sentence. The court agreed, and as a result, the offender was given a year of probation. The decision will have far-reaching consequences for the whole country. This case marked the first time a cybercrime had been successfully prosecuted. Still, it also showed that the Indian Penal Code could be utilised to try issues that included cybercrime but were not covered under the Information Technology Act of 2000.

4) *A Fraudulent Mphasis Call Center at Citibank in Pune (2005)*

Three and a half million dollars were stolen from four Citibank accounts in the United States in 2005 and moved to many bogus accounts that could be accessed over the Internet. Employees successfully obtained PINs from customers by assuring them of their willingness and ability to help them through challenging situations. Instead of trying to crack encrypted programmes or bypass firewalls, they looked for flaws in the MphasiS system.

The court has decided that the defendants are former workers at a contact centre operated by MphasiS. Employees who enter or leave the building are subject to a thorough inspection. The workers were forced to commit the figures to memory. The money was sent through SWIFT, the Society for Worldwide Interbank Financial Telecommunication. The fraudulent activity was carried out using hacked customer electronic accounts. This fact alone justifies labelling the act as a cybercrime. Since

the IT Act's purview is broad enough to include the commission of crimes involving electronic documents, the punishment for such crimes may be the same as for offences using conventional materials. The court reasoned that Section 43(a) of the Information Technology Act of 2000 applies because the transactions at issue involve the kind of unauthorised access protected by that provision. The defendants broke Section 66 of the Information Technology Act, 2000 and Sections 420, 465, 467, and 471 of the Indian Penal Code of 1860.

5) *Nasscom v. Ajay Sood & Others (2005)*

The National Association of Software and Service Companies is the plaintiff in this case (Nasscom for short).In India, Nasscom represents the software business more than any other organisation. Defendants oversaw an enterprise-wide placement firm that conducted leadership searches and recruited new employees. The defendants, posing as representatives of Nasscom, emailed unsuspecting recipients to get access to sensitive information that may be utilised in a "headhunting" operation. Emails purporting to come from Nasscom were used to contact other parties. Emails were sent to recipients outside of Nasscom utilising the company's domain. Defendants are prohibited from using the trade name or any name confusingly similar to Nasscom, according to the plaintiff, who says that the High Court of Delhi recognised the validity of the plaintiff's trademark rights and granted an ex-parte ad interim injunction.The request was issued after the plaintiff successfully petitioned the High Court of Delhi to recognise his trademark rights. The court has informed us that the High Court of Delhi issued this ruling. As another violation of the guidelines, the defendants could not state or imply that they were members of Nasscom in any capacity.

The plaintiff in this lawsuit is Nasscom, which stands for the National Association of Software and Services Companies. Regarding India's software sector, Nasscom is the largest trade group. The defendants oversaw an internal placement agency that recruited and hired top-level executives. The accused, posing as representatives of Nasscom, wrote emails to unrelated persons to glean contact information for

"headhunting." The email sent from a Nasscom account was used to contact other parties. Messages were sent to other parties using the Nasscom email domain. According to an ex-parte ad interim order given by the High Court of Delhi, which recognised the validity of the plaintiff's trademark rights, the defendants are prohibited from using the trade name or any name confusingly similar to Nasscom. The plaintiff had asked the High Court of Delhi to grant an injunction to safeguard his trademark, and the court complied.

6) Punjab National Bank, Head Office, New Delhi, and Others v. Poona Auto Ancillaries Pvt. Ltd., Pune (2013)

In 2013, Rajesh Aggarwal, who served as the Information Technology (IT) Secretary for Maharashtra, handed down one of the most significant compensation judgments ever given in a court adjudication of a cybercrime case. The complainant, Manmohan Singh Matharu, was the managing director of a firm headquartered in Pune. Aggarwal issued a demand for payment of Rs 45 lakh from the Punjab National Bank (PNB) to Matharu—auto Parts of Poona. Matharu's PNB account in Pune was emptied of Rs 80.10 lakh after he responded to a phishing email.However, the bank was held at fault for failing to conduct adequate security checks against fraudulent accounts set up to deceive the complaint. Because he fell for the phishing email, the complainant was made to feel somewhat responsible for the situation. The bank, however, was held at fault for failing to implement adequate safeguards against bogus accounts.

Conclusion

Cyber law is predicated on the Information Technology Act and the rules enacted to implement it. The Indian Penal Code from 1860 might be examined if a crime cannot be adequately handled by the Information Technology Act. However, the present cyber legal system cannot deal with various cybercrimes. New categories of cybercrime are being introduced to the cyber law regime regularly to keep up with the evolving nature of the crime as the government advances its 'Digital India'

project. As a result, the laws need to be adjusted to reduce the frequency with which such offences might be committed. In today's digital world, the boundaries of cyberspace are porous, and the Internet connects people all over the globe. This directly contributes to the rise of cybercrime worldwide, especially in India. The ever-evolving nature of digital technology makes cybercrime's flexibility the most formidable challenge it poses. This motivates the development of ever-evolving methods and techniques for conducting cybercrime. Every day Internet users and cyber criminals have a say in where the Internet goes. Many people worry that the world will end online, and widespread fraud might cause significant economic losses. Even if progress may be delayed, knowing that answers are being explored could help ease some of these worries. The many ways in which the Internet is proper should be enough to keep it from becoming a hotspot for criminal activity and a haven for the wicked. Commercial software providers and those with the ability to identify and halt fraudulent conduct must handle the majority of the job, even if the government has an important role to play. Protecting others from harm without causing them undue worry requires elaborate measures. Security systems need to be user-friendly while also providing maximum protection. If the Internet is to continue growing, cybercrime must be dealt with as well as, or better than, traditional crimes. To what extent cybercrime will still be an issue in the next decade is an open question.

References

Bowker, Art. “The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century" .” Charles C. Thomas Publishers, Ltd. Springfield., 2012.

Broadhurst, R and Lennon, Y.C Chang. “ "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds),.” *Asian Handbook of Criminology*. New York: Springer (ISBN 978-1-4614-5217-1), 2013. (pp. 49–64).

Chang, Lennon Y.C and P Grabosky. “"Cybercrime and establishing a secure cyber world", in M. Gill (ed).” Handbook of Security NY: Palgrave., 2014. (pp. 321–339).

Gibson, Owen. “ "Warning to chatroom users after libel award for man labelled a Nazi". .” The Guardian., 2006.

Glenny, M. DarkMarket. “ cyberthieves, cybercops, and you, .” *2011*. New York, NY : , n.d. Alfred A. Knopf, ISBN 978-0-307-59293-4.

Grabosky, P. “ Electronic Crime, .” New Jersey: : Prentice Hall, 2006.

Halder, D and K Jaishankar. “Cyber Crimes against Women in India. .” New Delhi:: SAGE Publishing. ISBN 978-9385985775., 2016.

McQuade, S. “Understanding and Managing Cybercrime.” Boston: Allyn & Bacon., 2006.

Myers, KS. “"Wikimmunity: Fitting the Communications Decency Act to Wikipedia".” *Harvard Journal of Law & Technology* (2006): 20: 163. SSRN 916529.

Solove, D and P Schwartz. “Privacy, Information, and Technology. (2nd Ed.).” New York, NY: : Aspen Publishers. ISBN 978-0-7355-7910-1, 2009.

Sujata, Pawar and Kolekar Yogesh. “Essentials of Information Technology Law.” Notion Press, 2015. pp. 296–306. ISBN 978-93-84878-57-3.

Taylor, Paul. “Hackers: Crime in the Digital Sublime (3 November 1999 ed.). .” Routledge;: ISBN 978-0-415-18072-6, n.d. 1 edition. p. 200.

Trout, B. “"Cyber Law: A Legal Arsenal For Online Business", .” New York: : World Audience, Inc., 2007.

Zittrain, Jonathan. “Be Careful What You Ask For: Reconciling a Global Internet and Local Law". .” SSRN 395300., 2003.