Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Cyber Fraud in Relation with Cyber Crime Critical Study

[1]Debalina Das, [2]Archana Aggarwal
[1]BALLB(H)
Amity University Uttar Pradesh, Noida
[2]Professor
Amity University Uttar Pradesh, Noida

***Abstract*:** In this digital era, cyber fraud is a constant and ever-changing danger that governments, companies, and people throughout the globe face. This critical research examines the complex relationship between cybercrime and cyberfraud, looking at its many facets as well as its effects, legal frameworks, technical solutions, and ways to stop or lessen it. This study delves into the many forms and techniques of cyber fraud, the economic, social, including psychological effects, and the efficacy of legal and regulatory countermeasures. It does this via theoretical examination, empirical research, through case studies. In addition, it finds proactive ways to strengthen cybersecurity resilience and investigates how cryptography, authentication, intrusion detection systems, AI, and ML fight cyber fraud. The goal of this project is to help improve cybersecurity in a digital environment that is becoming more linked and susceptible to cyber fraud by expanding knowledge about cyber fraud and providing evidence-based solutions to avoid and respond to it.

Keywords: *Cyber fraud, Cybercrime, Cybersecurity, Legal frameworks, Technological approaches, Prevention, Mitigation.*

Theoretical Foundations, Nature And Scope Of Cyber Fraud

If a crime is committed or aided by means of a computer, network, or hardware device, then it is known as cybercrime. Depending on the circumstances, the computer or gadget might be either the criminal's tool, their accomplice, or even their victim. The only required setting is a computer, yet it might also happen in other virtual or physical places. The existing legal definition of cybercrime differs greatly among countries, and this is acknowledged. Cybercrime is defined in a practical way by Kshetri (2010). The way he sees it, "Cyber Crime" is any illegal conduct that primarily involves the use of computers and computer networks to break the law or violate regulations[1]. Attacks on vital infrastructure, denial of service, theft, trespassing, obscenity, fraud, identity theft, cyber terrorism, and extortion are all examples of cyber crimes. There is no denying that criminal organizations use cybercrime as a means to communicate and interact with their wide global network. As a result, the cyber world is much more dangerous now that organized crime and the internet work hand in hand.

According to many sources (Tade & Aliyu, 2011; Whitty, 2015, 2019, and Gao, 2021), online fraud occurs when someone uses deceit to gain money via the use of network communication technology, sends false invites to prospective victims, or conducts fraudulent transactions utilizing the internet. Emails purporting to come from reputable sources are a common tool in phishing and other forms of online fraud (Frauenstein & Flowerday, 2020). Email isn't the only channel by which online fraud happens in this day and age; SMS, cellphones, and social media platforms are also potential entry points (Vishwanath, 2015; Aleroud & Zhou, 2017; Frauenstein & Flowerday, 2020).

When it comes to security issues, internet fraud (including phishing) ranks sixth and has the best success rate among any attack vector (Verizon, 2019). In 2017, a phishing scam posing as a major Asian manufacturer tricked

[1] Diwanji, S. (2018). Total number of cyber-crimes reported across India from 2012 to 2018. Statista.

Google and Facebook into losing over $100,000 (United States Department on Justice, 2017). The United States[2] lost around $2.7 billion to online fraud in 2018, according to a meta-analysis. With 3.25 million victims annually, internet fraud is additionally the fastest rising crime in the UK (Norris and colleagues, 2019). Online scammers started using phishing assaults in 2020, just after the COVID-19 epidemic started, to take benefit from people's fear and confusion (Muncaster, 2020). According to Burnnes et al. (2017) and other academic studies (e.g., Modic & Lea, 2013; Harrison and colleagues, 2016a; Modic & al., 2018), internet fraud has emerged as a significant issue in social governance.

Motivated offenders, suitable victims, and ineffective supervision are the three main components of routine activity theory that lead to victimization (Cohen & Felson, 2010). In order to swindle their victims, crooks that are motivated adopt ingenious tactics. Reciprocity, social proof and conformity, commitment or uniformity, authority, like, and scarcity are the six guiding principles of persuasion that Cialdini (2018) summarizes as being often used by con artists[3]. To prevent missing out on chances, for instance, people react to information about scarcity (Bullée and colleagues, 2015). When it comes to effective guardianship, fighting and eliminating online fraud is something that every country takes very seriously. The most common approaches are enforcing stringent legal penalties on offenders, raising awareness among possible victims, and using technological means of interception (Chen & Yang, 2022). If we want to know why so many individuals fall prey to online fraud assaults daily, we need to change our focus to the right people. Research on possible victims of online fraud may be categorized into three primary areas.

For starters, there's the field of demographics, which studies the correlation between the following characteristics of online fraud victims: age, income, education level, gender, and race (Cohen and colleagues, 1981; Holtfreter et a., 2006; Salthouse, 2012, and Burnes et co., 2017; Gavett as al., 2017). Internet fraud and other forms of personal crime disproportionately affect males, according to research by Carcach et al. (2001). The idea that the elderly are more susceptible to fraud has been developed from anecdotal evidence, including news stories, and the increasing number of studies examining the topic of aging. Research by Carcach et al. (2001) and others has shown that older persons are disproportionately victims economic consumer fraud when compared to victims of other forms of crime. It is connected to their poor cognitive processing as well as elevated feelings of loneliness, which makes the elderly more easily fooled, as Burnes et al. (2019) concurred. Also, victims' wealth and degree of education are correlated with their susceptibility to fraud, according to James et al. (2014). It has been shown in research carried out by the Federal Trade Commission (FTC) that non-Hispanic white Americans are less likely to fall prey to fraud than Aboriginal the Americans, African Americans, & Hispanic Americans (Anderson, 2004; Anderson, 2013).

In addition, researchers have mostly focused on studying the elements that influence susceptibility in online fraud when it comes to the direction psychological features. Factors such as risk perception, trust, suspicion, personality, self-control, and Ashton and Lee's (2009) and Harrison et al.'s (2016a) research on these topics are cited in Moody et al. (2017) and Wright and Marett (2010), respectively. According to Holtfreter et al. (2008), groups who lack self-control are more prone to being deceived. People who lack self-control often want to satisfy their desires right away, which leads to this. In order to get what they want, they could fall for a con artist's tricks. Not all personality qualities are predictive of susceptibility to online fraud, according to studies that examined the correlation between the two. While no other personality qualities were shown to have a predictive influence, Alseadoon and colleagues (2012) demonstrated that openness as well as extraversion might increase the likelihood of responding to emails in a fraud simulation involving 200 college students. Researchers have looked at how victims' internet history, security awareness, and personality traits affect their vulnerability for online fraud (Larcom & Elbirt, 2006; Wright & Marett, 2010).

[2] National Crime Records Bureau. (n.d.). *Crime in India 2018 - Volume 1*. Retrieved from https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf

[3] Grabosky, P. (2000, March 9-10). Cyber Crime and Information Warfare. Paper presented at the Transnational Crime Conference, Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service, Canberra.

3.1 CYBERCRIME: A CONCEPTUAL PERSPECTIVE

Cybercrime and cyber deviance originate from the fact that cyberspace enables near-instantaneous contacts between geographically distant persons, which in turn opens the door to new kinds of associations. To put it simply, cybercrime refers to any illegal activity that makes use of, or is aided by, a computer, network, or other physical device. Depending on the circumstances, the computer or gadget might be either the criminal's tool, their accomplice, or even their victim[4]. The only required setting is a computer, yet it might also happen in other virtual or physical places. There is widespread agreement that the present legal definition of cybercrime differs significantly among countries. According to Kshetri (2010), a cyber crime may be defined in a practical way. "Cyber Crime is defined as a criminal activity in which computers or computer networks are the major method of committing an offense or breaching laws, rules or regulations," he states. Denial disruption attacks, cyber-theft, trespassing, cyber obscenity, assaults on key infrastructure, online fraud, ID fraud, cyber terrorism, and cyber extortions are all examples of cyber crimes. Evidently, organized crime groups rely heavily on cybercrime as a means of communication and collaboration inside their huge global network. Thus, the digital world is even more vulnerable due to the fact that organized crime and the internet work hand in hand.

The phrase "cyber crime" is used globally to characterize illegal actions that occur on the internet. These days, it's becoming a major issue for people everywhere. The law states that nothing may be deemed a crime[5]. Many forms of cybercrime, nevertheless, go unpunished. Cybercrime is a worldwide problem, making geographical boundaries irrelevant. Given its global scope and nature, cybercrime does, in fact, impact different parts of the world in different ways.

Uniform cybercrime laws that apply worldwide are few. Unfortunately, cyberspace and the internet have become preferred tools of cybercriminals who may avoid detection even in the absence of international collaboration among law enforcement authorities, despite their widespread use for various crimes[6]. There must be a global solution to the problem of inconsistent regulation if we are to successfully fight cybercrime and those who commit it. The advent of new forms of electronic communication has, unsurprisingly, opened many opportunities with a potentially criminal bent. The Internet, often called "Cyberspace," enables the rapid execution of several activities thanks to contemporary computer technologies. Machines replaced people, opening up more opportunities and choices. Businesses, banks, schools, and train bookings have all gone computerized, which is a clear indication of how dependent human civilization is on these little computers. Working routines based on archaic paper have become outmoded due to the rapid pace of modern life. The physical damage that criminals inflict on individuals and their belongings has been a significant concern for civilizations worldwide for than a hundred years. Police forces throughout the world have evolved to combat these new forms of criminality. Emerging crime types are a direct outcome of rapid industrialization and urbanization, and they pose a greater danger to societal order, safety, and security.

If Cyberspace is the sort of community that exists, a huge neighborhood made by networked computer users all over the globe, then it stands to reason that many parts of traditional society may be understood as data. Electronic merchants emerge from e-commerce, doctors establish online relationships with patients, and connected educators offer networked education. It should not be surprising that there are individuals who engage in cybercrime. Computers, when used properly, can make any company function more efficiently. Data is processed and manipulated by the computer, an exceedingly complicated electrical instrument. The Information Technology (Certifying Authorities) Regulations, 2000[7] states that a computer is "any high-speed data processing device or system that performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic, or optical impulses." This definition covers all aspects of a computer system & computer network, including the computer itself as well as any input, output, storage, processing, software, and communication facilities which are connected to it.

[4] Central Bureau of Investigation. (n.d.). *Manual*.
[5] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000
[6] Economic and Political Weekly. (1999, May 15). Dithering over Cyber Laws. *Economic and Political Weekly, 34*(20), 1151.
[7] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000

- **THE ECONOMY AFFECTED**

For the purpose of sending and receiving money, most individuals nowadays use their computers and the internet. Internet money scams are quite common, hence the chances of being a victim are high. More than 72 million Americans were victims of cybercrime in 2010, resulting in losses exceeding $32 billion, according to Norton Cybercrime in 2011. Online fraud is becoming more common in India as a result of programs like "cashless India" and others like it, particularly among the country's less tech-savvy citizens[8].
Companies have the same financial burden as individuals when it comes to cybercrimes. Actually, up to 80% of the businesses polled have reportedly felt the effects already.

- **THE DISCLOSURE OF PRIVATE DATA**

When people's private information is stolen, it costs them more than simply money. Because everyone can see users' life on social media, even most secure systems put users at risk. On top of that, bad guys may still breach user accounts and steal personal information. Not only that, but spam and phishing hurt people as well. When users experience money losses or get their personal information stolen, they lose trust in these kinds of apps and services. Even if the real criminal is never revealed[9], the program or website is still marked as harmful and false. Customers are also wary about submitting their credit card information when asked to do so. Due to the harm it does to an internet company's reputation, this endangers a potential client.

- **DECLINE IN CUSTOMER CONFIDENCE**

Customers start to lose trust in these platforms as they experience financial losses and see a risk of providing personal information. The website or software is still considered harmful and deceptive regardless of who does it. It makes consumers think twice before entering their credit card information when asked to do so. If customers can't trust an internet business, they could not do business with them in the future. Most modern military depend on cutting-edge computer networks & technology. Even though the technique is not new, cybercriminals still use information warfare to spread malware that may compromise networks and spread misinformation. Terrorists, hackers, and even militaries utilize these technologies to get into other nations' security networks and steal data. Dangers and warnings are also sent using computer systems.

TYPES OF CYBERFRAUD

In this context, "cybercrime" is any kind of unlawful action that involves or is directed at a computer. Theft, deception, forgery, defamation, so injury are all examples of traditional crimes that may occur in cyberspace, and they are all punished under the Indian Penal Code. The Information Technology Act of 2000[10], which was introduced on October 17, 2000, aims to tackle these problems and many more caused by computer abuse. Cybercrime may be broadly categorized into two main areas (Section 5.1):Computing as a Weapon: attacking other computers via the use of one's own computer. For example, viral attacks, hacking, and Denial or Service (DOS) attacks.Using a computer to commit a crime in the real world is a prime instance of weaponizing the machine. There are many examples, such as cyber terrorism, pornography, credit card fraud, and infringements of intellectual property.

Security Monitoring: To have "access" is to be able to use, instruct, or connect with the mathematical, logical, or memory function capabilities of a computer or network. Thus, anyone who gains possession of a computer, system, or network without the owner's or controller's consent is committing an act of illegal access.
Exploits for Security Flaws: Any attempt to breach security measures and get sensitive information from a network or computer is known as a hack. Cybercriminals often employ custom-made or publicly-available

[8] Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electronic Commerce Research, 13, 41-69.
[9] Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.
[10] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000

software to gain unauthorized access to computer systems[11]. Their natural inclination is to ruin things, and they like doing it. It is common practice for hackers to transfer stolen monies to their personal bank accounts after gaining access to sensitive information like credit card numbers. Damage to the system may occur if hackers steal or modify data or implant malicious software like worms or viruses. When an intruder gets control of another website's server via hacking, it is known as web hijacking.

Cybercrime and Online Deception: One major perk of the internet is the ease and speed with which people may do business. The proliferation of con artists on the internet has led to an epidemic of online fraud.

- **Make bogus security alerts and impersonate websites:** Con artists create counterfeit websites that seem authentic. Collecting users' personal information was the main goal of these websites. With this data, we may access your bank and corporate accounts. If you get an email requesting personal information and include a link to a potentially dangerous website, you should proceed with care. Never, ever, ever give up your personal data to Report Phrase a website just because it appears legitimate. That's just asking for trouble from hackers. This kind of unwanted email would never be sent by any legitimate company.

- **Scandals involving lotteries:** A lottery winner might be notified of their prize via these electronic communications. The money can't be transferred until the recipient confirms receipt. After that, you'll get another email that asks for your bank details so that money may be sent directly to your account. Last but not least, the email asks for the processing/handling fee. The processing fee is a hoax, and the banking data is used for additional fraudulent reasons; obviously, no payments are ever transferred.

- **Spoofing for Deception:** is to gain unauthorized access to a system by impersonating a genuine user. By taking on a phony persona, a hacker is able to get illegal access onto a computer system. He is able to carry this out since he has already obtained the actual password. A new identity is formed when he tricks the computer into thinking he is the actual system operator. When that happens, the hacker has successfully gained access to the system. He may pull off a number of con jobs using this false persona. To put it simply, spoofing occurs when an item gives the impression of having originated from one location while, in reality, it has originated from another.

- **Theft of Credit Cards:** Online commerce has become an integral part of most people's daily life. Whether intentional or not, transmitting sensitive financial data over the internet is fraught with danger. In the absence of adequate security measures, criminals may get access to private financial data and use it illegally by impersonating the cardholder.

Crime on the Internet: Taking someone else's money or personal information by using their computer dishonestly or illegally. Verification Crimes: -Theft or fraud committed by an unauthorized third party using another's personal details is known as identity theft. Identity theft is a stepping stone to other types of financial crime that criminals engage in[12].

- **Theft of Online Time: -** Using someone else's paid-for internet access without their consent.
- **Theft of computer hardware:** This kind stealing crime includes the theft of computers, computer components, or any equipment that is linked to a computer.

Internet-Based Terrorism: Power plants, military installations, financial institutions, control centers for air traffic, road traffic control, & communication networks are among the most probable targets. There are others, such as emergency medical, fire, & police departments, among others. Modern terrorists find cyber terrorism attractive for several reasons.

- Terrorists' traditional methods were more costly.

[11] Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, Policy and Practice, 6(1), 17-33.
[12] Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge.

- Cyberterrorism has the benefit of secrecy compared to more traditional types of terrorism.
- Both the variety and the amount of goals are enormous.
- Cyberterrorism, the capacity to conduct attacks remotely, is an appealing feature to terrorists.
- More people could be directly affected by cyberterrorism.
- Phishing, Worms, Trojan Horses, and the Logic Bomb

What at first glance seems to be useful software really applies a light dampening. These kinds of software are called Trojan horses. Trojan horses consist of a client and a server. The attacker may begin using the trojan when the victim (unknowingly) launches the server on their PC. The attacker connects to the server using the client. Although TCP/IP is the most used protocol type, UDP is also used by certain malware functionalities. Essentially, what we call a "virus" is just software that can infect other programs and duplicate itself. It may take some time for symptoms of a viral infection to become noticeable. Many factors may trigger a virus to start spreading; they include chance, a predetermined number of executions, a certain day (such as Friday the 13th), or an event-driven effect. One possible function of a virus is to display a signal that, when activated, might lead to the propagation of the infection. Among its many possible effects are file deletion, data jumble, screen irregular behavior, computer freezing, and so on.Similar to viruses, worms may proliferate and infect other systems. The February 2001 appearance of the Maria Kournikova worm is one such occurrence[13]. The first computer virus, BRAIN, appeared in 1986. Famous viruses include CodeRed, Nimda a (2001), Michel-angelo (1991), Thought (1995), a Melissa, CIH (1999), Dark Avengers (1989), and many more. A logical bomb is a program that depends on an event. If this is so, the purpose of these programs is to respond to particular events by carrying out predefined actions. An example the a logic bomb would be the Chernobyl virus, which sits dormant most of the year and only goes off on a certain day.

Pornography: "The depiction of sexual acts for the purpose of arousing sexual desire in media such as books, films, etc." is the definition of pornographies. This class includes both websites that display pornographic material and those that develop and distribute pornographic content digitally. Approximately 420 million unique pornographic websites exist today. Much to everyone's dismay, child pornography is accessible online. Online, sexual predators prey on children from all over the world.

Deceptive Claims: The core of defamation is the intentional damage to another person's reputation. Anyone whose honor, dignity, or character is tarnished in the view of law-abiding persons is guilty of defamation.Cyber defamation refers to any type of defamation that involves the use of computers and/or the Internet. For illustration's sake, let's say someone spreads false and defamatory information about another individual via email or internet postings. Direct delivery of an insulting email does not constitute defamation; nevertheless, the contents that damage the recipient's reputation when sent to other parties via CC or BCC do constitute defamation. Publishing libellous articles or other information online constitutes defamation. Online smearing is also known as cyber defamation.

Misconduct in Cyberspace: Cyberstalking occurs when a cybercriminal persistently threatens or harasses a victim through the victim's usage of Internet services. Cyberstalking, in contrast, is monitoring a person's online behavior by means such as flooding their inbox with emails, leaving threatening comments on message boards frequently frequent, and other associated practices.

- **Malware Problems:** Malicious software comes in many forms, but it always has the same purpose: to compromise a company's network and enable criminal activity. Instances of this include gaining control of their systems and networks, stealing sensitive information or funds, intentionally damaging data or infrastructure, or committing multi-stage cybercrimes. Adware displays invasive adverts; rootkits enable hackers to take over a user's devices connected to the internet; keystroke loggers & spyware covertly record user activity; and so on.

[13] Halder, D., & Jaishankar, K. (2011). *Cyber Crimes against Women in India*. New Delhi: Sage Publications.

- **Ransomware Dangers:** Since ransomware is so common in cybercrime, it deserves particular attention, even if it is a subtype of malware. Ransomware encrypts data and files in order to either demand payment to decrypt them or to provide the victim very limited access to certain files. When the hacker wants to give the user back power, they'll demand payment in Bitcoin and another cryptocurrency.

- **Scams:** One of the more common types of online fraud is phishing, in which scammers send malicious links in an email in an effort to deceive their victims into giving up important information. Reputed brands send out phishing emails pretending to provide deals that are "too good to be true." Consequences can befall the receiver if they do not react promptly.
  If the consumer clicks on the link, a malicious website is going to be loaded into their browser that looks and feels like the actual company. Attempting to log in puts them at danger of having their information stolen or having malware installed on their system. These cybercrimes have been among the most effective, as 89% of firms had a significant email breach every year.

Trends And Patterns

A growing number of nations are worried about cybercrime as a result of the increased global connectivity brought about by technology (Horgan and colleagues, 2021). The information technology industry in India is booming, and the country is becoming more data dependent.
technological advancements are spearheading this transition to digital. While the country experiences record-high levels of internet usage, online shopping, & digital communication, cybercrime as well as other cyberthreats are also on the rise (Shah et al., 2022). In order to comprehend, assess, and address this intricate issue, this research delves in a statistical analysis of cybercrime trends and patterns in India[14]. Our research of the dynamic cyber threat landscape that the nation faces is summarized in this article. We want to use rigorous statistical analysis to uncover insights, trends, and patterns in cybersecurity. These results will shed light on the current situation of cybersecurity and guide the creation of more effective defenses against potential dangers.Due to its potential to close the divide between the two, this work is of utmost importance. By sifting through mountains of data on cybercrime, this study aims to provide a comprehensive picture of the risks that Indian citizens face online. Researchers are taking these measures with the expectation that policymakers, law enforcement, and cybersecurity professionals would benefit from evidence-based recommendations for securing the country's digital infrastructure. This research begins by exploring the history for cybercrime in India in order to provide the groundwork for analyzing current trends. After that, to make sure our findings are clear and easy to replicate, this study analyses the statistical methods utilized in the research. The essay continues with an in-depth examination of the most frequent forms of cybercrime, how cybercriminals remain ahead of the game, and the most common entrance points for assaults[15]. While navigating the complex web of cyber dangers, this research seeks to quantify the scope of the problem and expose the methodology behind cyber-attacks. Through an understanding of the statistical nuances, we want to offer stakeholders with the knowledge necessary to fortify India's cybersecurity defenses while building a strong digital ecosystem.

Motivations And Effects Of Cyber Fraud

The goal and need of the cybercriminal determine the motive for cybercrime. Common reasons for cybercrime include:

- **Financial Gain:** Financial gain is the driving force behind many cybercrimes, just as it is for many offline crimes.

- **A Political Goal:** Radical and extremist organizations utilize the Internet for propaganda and to launch attacks on the websites and networks of their opponents.

[14] Mali, P. (n.d.). IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1
[15] India Forensic. (2021, January 20). Case of Cyber Extortion.

- **Arousal Symptoms:** Engaging in sexually aberrant behavior is both detrimental and criminal. People satisfy their immoral urges and cravings by viewing porn sites.

- **Audiovisual:** While some cybercrimes use the internet to do evil, others use it for pure entertainment. Fun serves as a means to an end for cyber criminals like hackers.

- **Things That Inspire On An Emotional Level:** Cybercriminals who inflict harm out of rage often include those who have experienced betrayal in some way, whether it is a romantic partner, a boss, a business colleague, or a customer. Anger isn't quite as well-planned as revenge, which may be even more risky because to internet
The offender has more time to plot his moves, which usually makes him more evasive.
In a short amount of time, global connection has the potential to wreak devastation on every continent. The worldwide reach, anonymity, rapidity of crime, ephemeral nature of evidence, and high costs of investigations are some of the reasons why its nature and specific features have presented a unique challenge to investigators. Law enforcement agencies face numerous challenges, including but not limited to: policing, acquiring, developing, and retaining specialized personnel, bridging multijurisdictional boundaries, retaining evidence, deciphering encryption (a complex process), proving identity, coordinating investigative activities, and improving the reporting of internet crime. In today's developed world, almost everyone has a computer and internet connection[16]. Many people rely on cybercafés or other public spaces to use the internet, and children learn to use PCs at a young age as well. Therefore, in any modern, developing civilization, the significance of technology and networking is paramount. A theoretical framework provides an explanation for the phenomena under investigation, while a conceptual framework organizes what has been learnt to best describe the phenomenon's natural evolution. The ideas, concepts, and research results that make up the theoretical framework are all very relevant to the current study. It helps the researcher understand the findings better. The investigator has made an effort to construct a theoretical framework pertaining to cybercrime. In order to comprehend the cyber domain and the technology that profoundly affects global relations, such a theoretical framework is essential.

Analysing Cybercrime Statistics In India

To effectively safeguard electronic ecosystems in the ever-changing realm of cybersecurity, it is necessary to comprehend cybercrime patterns and trends. This section, "Review of Literature," elaborates on our understanding of cyber threats in India by critically examining prior scholarly works. For our study, it serves as a guide.
By shedding light on the nature, scope, expression, and dynamics of criminal behavior, Nag et al. (2022) argue that interdisciplinary research has transformed traditional approaches to investigating crimes.
In order to monitor criminal events, government organizations and police agencies nowadays utilize intricate systems to capture exact data together with spatial-temporal information. In order to forecast time series data, the article introduces the Prophet model, that employs an additive technique. By highlighting non-linear patterns, seasonality, and the effect of holidays, the model is used to predict criminal behavior.
Big Data offers both obstacles and opportunities for enhancing crime prevention and investigation, as highlighted by the researchers (Subashka Ramesh and colleagues, 2021).
The suggested strategy proposes novel countermeasures against cybercrime, which is becoming more difficult to investigate due to the proliferation of big data. The findings should provide police agencies with a better grasp of criminal issues, enabling them to enhance resource allocation, operational monitoring, incident prediction, and policy optimization. In order to better prevent and identify crimes, this paper highlights the usefulness of computational approaches for analyzing big, unstructured information and argues for the integration of cutting-edge machine learning, data mining, and computer modeling within criminal investigations.
Patterns & trends in cybercrimes and cybereconomic crimes were studied by Rajput and Rajput (2020). The research primarily focused on gender distribution, criminal characteristics, and crime registration. Cyber economic crimes make up the great majority of cases in the two most cybercrime-prone states in India,

[16] The Citizen. (2021, January 21). Trolls Target Women: Dealing with Online Violence.

Maharashtra and Mumbai, according to case studies. This research elucidates the regional variations of cybercrime in India by comparing the findings with six other metro areas and utilizing information from 2002 to 2016.
The multi-faceted discipline of cyber-criminology has lately shifted its emphasis from rehabilitation to prevention and prediction (Farsi et al., 2018). In specifically, it examines how governmental organizations dealing with crime prevention and control may use quantitative approaches, such as machine learning, to get strategic insights. In order to assist authorities and businesses cope with online risks, the discussion continues with an analysis of cybercrime trends. With a focus on data mining and predictive analysis, this paper summarizes machine learning techniques used in cyber-crime investigations.

- **Cybercrime rate Per lakh**

In terms of cybercrime rates per lakh population, the following information includes all states and union territories of India for 2020, 2021, and 2022. The data presents a mosaic all cybercrime occurrences, highlighting variations among states as well as trends over time. This data is the foundation of our study, enabling us to conduct precise countrywide analyses of cybercrime trends and patterns. By examining these rates and their fluctuations, our study aims to illuminate the dynamics of cybercrime. Our goal is to give a more detailed understanding of cybercrime's frequency and regional differences in India.

State/UT	Mid-Year Projected Population (in Lakhs)	Cybercrime rate Per lakh in 2020	Cybercrime rate Per lakh in 2021	Cybercrime rate Per lakh in 2022
Andhra Pradesh	530.3	3.58	3.54	4.41
Arunachal Pradesh	15.5	1.94	3.03	0.90
Assam	354.9	9.95	13.65	4.88
Bihar	1255.3	1.20	1.13	1.29
Chhattisgarh	299.5	0.99	1.18	1.47
Goa	15.7	2.55	2.29	5.73
Gujarat	709.3	1.81	2.17	2.00
Haryana	299.7	2.19	2.08	2.27
Himachal Pradesh	74.4	1.32	0.94	1.03
Jharkhand	391.4	3.08	2.43	2.47
Karnataka	674.1	15.93	12.07	18.63
Kerala	356.8	1.19	1.75	2.17
Madhya Pradesh	858.9	0.81	0.69	0.96
Maharashtra	1257.4	4.37	4.42	6.56
Manipur	32.0	2.47	2.09	0.56
Meghalaya	33.3	4.26	3.21	2.25
Mizoram	12.3	1.06	2.44	0.08
Nagaland	22.2	0.36	0.36	0.18
Odisha	460.8	4.19	4.42	4.30
Punjab	306.0	1.24	1.80	2.28
Rajasthan	804.4	1.68	1.87	2.28
Sikkim	6.8	0.00	0.00	3.82
Tamil Nadu	767.1	1.02	1.40	2.71
Telangana	379.5	13.24	27.15	40.31
Tripura	41.2	0.83	0.58	0.73
Uttar Pradesh	2340.9	4.74	3.77	4.32
Uttarakhand	115.6	2.10	6.21	4.84
West Bengal	987.6	0.72	0.52	0.41
A&N Islands	4.0	1.25	2.00	7.00
Chandigarh	12.2	1.39	1.23	2.21
D&N Haveli and Daman & Diu	12.0	0.25	0.42	0.42
Delhi	211.0	0.80	1.69	3.25
Jammu & Kashmir	135.4	0.89	1.14	1.28
Ladakh	3.0	0.33	1.67	1.00
Lakshadweep	0.7	4.29	1.43	1.43
Puducherry	16.2	0.62	0.00	3.95
TOTAL ALL INDIA	**13797.5**	3.63	3.84	4.78

(Table-1Cybercrime in india from 2020-2022)

- For 2020, 2021, and 2022, this data set summarizes the rate for cybercrime per lakh population of India[17], disaggregated by union territory and state. When we look at the data, we see that many of the results match the goals of the study.

- The incidence of cybercrime varies greatly among states. As an example, in 2020, the rate in Telangana was 13.24%, but by 2022, cybercrime had increased to 40.31%. Karnataka exemplifies the variation in cybercrime rates between states by seeing a substantial rise from 15.93 in 2020 to 18.63 in 2022.

- Looking at the increase or decrease in cybercrime rates during the past three years might provide us with valuable insights. Cybercrime patterns remained dynamic throughout the study period, as shown by notable shifts in places like Assam and Kerala.

- Further investigation is needed on potential vulnerabilities in smaller territories like as Lakshadweep and A&N Islands due to their relatively high cybercrime rates per lakh people.

- Cybercrime is prevalent in some states, such as Maharashtra, Delhi, and Telangana, which raises the possibility that economic and technological factors contribute to this problem. The data provided here establishes a foundation for the analytical section of the study, which aims to examine patterns and trends throughout the rate for cybercrime across various places in India.

Types Of Cybercriminals

There is a vast variety of cybercriminals out there, each with its own unique methods of operation and agendas. They are not a unified front, but rather a patchwork of disparate organizations and individuals pursuing different goals in different ways. From local "lone wolves" to foreign "state-sponsored groups" that undertake organized, highly targeted attacks, cybercrime encompasses a wide range of behaviors[18]. What follows is an examination of the many motivations and tactics used by cybercriminals. A hacker is a criminal who gains unauthorized access to computer systems and networks. Many things motivate hackers, but two of the most common are celebrity and money. In order to get illegal access, steal sensitive information, or stop operations, these bad actors exploit security weaknesses. The motivation behind identity theft, which involves the use of personal data, is financial gain. This kind of person may use tactics like phishing and malware assaults to cause their victims a lot of emotional and financial distress. Lastly, cyber terrorists aim to harm vital infrastructure in order to inspire fear; their actions are usually motivated by political or religious fanaticism. These individuals or groups employ cyberattacks as a form of intimidation and extortion. Critical infrastructure and government entities are their targets.

Hackers

Typically, when people hear the term "hacker," they envision an enigmatic figure hunched over a computer, swiftly penetrating networks. However, there are many nuances to the reality. At their core, hackers are those who actively seek for and exploit vulnerabilities in computer systems and networks with the intent to steal data or render them inoperable. There are malicious hackers followed by there are those inquisitive ones who are always trying to penetrate more and harder security systems. No matter their motivations, hackers pose a real and pervasive threat, which is why stringent cybersecurity measures are required.

Deceitful Individuals

Theft of personal information is another major tactic used by hackers. A key component of their activities is the theft of sensitive personal data, which they often engage in for financial gain. They could disguise their true identity, conduct identity fraud by assuming another person's identity, or steal credit cards. Victims of identity theft can endure severe emotional and financial hardship as a result of the ordeal. The prevalence of freely

[17] Statista. (2021, January 21). Digital population in India as of January 2020.
[18] Internet and Mobile Association of India. (2021, January 28). India Internet 2019.

available personal data online makes robust data protection and personal attention all the more important in light of the prevalence of identity theft.

Online Threats

Cyberterrorists are the most dangerous kind of cybercriminal. When launching cyberattacks, these terrorists often aim for critical infrastructure and networks. They represent a threat because of the chaos and fear they want to inflict; their motivations might be political or ideological. The reality of this threat has been shown by several high-profile incidents of cyber terrorism in recent years. Cyber terrorism is a severe and widespread problem, as shown by attacks on Iranian gas stations and large-scale hacking on Danish power businesses.

Common Tactics Used By Cybercriminals To Do Cyber Fraud

Criminals that operate in the cyber realm use a wide variety of tactics while committing crimes online. In order to devise effective defensive strategies, it is helpful to understand these methods. Distributed denial of service (DDoS) attacks, virus distribution, and phishing are common tactics used by cybercriminals[19]. Phishing campaigns use a wide range of tactics, such as phone calls, email (vishing), text (smishing), as well as targeted spear phishing, to spread malicious links and trick victims into giving important information. Malware dissemination, meanwhile, involves inserting harmful software onto customers' computers using email attachments or executable files, and sometimes employing social engineering tactics to trick individuals into infecting their personal devices. On the other hand, distributed denial if service (DDoS) attacks include overwhelming a service or site with traffic to the point where it becomes inaccessible to real users.

The Impact Of Cybercrime On Businesses And Individuals

Cybercrime may have far-reaching effects for both individuals and corporations. Many people have lost money, had their reputations tarnished, and experienced emotional distress because of cybercrime. Significant monetary losses for businesses could result from cybercrime. Companies may find themselves in a precarious financial position due to the sudden demands for ransom, revenue loss, and costs linked with breach remediation. In 2020, ransomware assaults cost companies over $400 million, while identity theft cost them around $112 billion over six years. But the bottom line isn't the only thing cybercrime impacts. Reputational harm to a business may result in less trust from customers and negative stories in the media. An further issue is that cybercrime, or identity theft specifically, may have a significant impact on the mental health of victims. The consequences for individuals and businesses of intellectual property theft may be far worse. Strong laws and regulations, such as the Cybersecurity Act, must be established and maintained by governments in order to effectively combat cybercrime. Common elements of these statutes include rules for the abbreviation and description of cyber-related offenses, guidelines for their investigation and prosecution, and standards for both.

Case Studies

Cybercriminals' strategies and potential responses may be better understood by analyzing high-profile cybercrime occurrences and their subsequent aftermath. The Sony hack and the Melissa virus are two examples of incidents that show how cyber dangers are always changing and how important it is to keep up cybersecurity measures. For example, the **1999 Melissa virus** epidemic highlighted the need of antivirus systems and the dangers of opening attachments in emails. At the same time, even major companies may be targeted by cyber extortionists, as the **2014 Sony hack** demonstrated[20]. The need of constantly improving defensive methods to prevent future events is highlighted by understanding the historical and economic effects of these occurrences. Cybercrime is becoming an increasingly serious danger to economies throughout the globe, with estimates putting the total cost at $10.5 trillion by 2025.

[19] National Crime Records Bureau. (2021, January 28). Crime in India- 2018.
[20] National Crime Records Bureau. (2021, January 28). Crime in India- 2018. Retrieved from https://ncrb.gov.in/crime-india-2018

The data breach at Target impacted more than 40 million customers and exposed sensitive information such as credit card numbers, expiration dates, CVV codes, and encrypted PINs. In addition to email addresses and phone numbers, the stolen data includes the names and addresses nearly 70 million customers. As a result of the hack, Target suffered substantial financial losses. It cost money to conduct investigations, keep tabs on customers' credit, as pay to resolve legal disputes. Furthermore, due to the catastrophic harm done to the company's reputation, both sales and customer confidence collapsed. Target quickly countered the assault by disabling the infection, bolstering its cybersecurity systems, and implementing stricter access limits for third-party providers. In addition to spending $100 million to fortify its cybersecurity systems, company executives assured affected clients that they would provide free credit monitoring and identity theft protection. Beyond the many lawsuits filed against the company by shareholders, customers, and financial institutions, Target's chief executive officer & chief technology officer resigned after the attack.

- **WannaCry Ransomware Attack:** Hundreds of thousands of personal computers across the world were attacked with the WannaCry ransomware early May 2017. This spyware encrypts data and demands Bitcoin as ransom, taking advantage of a Windows vulnerability. The assault demonstrated the extensive damage that ransomware is capable of inflicting by impacting hospitals, companies, and government entities.

- **Equifax Data Breach:** The credit reporting company Equifax was hit hard by a massive data hack in 2017. Of 147 million people, sensitive information including names, SSNs, and dates of birth was leaked. This incident demonstrated how sensitive personal information is and how serious the effects of identity theft may be.

- **Business Email Compromise (BEC) Scam on Toyota Boshoku Corporation:** In 2019, a BEC fraud targeted Toyota Boshoku Corporation, one of Toyota's subsidiaries. The corporation lost about $37 million when cybercriminals stole their identity and pretended to be a reputable business partner. This episode demonstrated how sophisticated and costly BEC assaults on major companies can be.

- **SolarWinds Supply Chain Attack:** A large number of businesses and government entities were affected through the SolarWinds supply chain assault that occurred in late 2020. Attackers compromised SolarWinds' Orion platform by inserting malicious malware inside a software update. Because of this, they were able to infiltrate SolarWinds client networks and steal a lot of data.

- **Pune Citibank MphasiS Call Center Fraud:** Some former workers of the business process outsourcing (BPO) division of MPhasiS Llc MsourcE stole Rs 1.5 crores from Citibank customers in the United States. "Data Protection" was only one of several issues brought up by this cybercrime case[21].
  "Unauthorized Access" to consumers' "Electronic Account Space" was clearly used to conduct the crime. "Cyber Crimes" is the proper category to assign it after careful consideration.
  Since any offense under the Indian Penal Code (IPC) that involves the possession of "Electronic Documents" may be seen as a crime involving the use of "Written Documents," ITA-2000 becomes flexible enough to handle the features of crime that aren't governed by ITA-2000 but are covered by other laws. This means that the terms "cheating," "conspiracy," "breach of trust," etc., are relevant not just to the aforementioned case but also to the relevant clause of ITA-2000.
  The crime is acknowledged under both Section 66 & Section 43 of the ITA-2000. Therefore, those responsible face jail time, fines, and victim damages up to a cap of Rs 1 crore per victim, with the "Adjudication Process" as a possible avenue for redress.

- **SONY.SAMBANDH.COM CASE:** The year 2013 saw India's first cybercrime conviction. The story starts with a complaint filed from Sony India Pvt Ltd, the proprietor of the website www.sony-sambandh.com, which

[21] Pasricha, M., & Japleen, (2019). "Violence" online in India: Cybercrimes against women and minorities on social media.

specifically targets Non-Resident Indians. After making an online payment, non-resident Indians may have Sony items sent to friends and family in India[22].

Products will be sent to the designated recipients by the firm. An individual placed an order for a Sony Color Television and a pair of cordless headphones in May 2002 under the name of Barbara Campa, as revealed in the cybercrime case study. She paid with her credit card and asked that the items be sent to Arif Azim at Noida. The transaction was finalized once the credit card company officially cleared the payment. The firm sent the goods to Arif Azim after making sure they had followed all the necessary due diligence and inspection processes.

Digital images were captured by the firm at the moment of delivery, showing Arif Azim accepting the item. At that point, the deal was considered concluded. However, after 1.5 months, the credit card company notified the business that the purchase had been made without authorization as the rightful owner had disputed responsibility. The business went to the CBI with a grievance over internet cheating, and the bureau filed a case under Sections 418, 419, and 420 in the Indian Penal Code. Arif Azim was taken into custody after an investigation into the situation. Arif Azim, according to investigations, obtained the American customer's credit card data while working in a Noida contact center and then used it fraudulently on the business's website.

In this unique instance of cyber fraud, the CBI was able to retrieve a color television and a cordless earphone. Because the CBI possessed proof in this case, the accused had no choice but to acknowledge guilt. It is the first conviction for cybercrime in India, and Arif Azim was found guilty under Sections 418, 419, and 420 in the country's penal code.

But the court believed a more moderate stance was necessary since the defendant was a young man of 24 years old and a first-time offender. As a result, the accused were granted a one-year probationary sentence by the court. The whole country is watching this decision with bated breath. In addition to being the first conviction involving cybercrime, it has shown that some types of cybercrime not addressed by the Information Technology Act of 2000 may be efficiently prosecuted under the Indian Penal Code. Second, everyone should be aware that the law is not to be trifled with when faced with a ruling like this.

- **The Bank NSP Case:** The engagement and subsequent marriage of a bank management trainee is one of the most high-profile examples of cybercrime. The case involved Bank NSP. Using the company's computers, the pair exchanged several emails. She sent letters to the boy's international clientele using phony email accounts like "indianbarassociations" after the couple split up[23]. To achieve this, she used the computer system at the bank. Following a significant drop in business, the boy's firm decided to sue the bank. The emails sent via the bank's system were found to be the responsibility of the bank.

- **Andhra Pradesh Tax Case:** Officials from the department obtained laptops used by the suspect in a single of the several cyber fraud cases throughout India, exposing the dubious practices of a renowned Andhra Pradesh businessman[24]. Investigators from the Vigilance Department apprehended the proprietor of a plastics company and retrieved 22 million rupees in cash from his residence. In the ten days that followed, they pressed him for an explanation about the missing funds.

  The accused assumed his crime would go unnoticed until he supplied 6,000 vouchers as proof of trade validity; nevertheless, upon closer examination of the vouchers and the contents on his computers, it became clear that they were all created after the raids. Accused utilized computerized vouchers to falsify sales records and avoid paying taxes; it was subsequently discovered that he was really operating five enterprises under a single name.

[22] Trend Micro. (2014). The Hack of Sony Pictures: What You Need to Know.
[23] The Bank NSP Case Study. (n.d.)
[24] Dubious tactics of a prominent Indian state tax official. (n.d.). Retrieved from https://www.indiancybersecurity.com/case_study_andhra_pradesh_tax_case.php#:~:text=Dubious%20tactics%20of%20a%20prominent,sleuths%20of%20the%20Vigilance%20Department

References

[1] Electronic Frontier. (2000, March). The Challenge of Unlawful Conduct involving the use of the Internet – A Report of the President's Working Group on Unlawful Conduct on the Internet. Retrieved from http://www.usdoj.gov/criminal/cybercrime/kvd0698.htm#Q2
[2] Diwanji, S. (n.d.). Total number of cyber-crimes reported across India from 2012 to 2018. Statista. Retrieved from https://www.statista.com/statistics/309435/india-cyber-crime-it-act/
[3] National Crime Records Bureau. (n.d.). Crime in India 2018 - Volume 1. Retrieved from https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf
[4] Grabosky, P. (2000, March 9-10). Cyber Crime and Information Warfare. Paper presented at the Translational Crime Conference, Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service, Canberra.
[5] Central Bureau of Investigation. (n.d.). Manual. Retrieved from http://www.cbi.gov.in/aboutus/manuals/Chapter_18.pdf
[6] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[7] Economic and Political Weekly. (1999, May 15). Dithering over Cyber Laws. Economic and Political Weekly, 34(20), 1151.
[8] Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electronic Commerce Research, 13, 41-69.
[9] Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.
[10] Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, *6*(1), 17-33.
[11] Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge.
[12] Halder, D., & Jaishankar, K. (2011). Cyber Crimes against Women in India. New Delhi: Sage Publications.
[13] Mali, P. (n.d.). IT Act 2000: Types of Cyber Crimes & Cyber Law in India-Part 1. Retrieved from [Link]
[14] India Forensic. (2021, January 20). Case of Cyber Extortion. Retrieved from http://www.indiaforensic.com/cyberextortion.htm
[15] The Citizen. (2021, January 21). Trolls Target Women: Dealing with Online Violence. Retrieved from https://www.thecitizen.in/index.php/en/NewsDetail/index/7/17330/Trolls-Target-Women-Dealing-with-Online-Violence
[16] Statista. (2021, January 21). Digital population in India as of January 2020. Retrieved from www.statista.com/statistics/309866/india-digital-population/.