ISSN: 2349-6002

A Critical Study in Mordern Perspective of Cyber Crime in India

Dr Jatin P. Bhal
Assistant Professor, Maharani Shree Nandkuvarba Mahila Arts & Commerce Collage, Bhavnagar, Gujarat
doi.org/10.64643/IJIRTV12I5-191339-459

***Abstract*—Computer technology has drawbacks in addition to its benefits. Despite the fact that computers speed up and simplify life, they are also vulnerable to the deadliest kind of criminal activity, known as "Cybercrime." Whole companies and governmental operations would all but vanish without computers. A growing number of people are able to use and, more importantly, depend on computers as part of their daily lives due to the widespread availability of affordable, potent, and user-friendly computers. As businesses, governmental organizations, and individuals grow increasingly dependent on them, so does the dependence of criminals. Preventing cybercrime necessitates analyzing their actions in detail and being conscious of the effects they have on society at large. Consequently, the present paper provides a methodical comprehension of cybercrimes and their impact on various domains, including socio-economic, political, consumer trust, adolescence, and future developments in cybercrimes.**

***Index Terms*— Cyber, Crime, Technology.**

I. INTRODUCTION

Cybercrime is a broad term that includes everything from denial-of-service attacks to electronic cracking, where computers or computer networks are used as a target, a tool, or a place for unlawful activity. It can also be used to describe traditional crimes where criminal activity is facilitated by computers or networks1. Cybercrime has the ability to stop any railway where it is, divert aircraft by sending out false signals, give critical military information to foreign nations, block e-media, and bring down any system in a matter of seconds.With an emphasis on the threat that cybercrime poses to India, the goal of this study is to examine some of the components, implications, and opportunities of cyber technology. In order to handle it, efforts have been made to look at India's legislative framework. First, it is necessary to specify the parameters of the term "crime." Therefore, there is little question that "crime" is a universally relative phenomenon that has existed in almost every community from antiquity to the present. Every culture has its own definition of what constitutes criminal activity and conduct that is punishable by the express will of the political community in charge of the society, which is always impacted by the social, political, religious, and economic values of that society. Therefore, since the beginning of time, the entire consequence of these rules has influenced and defined the behaviour that carries "penal responsibility."

Interestingly, the kinds of criminals that commit crimes have changed along with the concept of crime due to the development of information technology. The notion of crime in Indian society has historically been shaped by religious interpretation, especially in the past. During this time, religion completely dominated. It is believed that divine force is responsible for all social and political events, including "crime." The Demonological Theory of Crime Causation emerged at this time.

Throughout the Middle Ages, there were periods of renaissance and restoration, which gave "crime" a novel and modern appearance. During this period, new ideas in the study of crime were developed, including utilitarianism, a positive outlook, analytical thinking, natural justice principles, Lessie Fairy's ideas, hedonistic philosophy, and pain and pleasure theory. Later times saw a predominance of logical thought and prepared the way for the scientific and industrial revolutions.

II. CATEGORIES OF CYBER CRIME

Data Crime

Interception of Data

An attacker tracks the flow of data to or from a target in order to gather information. This attack may be conducted to collect information for a subsequent episode, or it may be used to obtain information for its ultimate goal. Usually, this attack involves sniffing network traffic, but it may also involve monitoring other data streams, like radio. The attacker typically maintains regular communication and remains passive. Nevertheless, in other cases, the attacker might attempt to alter the type of data transmitted or begin building a data stream. This attack differs from previous data collection techniques in that the attacker is not the intended recipient of the data stream in all of its forms. The attacker is observing and gaining access to specific data conduits (such network traffic), in contrast to certain other data leaking attacks. Attacks that collect more qualitative data, including conversation volume, which is not conveyed through a data stream, stand in contrast to this.

Modification of Data

To prevent data from being altered or viewed while in route, communications must be kept confidential. A malicious third party could conduct a computer crime in a distributed environment by tampering with data while it moves between locations. In a data modification attack, an unauthorized party on the network intercepts data while it is in transit, changes certain parts of it, and then retransmits it. An illustration of this would be altering a financial transaction's dollar amount from $100 to $10,000. In a replay attack, an entire collection of legitimate data is repeatedly added to the network. For instance, a valid $100 bank account transfer transaction might be made 1,000 times.

Theft of Data

This phrase is applied when data is unlawfully taken or acquired from a business or another person. Passwords, credit card numbers, social security numbers, and other private company information are examples of user information that is frequently used. Since this information was obtained illegally, the individual who stole it is probably going to face the worst legal penalties possible when they are caught.

III. NETWORK CRIME

Interferences in Networks

Network Entering, sending, erasing, deteriorating, altering, or hiding network data in order to interfere with a computer network's ability to function.

Sabotage of Networks

Incompetent managers, or "Network Sabotage," are trying to carry out the responsibilities of those they are typically in charge of. One or more of the previously listed causes may be the cause. On the other hand, Verizon might be using network problems as a ruse to get the federal government to take action in the interest of public safety if they are abusing the help the children line to impede first responders. Therefore, if the federal government forces these people to return to work, what good are unions and strikes?

IV. ACCESS CRIME

Unauthorized Entry

From the inside, "Unauthorized Access" explores the computer cracking underground. Several locations in the US, Holland, and Germany were used for filming. "Unauthorized Access" looks at the people who use computers, trying to separate reality from the representation of the "outlaw hacker" in the media. Transmission of Viruses malicious software that joins other applications. (Malicious software that harms a victim's system includes Trojan Horses, worms, viruses, time bombs, logic bombs, rabbits, and bacteria.)

V. TYPES OF CYBERCRIME

Telecommunications Service Theft

The "phone phreakers" set the stage for what has subsequently grown into a significant criminal industry thirty years ago. By getting access to a company's telephone switchboard (PBX), individuals or criminal groups can obtain dial-in/dial-out circuits and use them to make calls or sell call time to third parties (Gold 1999). Posing as a technician, getting an employee's access code fraudulently, or using Options for accessing the switchboard include software that

can be found online. Some skilled crooks build a loop between PBX systems to evade detection. Service theft includes things like stealing "calling card" information, charging calls to the calling card account, and illegally reprogramming or counterfeiting stored value phone cards.

VI. COMMUNICATIONS IN FURTHERANCE OF CRIMINAL

Regarding spiracles

Similar to how lawful businesses and governmental entities depend on information systems for communication and documentation, technology also supports the operations of criminal groups. Organized drug trafficking, gambling, prostitution, money laundering, child pornography, and the trafficking of weapons (in those jurisdictions where such operations are prohibited) are all made possible by telecommunications equipment. If encryption technology is employed, law enforcement may not be able to access criminal conversations. Recently, there has been a lot of media coverage on the creation and dissemination of child pornography over computer networks. According to Grant, David, and Grabosky (1997), these materials can currently be imported over national borders at the speed of light. IRC and WWW infrastructure demand a minimal level of coordination for the more overt forms of online child pornography. However, it seems to be limited to human activity.

Piracy in Telecommunications

Digital technology has made it simple to reproduce and distribute paper, graphics, music, and multimedia combinations. Many people have given in to the temptation of using protected content for their own use, for free distribution, or even for sale at a reduced cost. This has caused a great deal of fear among copyrighted material owners. The United States, Information Infrastructure Task Force (1995, 131) estimates that copyright infringement costs the business between $15 and $17 billion annually. When creators of works in any media are unable to make money off of their efforts, it can have a chilling effect on creative activity generally in addition to causing financial loss.

Distribution of Harmful Content

There is a lot of stuff on the internet that some people find offensive. Examples include instructions for making explosive and incendiary devices, racial propaganda, and sexually graphic literature. Telecommunications networks can be used for harassing, threatening, or intrusive communications, ranging from the classic obscene phone call to its modern manifestation in "cyber-stalking," which involves sending persistent messages to an unwilling recipient.

Tax evasion and electronic money laundering

Computerized money transfers have long been used to help hide and transport illegal activities. It will be simpler to conceal the source of illicit funds thanks to emerging technologies. Legally obtained income may also be easier to conceal from tax officials. Electronic cash transfers across numerous jurisdictions at lightning speed will no longer be limited to large financial firms. The expansion of alternative banking networks and unofficial financial institutions may make it possible to evade central bank supervision. However, in nations that have them, it might also make it simpler to get around reporting requirements for cash transactions. Traditional underground banks, which have prospered in Asian nations for many years, will have even greater capacity because to telecoms.

Extortion, Terrorism, and Electronic Vandalism

More than ever, complex data processing and telecommunications networks are essential to Western industrial society. Any of these compromised or damaged systems could have catastrophic outcomes. Whether driven by curiosity or retaliation, electronic invaders are at best inconvenient and have the potential to do great harm (Hundley and Anderson 1995, Schwartau 1994).

Illegal Interception of Telecommunications

Technological developments in telecommunications have created new opportunities for electronic eavesdropping. From the conventional monitoring of an unfaithful spouse to the most advanced forms of political and economic espionage, telecommunications eavesdropping has an expanding range of applications. Again, technical developments

lead to the creation of new vulnerabilities. The electrical impulses that a computer produces can also be intercepted. Cables could be used to create broadcast antennas. The law does not forbid remote computer radiation monitoring.

Fraud involving Electronic Fund Transfers

The likelihood of such transactions being intercepted and misdirected has increased along with the development of electronic payment transfer techniques. Both physically and electronically, legitimate credit card numbers can be blocked, and digital information on a card can be faked.

A criminal might steal telecom services and use them for fraud, vandalism, or to further a criminal conspiracy, just like an armed burglar might steal a car to make a rapid getaway. Combining two or more of the above-mentioned broad types of computer crime is known as compound computer crime.

VII. THE EFFECTS OF CYBERCRIME

Crime as a Negative Social Factor

A society without crime is a fiction, because crime is an unavoidable and pervasive part of social life. Some people may find the question "Why is there so much ado about crime?" annoying. Nobody can dispute that crime is a social phenomenon; it is ubiquitous and nothing new; it is one of the most fundamental tendencies of all human activity and one of the distinguishing traits of all past civilizations, whether they were civilized or not! It is crucial to keep in mind, nevertheless, that high crime rates are a reason for concern in society due to the possibility of social unrest rather than their inherent nature. Additionally, some persons suffer more severe consequences from crime than others. All of a victim's possessions could be taken away. Since they enable the fulfilment of many goals, safety, peace, money, and property are arguably fundamental values.

Impact of Cyber Crime over Teenager

Bullying over the Internet is currently the biggest fear among youngsters. The investigation found that youngsters under the age of eighteen are more vulnerable to and afraid of cyberbullying, which has increased in frequency over the past five years. It is turning into a concerning trend in our society. Teenage girls are the most frequent victims of cybercrime, according to study. Cyberbullying is a concern that emerges when someone receives bad images or comments, threats, or harsh feedback comments.

This is mostly achieved by utilizing the important technologies listed above, which are mainly available via the Internet. Instant messaging, chat, and other online harassment can be utilized. Cyberbullying is more likely to affect users of social networking sites like Facebook, Orkut, and Twitter. I believe that generally feared individuals can become depressed, humiliated, and dangerous. This evidence suggests that individuals who experience cyberbullying may get so sad that they resort to self-harm.

Cybercrime's Effect on Consumer Behaviour

Many generally open societies are now at risk of cybercriminal and cyberterrorist attacks, especially in commercial corporate activities, as a result of the information revolution and the strategic use of the Internet. Thanks to the growth of e-commerce, this shadowy business side has been dubbed cybercrime and has assumed many forms that change our perceptions of how we shop online. Businesses should understand that these risks to their internet businesses have strategic ramifications for their long-term prosperity. To preserve consumer trust in the Internet as a purchasing option, they should take the necessary actions to remove or significantly reduce these risks. These safeguards, known as "cyber security," were developed to preserve customer data and privacy while enabling worry-free shopping. It is necessary to create models that will allow companies to assess how cybercrime affects online customer confidence and react by leveraging the advantages of current cyber security developments. Given how these two facets of e-commerce affect online shoppers, companies need to make sure that their security protocols will ultimately prevail and that clients will keep using the Internet to fulfill their purchasing needs.

Emotional Impact of Cyber Crime

The study, the first to examine the emotional effects of cybercrime, reveals that victims frequently blame themselves for the attack and are most likely to feel irate (58 percent), irritated (51 percent), and fooled (40 percent). The prosecution of cybercriminals will result

in a sense of impotence and ironic reluctance to act, as just 3% and over 80% of respondents, respectively, do not think it will happen to them. "We tolerate cybercrime due to a 'learned helplessness,'" stated Joseph LaBrie, Ph.D., an associate professor of psychology at Loyola Marymount University. "It's like getting ripped off at a garage you don't dispute with the mechanic if you don't know anything about vehicles." Even when a situation is not satisfactory, people just accept it. Despite the psychological toll, the pervasive threat, and the prevalence of cybercrime, people aren't altering their behaviour; only 51% of adults say they would behave differently if they were a victim. A victim of cybercrime, "I never thought I would be a victim of such a crime, so I was emotionally and financially unprepared." I felt as though my entire family had been the victims of this horrible crime and that someone had broken into my house to get this information. At this point, I can't help but wonder if more data has been illegally collected and is just waiting to be used by the wrong people. The "human effect" section of the paper delves deeper into the small transgressions or white lies that consumers perpetrate against businesses, friends, family, and loved ones. Almost 50% of respondents think it's acceptable to download a single song, album, or film for free. According to 24% of respondents, it is acceptable or acceptable to discreetly monitor someone else's emails or browser history. Certain behaviors, such as downloading data, put customers at risk.

Impact of Cyber Crime over Youth

Cyber communication is the newest kind of engagement in society. Through email, text messaging, and social networking sites, users can communicate with people worldwide. Using laptops or other portable electronics, teenagers in particular spend a lot of time online every day.

Friendships

According to Family-rescource.com, 48% of kids think that their friendships benefit from the Internet. Young people can stay in touch with both real and virtual friends thanks to the growing popularity of social networking services. Having online contacts, according to some youngsters, gives them the courage to be who they are. An estimated 13 million youngsters use instant messaging apps, which let them communicate with their friends in real time. Through online communication tools, teenagers from all around the world can become friends.

Cyber Bullying

One negative consequence of teenage online communication is cyberbullying. On social media platforms, victims of cyberbullying are regularly the target of rumours and false information. Bullies may post inappropriate or embarrassing pictures of their victims. The use of abusive text messages is another aspect of cyberbullying. More than half of all American youths are victims of cyberbullying, according to the National Crime Prevention Council. In some severe cases, teens have committed suicide as a result of cyberbullying.

Sexual Solicitation

Sexual solicitation is becoming a serious issue for children who utilize online communication platforms. It could occur on social media sites or in chat rooms. Sexual solicitation is the term used to describe when an adult or a peer tries to establish a sexual relationship online. Teens may be pressured to view pornography, discuss sexual topics online, or divulge private information. More than 70% of people who get sexual solicitation online are girls. Teens should use caution while interacting with strangers in chat rooms or posting explicit images online.

VIII. UPCOMING CYBERCRIME TRENDS

The sharp rise in cybercrime is among the most alarming features. According to US Treasury Advisor Valerie McNiven, "last year was the first year when proceeds from cybercrime were bigger than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion."" Additionally, she said, "Law enforcement cannot keep up with the rapid pace of cybercrime." iv Now that experts have acknowledged the potential windfalls if properly utilized, it seems that the issue will only get worse in the upcoming years.

The relationship between organized crime and cybercrime has been the subject of much recent discussion. An unfavourable future is undoubtedly hinted at by such a combo. Traditional methods of

containing and neutralizing the threat seem pointless given that the majority of criminal organizations are situated in Eastern Europe, Russia, and Asia, where there are insufficient laws and enforcement. A CERT visiting scientist named Phil Williams provided a succinct summary of the circumstances.

A surge in sophisticated phishing attacks and other two-pronged identity theft techniques will undoubtedly be the result. For instance, utilizing contact centers to notify "customers" in advance of an issue and then sending follow-up emails asking for personal data. Many thirdparty data centres' accumulations of personal data will make them attractive targets for intrusion. It's easy to see thieves using data mining tools to find the most trustworthy clients or tailoring phishing emails to particular people based on their personal, financial, or medical information. Additionally, theft detection will become more automated. For instance, botnets will be utilized as enormous search engines to find private data like social security numbers and credit card numbers27 in addition to being used for spam and denial-of-service attacks. The controllers of the botnet will then receive payment for running queries against its "database."

Because of this, almost anyone may try their hand at the industry and become one of the increasing number of cybercriminals. Given its low learning curve, it ought to provoke discussion on the need for a fresh, non-traditional approach to crime prevention and treatment. A burglar, for instance, needs to know how to pick locks, know how to get around security systems, and have the guts to cross ethical boundaries in order to enter a property covertly. On the other hand, it seems that the ease of cybercrime is inversely correlated with the profits it makes, and these trends persist.

IX. CONCLUSION

Both criminals and regular users are still fighting for control of the Internet's future. There are many people who fear a cyber apocalypse, and there is an almost limitless scope of harm that widespread fraud may do. The awareness that the issues are being addressed, albeit slowly, should help to appropriately reduce these fears. Numerous benefits of the Internet have been demonstrated, which ought to be sufficient to prevent it from turning into a center of illegal activity and a haven for bad actors. The bulk of the effort must be done by private software suppliers and those who are capable of identifying and stopping fraud, even though the government has a significant role to play.Non-stressing procedures that need substantial involvement must automatically protect others. For security to be successful, it needs to be straightforward and efficient. In some respects, it is impossible to predict whether cybercrime will remain a problem in 10 years, but if the Internet is to keep expanding, cybercrime needs to be resolved to the point where it is comparable to, if not superior to, crimes that occur in the actual world.

REFERENCES

[1] Pushparaj Pal, Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India, ResearchGate (Jan. 8, 2022, 12:43 PM), https://www.researchgate.net/publication/337818340_Cyber_Crime_An_Analytical_Study_of_Cyber_Crime_Cases_at_the_Most_Vulnerable_States_and_Cities_in_India

[2] Shivesh Shrivastava, A study of Emerging Issues of Cyber Law, CALR, (Jan. 8, 2022, 12:13 PM), https://calr.in/a-study-of-emerging-issues-of-cyber-law/

[3] Rita Dewanjee and Dr. R. Vyas, Cyber Crime: Critical View, vol.5 Issue. 1, International Journal of Science and Research, 85-87, (2016), https://www.ijsr.net/get_abstract.php?paper_id=NOV152579.

[4] Singh, Pushpinder, and Kirandeep Kaur., Role of Social Networking Sites as a Component in Modern Social Structure: A Study on College Students, vol.10 no.4, International Journal of Education and Management Studies, Indian Association of Health, Research and Welfare, p.447., Dec. 2020.

[5] Akash Kori, Critical Analysis of Cyber Laws in India, iPleaders, (Jan. 8, 2022, 11:05 AM), https://blog.ipleaders.in/cyber-laws-in-india/.