Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 6, August-2018, ISSN 2230-7540

Cyber Crime Classification

Vivek Sharma[1]*, Dr. Babu Lal Yadav[2]

[1] Research Scholar, Sunrise University, Alwar, Rajasthan

[2] Professor, Sunrise University, Alwar, Rajasthan

Abstract - As we all know, this is an age in which the majority of activities are done via the internet, from online trading to online transactions. Because the internet is seen as a global stage, anybody may use its resources from anywhere. Few individuals have been utilising internet technology for illegal actions such as unlawful access to other people's networks, frauds, and so on. Cyber crime refers to these illegal behaviours or offenses/crimes involving the internet. The phrase "Computer Law" was coined in order to deter or punish cyber thieves.

As cybercrime continues to gain notoriety as one of the century's most troubling developments, governments, corporations, and the international community's dedication to combating this epidemic is unsurprising. Combating this ailment, however, will include recognising, diagnosing, and categorising cybercrime. Meanwhile, the phenomena of cybercrime has become well-known and characterised, with top-level categorization confined to a duality of "computer-assisted" and "computer-focused" cybercrimes. The categorisation of cybercrime is examined in this paper.

Keywords - cybercrime; cybercrime classification, Internet, Unauthorized access, Cyber crime, Cyber law, Cyberspace, Punish, Network.

---------------------------------x---------------------------------

INTRODUCTION

As far as most people are concerned, cybercrime is just another kind of criminal activity IT Act defines "cybercrime" as any illegal behaviour carried out on or via a computer, the internet, or any other kind of technology. Today, cybercrime is the most common kind of criminal activity in India, and it has a particularly damaging effect. The IT Act defines cybercrime as any illegal behaviour carried out on or via a computer, the internet, or any other kind of recognised technology. In today's India, cybercrime is the most widespread kind of crime, and it has a devastating impact. Criminals not only cause significant damages to society and the government, but they may also hide their identities to a large degree. Technically adept criminals engage in a variety of unlawful activities while using the internet. Computers and the internet are used in cybercrime, which includes any criminal activity that utilises these tools to perpetrate crimes.

Although the word "cyber crime" has been judicially defined in several Indian decisions, it is not defined in any Indian legislation or law. Increasing dependence on technology has led to an uncontrollable evil known as cybercrime. It is becoming more commonplace to use computers and other technological devices in our daily lives, and it has evolved into a desire to make life easier for users. It's a limitless, unquantifiable medium. Whatever the positive aspects of the internet are, it also has some negative aspects. If they are done via the use of a computer or the Internet, several traditional crimes may be classified as cybercrimes.

CYBERCRIME'S ORIGINS AND EVOLUTION

Everyone would be surprised to learn that the first successful computer was developed and that the computer was so large that it took up the entire room and was too expensive to run. The operation of these computers was incomprehensible to a huge number of individuals, and only a few experts had direct access to them and knew how to use them.

Computer technology has been around for a long time for obvious reasons. prohibitively expensive and out of reach for almost the entire population until IBM's introduction of its stand-alone "personal computer" in 1981, exposing many to the benefits of Data manipulation and access is rapid. that had previously only been realised by a select few. Personal computers were increasingly accessible and ubiquitous in India during the start of the twenty-first century, according to the USD Department. created the The purpose of the Internet was to build a network that could operate in the case of a disaster or conflict and securely convey data.. First, ARPANET was established. Then came TC Protocol, the WWW, and Hypertext. The internet was born. As the Internet's popularity has risen, so has the quality and variety of information available. Nevertheless, no one anticipated the potential dangers the internet would provide to criminals with advanced computer skills at the time.In India, the state-owned VSNL began providing internet services and the government removed VSNL's monopoly, allowing private operators to enter the market. In most common law jurisdictions, the process of criminalising human behaviour deemed to be harmful to the public takes time. Before undesired behaviours are categorised as "criminal," momentum built up through problem identification and pressures from special interest groups can easily last decades. In certain circumstances, "catalyst events" that capture public and legislative attention might speed up this process.

CYBERCRIME'S DEFINITION

"Criminal activities carried out through computers or the Internet," according to the Dictionary. "Those species of which the genus is the conventional crime, and where the computer is either the object or the subject of the criminal conductsays the definition. the following three definitions:

1. Any unlawful conduct that involves the use of a computer as a tool or as the object of the crime, i.e. any offence performed with the goal or methods of interfering with a computer's functionality.

2. Any computer-related incident in which a victim has suffered or may have incurred a loss. and a perpetrator has made or may have made a profit, either intentionally or unintentionally.

3. Any illegal, unethical, or inappropriate conduct involving the data processing and transmission in an automated manner is referred to as "computer abuse."

CYBERCRIME: ITS NATURE AND SCOPE

In other words, criminality is something that happens in society. To say that our attempts to prevent cybercrime are in futile is an understatement. What if we can't keep crime to a minimal in the actual world? How can we hope to do it in the virtual world, which is considerably more unreal, everlasting, and legally uncontrollable? On the other hand, the nature, scope, and definition of crime in a particular society change throughout time. No civilization can be devoid of crime in its entirety, since the idea of a society free of crime is a myth. As a consequence, society's values and norms have an impact on criminal behaviour.

An environment's level of complexity is determined by its civilization's complexity. verifying all of the components that influence and contribute to the outcome is essential. Having a basic knowledge of crime is essential to understanding how it affects society. Social, economic and political organisations must understand crime and the steps that may be done to avoid it. It is also necessary to consider the machinery in place to govern crime and delinquent behaviour in society when determining the scope of a crime and the type of the harm it causes. It is difficult to grasp and much more difficult to apply present legislation to the new complicated scenario that technology advancements have produced in society, creating new socioeconomic and political difficulties for government to handle.

CYBERCRIME'S CHARACTERISTICS

Traditional crime varies in various ways from cybercrime. In comparison to traditional crime, this crime has garnered severe and unrestricted attention as a result of the rise of Internet Technology. . As a result, it's crucial to investigate the unique characteristics of cybercrime.

1. **People with specialised expertise -** Because cyber crimes can only be perpetrated through technology, perpetrators must be extremely knowledgeable about the internet, computers, and the internet. Because cyber criminals are well enough to have a full grasp of how to utilise the internet, it is difficult for law enforcement to apprehend them.

2. **Problems due to geography —** Geographic boundaries in cyberspace are non-existent. In a matter of seconds, a While sitting anywhere in the globe, a cyber criminal may conduct crime in another part of the world. India's first hacker, for example, could compromise a system in the United States.

3. **Virtual World -** Cybercrime occurs in cyberspace, although the perpetrator is physically located outside of it. The culprit's entire illegal activities takes place in the virtual world.

CYBERCRIME CLASSIFICATION

The following is a list of common cyber crimes, some of which are widespread while others are not. Following are examples of cybercrime:

Cyber Pornography: "Pornography" refers to any work of art or literature that deals with sexual themes; the term comes from the Greek words "porne" and "graphein." Since each country has its unique set of norms and traditions, the term "pornography" is difficult to define and has no clear legal connotation. The legality of pornography varies widely from country to country. If you want to put it another way, cyber pornography is any of these things that is done on or over the internet: When cyberspace was born, conventional pornography was mostly replaced by online/digital content. A legal definition of pornography does not exist. Response of the general public and social norms to pornographic material.

Stalking on the Internet: In general, stalking entails pestering or threatening another individual. Cyber stalking is a type of stalking that is carried out through information technology over the internet. Cyber stalking is using the internet, e-mail, and chat rooms to track down someone. According to Wikipedia, cyber stalking is when an individual, a group of individuals, other electronic methods. False charges or claims of fact monitoring, All of the above scenarios are examples of threatening behaviour, such as identity theft, data or equipment damage, or solicitation of children for sex. Continuous stalking entails several different elements, all of which may or may not be considered legal in and of itself. Because the definition of cyber stalkings differs by location, it is not globally accepted. Professor Lamber Royakkers – according to him — "Cyber stalking" is defined as harassing or threatening someone using the internet or many electronic methods of communication on a regular basis. A cyber stalker is someone who uses the bulletin board, chat room, email, spam, fax, buzzer, or voice mail to harass someone else. Following someone, showing up at their home or place of business, etcare examples of stalking. It's difficult to give a detailed description of stalking because stalking acts are so diverse and must be seen in relation to one another."

Terrorism in the Digital Age: In today's world, terrorism is a highly complex topic. Terrorist acts against humanity have risen dramatically during the previous decade. Terrorism has hurt everyone, from the victims to the status of the nation as a whole. Because of the Cold War's conclusion, terrorism has now become a major concern for the whole world. Terrorist assaults against humanity have killed a significant number of people throughout the globe because state authorities are ill-equipped to confront or govern them. Terrorist attacks continue to occur despite several countermeasures adopted by both the United States and the international community. It's not uncommon for these devices to be developed to operate in the event of a normal terrorist attack. Terrorists' arsenals today include computers and the internet, since we live in a digital era.

Many economies have been thrown into chaos as a result of the current financial turmoil. There is no consensus on where the road ahead will take us. No matter how big or little a company was, technology was always there to help it survive. Technology has become a business enabler in a manner that is almost hard to perceive. When it comes to cyberwarfare, a new chapter has been added. Specialized cyber-attacks are known as cyber-terrorism. attacks with the goal of causing harm. It's a new menace with the potential to do a lot of harm. While we commonly identify terrorism with death, we must not neglect the critical consequences of cyber-terrorism, such as intimidation and coercion.

Hacking: Hacking is considered one of the most dangerous types of cybercrime. People's trust in information technology and the Internet has been stated to be eroded by hacking. Hacking a computer system has been portrayed as a threat that necessitates punitive legislation. A broad prediction like this is a little off the mark. Simply described, a computer hacker is someone who gains unauthorised access to another person's computer. Hacking is the act of gaining unauthorised access to another person's computer without their permission.Hacking is the unauthorised use of another person's computer. It's akin to tapping on the phone. Hackers identify the target computer program's flaws and then devise methods to get access to it. Antihacking solutions Prevention methods that may be used to keep a computer secure include those like 'Firewall' technology systems. safe from hackers. Hacking is prevented by a firewall, which acts similarly to a fire wall. In addition, intrusion detection systems will attempt to locate the hacker source.

In layman's terms, hacking is trespassing on a private computer. It is illegal to stay on someone else's property after entering it legally with the intention of intimidating, insulting, or annoying the person who owns it or to conduct an offence. It is also illegal to remain on someone else's property after lawfully entering it with the same motive. 96 trespassing is a felony in the eyes of the law. may result in a sentence of up to three months in jail or a fine of up to Rs 500, or both97. As a result, criminal trespass is a minor infraction.

Contaminants and Viruses: These viruses were distributed through unlicensed video games. The 'Lehigh' virus infiltrated the computer files of 'command.com' in 1987. 'Jerusalem,' one of the most widespread viruses, was released in 1988. Every Friday the 13th, this virus was triggered, and it attacked both '.exe' and '.com' files, as well as any applications that were executed on that day. Symantec released 'Norton Anti-virus' in 1990, which was one of the earliest anti-virus solutions made by a multinational corporation. There were 1300 viruses identified in 1992, a 420 percent increase from December 1990. T (DAME), a toolset for turning viruses into polymorphic viruses, was invented in this year. The 'Good Times' e-mail scam engulfed the computing world in 1994. The hoax warns of a harmful virus that may wipe a cleaning your hard disc with an email with the subject "Good Times" One of the most popular viruses at the time was dubbed "Word Concept," which propagated via Microsoft Word documents. There were three virus outbreaks in 1996 that impacted Microsoft Windows 95, Excel and Linux files: the "Staog," "Baza" and

"Leroux." The 1st virus to infect Java files was 'Strange Brew' in 1998. The 'Chernobyl' virus spread swiftly this year through '.exe' files as well. The virus was very damaging, affecting not just data but even the computer's chip.

Finance-related cybercrime: Cybercrime as a Threat to the Economyis described as "an economic crime perpetrated utilising computers and the internet," according to Price Waterhouse Coopers, which conducts economic crime surveys. Virus distribution, unauthorised file downloads, and the theft of Bank account numbers, for example, are examples of private informationare all examples. "A cyber crime is one in which a computer or computers, as well as the internet, play a central, rather than incidental, role in the crime."

According to the results of the GEC Survey 2011's ECI survey. In India, internet usage is quickly increasing. According to a recent (TRAI) survey, there are currently 354 million internet subscribers in the United States. 122 While the increasing usage of the internet provides cyber citizens with a variety of alternatives in many areas of life, In addition to providing pleasure and education, cybercrime has also emerged as a result. It's a new generation of tech-savvy people. con artists presents a whole new set of problems. Cyber crime was reported by 24% of respondents who prior year's reported financial crimes. We believe that this data alone demonstrates the seriousness of the threat of cybercrime to businesses. As a result of recent cyber-attacks on global corporations and financial institutions, an increasing Many organisations are falling prey to cyber-attacks, which is a worrying trend. Increasing e-business volume and internet and e-commerce usage might be two plausible reasons for the sudden rise in cyber crime.

Phishing and Vishing: When a person or company pretends to be someone or something else in an apparent official electronic communication like an e-mail or an instant message in order to fraudulently obtain sensitive information like passwords and credit card numbers, that is phishing, a type of social engineering in computing. Phenomenon known as phishing refers to the use of ever more sophisticated baits to attract people into handing over personal and financial information. Falsely representing oneself as a well-known company in order to get personal information from the recipient in order to commit identity theft. User information, such as passwords, credit card numbers, social security numbers, and bank account details, are sent to a website where they must be updated by the genuine organisation. A fake intended to steal the user's personal data, the website is the opposite.

Attack on the Service: Spam attacks are when a criminal sends an excessive amount of unsolicited email to a victim's computer or email account, depriving him of the services he is legally authorised to receive or provide. By flooding a network with meaningless traffic, a denial-of-service tries to knock the attacker down the whole system.. Many DoS attacks take benefits of flaws in the TCP/IP protocols, such as the POD and Teardrop attacks.

A normal connection begins with the user sending a message to the server requesting authentication. The authentication approval is returned to the user by the server. The user accepts this approval and is subsequently granted access to the server. In a denial of service attack, the user floods the server with login requests, overloading it. Because all queries have fake return addresses, the server is unable to locate the user when sending the authentication approval. Before disconnecting the connection, the server waits a long period, often more than a minute. When the connection is closed, the attacker sends another batch of faked requests, and the process repeats itself, tying up the service indefinitely.

Theft of Data: debit cards' data was stolen in a worldwide conspiracy orchestrated, of the United States, and two Russian accomplices in January 2009, when they hacked computers at Hannaford Bros. Authorities have labelled Gonzalez as one of the nation's (US) top cybercrime masterminds, according to reports. In our digital age, data and information are precious assets. It is important to note that information economic property includes everything from business secrets to technological know-how to designs to music to films to books. The creation and compilation of data and information takes money, time, effort, and ingenuity.

Data mucking: A computer may be tampered with before or after the data is input. Anybody who is engaged in the process of entering data into a computer file, whether it be a person, a computer virus, or the developer of the database or programme, may edit the data. An individual or organisation that is engaged in the generation or transmission of data is known as a "data processor." could be the offender. Because it needs absolutely little computer knowledge, this is one of the easiest ways to perpetrate a computer-related crime. Despite how simple it is to commit the crime, the cost can be substantial.

Attacks of the Salami: A salami assault is a sequence of smaller data security breaches that combine to become a larger breach. A salami assault, for example, could be a bank fraud in which an employee steals a little amount of money from multiple accounts. Salami-related crimes are notoriously difficult to identify and track. Financial crimes are carried out using these attacks. The trick here is to make the change so minor that it would go completely unnoticed in a single scenario. A bank employee programmes the bank's servers to deduct a little amount of money from each customer's account. This illicit debit will most likely go unnoticed by the account holder, but the bank employee will profit handsomely every month.

Bombings by email: Abuse on the internet that includes sending large quantities to one particular address with the hope of overflowing the inbox or overloading the server is known as an e-mail bomb. There are many similarities between the practise of sending an email or mail bomb and the practise of actually delivering an explosive device. Sending spam to a large number of recipients using the victim's email address is one way to commit mail bombing. One of the Russian online communities has a different definition for "mail bomb." Computer systems are the intended target of a mail bombing denial of service attack.

Spoofing e-mails: Sender addresses and other header information may be altered to make a message seem to have come from another source, a practise known as e-mail spoofing. Using the email spoofing method may help spam and phishing hide their genuine origins. Unintentional users might make an email seem to have come from someone other than the intended recipient. using different methods. In the context of website spoofing, which mimics a reputable and well-known website but is run by a third party, either for fraudulent or critical objectives,"

Logic Bombs: A logic bomb is a piece of programming code hidden or purposely added into a computer programme that is meant to execute (or "explode") when specific conditions are met, such as the passage of time or the failure of a programme user to reply to a programme command. Logic bombs are typically seen in malicious software, such as viruses and worms, that execute a payload at a pre-determined time or when a certain condition is satisfied. A virus or worm can utilise this strategy to acquire speed and spread before being detected.. Trojans that activate on specific dates are commonly referred to as "time bombs." It's a Trojan horse or Slowly-acting malware on a computer. In the event that a logic bomb is "detonated," it might display or print a bogus message or delete or distort data, among other things. These are events-driven applications

Theft of Internet Time: Using someone else's internet hours is referred to as theft of internet hours. The IT Act of 2000, establishes civil responsibility for this offence. It states that whoever charges the services of a person to the account of another person without authorization from the computer's owner or other person with administrative authority over the machine,computer system, or computer network by Computer tampering or manipulation is punishable by a fine of one crore rupees for the person in charge of the office. Typically, in these types of Internet thefts, another individual consumes the victim's surfing time. This is accomplished by obtaining the login credentials.

Intellectual Property Rights-Related Cybercrime: In the Internet, a A computer or a group of computers is identified by its domain name. To put it another way, a domain name is the online equivalent of a physical address. A domain name is a unique identifier assigned to a computer or other Internet-connected device. The goodwill and reputation of the websites they represent are now carried by their domain names, which serve as trade brands or trademarks of their own, thanks to the expansion of internet communication and expanding e-commerce and its future possibilities. Since e-commerce is conducted without physical interaction or the possibility to check the items, domain names employed as corporate identifiers have gained relevance and legal legitimacy as a means of distinguishing amongst e-players.

Mobile and Wireless Technology and Cybercrime: As is obvious, the mobile phone has evolved to the point where it has become something equal to as smartphones have replaced personal computers in many ways, including the ability to access the web, send e-mails, and so on. Another reason for concern is the rise in the amount of services accessible on mobile phones, all of which may be exploited by cybercriminals. cyber crime on mobile devices is expected to rise as mobile and wireless technology improves, like other cyber crimes on the internet, is becoming a big danger.

CONCLUSION

Given the trend to adopt a more permissive stance on most cybercrimes, businesses should forget about putting their rogue workers behind jail for exploiting their personal data and information. The new amendments' failure to provide a meaningful recourse for corporations is expected to further damage the industry's faith in the new cyber legal environment. The new cyber law changes establish a maximum compensation amount of Rs 5 crore for damages. When expressed in US dollars, this is a tiny sum that offers little solace to companies whose sensitive information worth millions of dollars is stolen or exploited by their workers or agents.

It's worth noting that nations like the United States, Australia, and New Zealand have proved their commitment to fighting spam by enacting special anti-spam laws. However, there is no anti-spam law in India, nor are there any special mechanisms for efficient spam prevention and control. As far as Spam is concerned, this makes India a paradise. This is all the more concerning since India is already one of the top 10 countries in the world where Spam originates.

Every country is faced with the same problem of combating cybercrime and effectively promoting security to its inhabitants and companies. Unlike conventional crime, which is conducted in a single physical area, cybercrime is perpetrated online and is often not tied to any specific geographic location. As a consequence, regardless of whatever criminological opinions define crime based on social, cultural, and material characteristics, and see crimes as happening in a specific geographic region, a coordinated global response to the problem of cybercrime is required. It is now possible to categorise crime using this definition. This category, however, cannot be used to cybercrime since the context in which it is perpetrated is not limited to a geographical location or to certain social or cultural groups..

REFERENCE

1. KPMG (2013). Global eFr@ud Survey, KPMG Forensic and Litigation Services.

2. Lee, J. R., & Downing, S. (2017). An exploratory perception analysis of consensual and nonconsensual image sharing. International Journal of Cybersecurity Intelligence & Cybercrime, 2(2), 23-43.

3. Lloyd Ian, "Information Technology Law", Edition-2000, Butterworths Publishers (Pvt.) Ltd., New Delhi
4. Lloyed Ian, "Legal Aspects of the Information Society", Edition-2000, Butterworths, London.
5. Louw, D. Forensic psychology. In International Encyclopedia of the Social & Behavioral Sciences, 2nd ed.; Elsevier: Amsterdam, The Netherlands, 2015; pp. 351–356.
6. Lukens Rebecca J., "A Critical Hand Book of Children's Literature", Edition1998, Diane Publishing. Majid Yar, "Cyber Crime and Society", Edition-2006, SAGE Publication India Pvt. Ltd., New Delhi.
7. Lynne Roberts, “Jurisdictional and Definitional Concern with Computermediated inter-personal Crimes: an Analysis of Cyber stalking” published in International Journals of Cyber Criminology, Vol.2, Issue 1, Jan.2008.
8. M. Dasgupta: Cyber Crime in India (A comparative study), 2009.
9. R. Blainpain and B. Verschraegev (eds), InternationalEncyclopedia of Laws: Private International Law (The Hague: Kluwer Law International, 2005)
10. R. Nagpal: What is Cyber Crime; (2003).
11. R.C. Mishra: Cyber-Crime: Impacts in the New Millennium: 1st Ed. (Author’s Press Delhi) 2002.
12. R.K. Chaubey (Dr.): An Introduction to Cyber Crime & Cyber Law (Kamal Lay House Kolkata) 2008.
13. R.K. Suri. and T.N. Chhabra: Cybercrime (Pentagon Press, New Delhi) 1st Ed. 2001 reprint 2003.
14. Rabkin, Jeremy; Eisenach, Jeffrey "The U.S. Abandons the Internet: Multilateral governance of the domain name system risks censorship and repression".2009

Corresponding Author

Vivek Sharma*

Research Scholar, Sunrise University, Alwar, Rajasthan