CYBER CRIME - A DETAILED STUDY

Author: Sanjay Rakul, V year of B.B.A.,LL.B.(Hons.) from SASTRA Deemed to be University

ABSTRACT

Crime has a negative impact on all members of society, regardless of its form, in terms of social and financial aspects. Previously, a criminal would have to commit some sort of robbery in order to gain access to a person's goods. In the case of data theft, the thief would have to break into a facility and search through files for the most valuable and profitable information. Criminals may attack their victims from afar in today's society, and due to the nature of the internet, these actions are unlikely to be punished. The emergence of cybercrime marks a watershed moment in human history. Cybercrime has increased dramatically in developing countries as a result of the Internet's rapid spread and the digitalization of commercial activity. The entire world is moving towards development while also advancing technologically, and the rapid development of internet and computer technology globally has led to the rise of new forms of transnational crime in particular. Virtually no boundaries exist for the issues and crimes caused by or committed in the information technology or internet sector. This research believes that the final paper will provide readers with knowledge of cybercrime and Indian cyber laws, particularly the Information Technology Act of India.

INTRODUCTION

People have become increasingly reliant on the internet for all of their needs as technology advances. We can now access everything while sitting in one place thanks to the internet. Everything imaginable can be done through the internet, including social networking, online shopping, data storage, gaming, online schooling, and online jobs. The internet is used in almost every aspect of life. As the internet and its associated benefits gained popularity, so did the concept of cybercrime. Today, the international community has begun to draft cybercrime legislation in response to the rise in cybercrime in the virtual world. If we look at the history of cybercrime laws, we can see that it began with the invention of the internet. The laws that govern

this area are known as Cyber laws, and all netizens of this space are subject to them due to their universal jurisdiction. Cyber law is also defined as the branch of law concerned with legal issues arising from the use of interconnected information technology.

As people's reliance on the internet has grown, so has the variety of cybercrime. There was a lack of understanding about the crimes that could be committed over the internet a few years ago, but today, in terms of cybercrime, India is not far behind other countries, where the rate of occurrence of cybercrime is also on the rise. According to a report from Norton Lifelock, a cybersecurity software company, 27 million Indian adults have been victims of identity theft in the last 12 months, and 52 percent of people in the country are unaware of how to defend themselves against cybercrime. In addition, on August 30, 2019, the Ministry of Home Affairs launched the National Cyber Crime Reporting Portal to provide people with a centralized system for reporting all types of cybercrime occurrences online, with a particular emphasis on cybercrime against women and children. According to the portal's statistics, 3,17,439 cybercrime events and 5,771 FIRs have been recorded in the country since its inception until February 28, 2021, with Karnataka recording 21,562 cybercrime occurrences and 87 FIRs and Maharashtra recording 50,806 cybercrime incidents and 534 FIRs. According to the data, the number of victims of cybercrime is not insignificant; thus, cybercrime is a serious concern. The goals of this research are to investigate the history of cybercrime around the world, to examine the concept of cybercrime and cyber laws in India, to highlight the impact of cybercrime on national and international security, and to discuss the cybercrime breach of national security confidentiality and privacy.

EVOLUTION OF CYBER CRIME

According to one theory about the historical genesis and evolution of cybercrime, "the primitive type of computer has been in Japan, China, and India since 3500 B.C, but Charles Babbage's analytical engine is considered to be the time of modern computers." The first successful computer was built, and it was so large that it took up the entire room, and it was too expensive to operate. Carrying out cyberattacks was difficult for nearly two decades after the creation of the world's first digital computer in 1943. Access to the massive electronic machines was restricted to a small number of people, and they were not networked, so the threat was almost non-existent.

Personal computers become more affordable and commonplace in India at the start of the twenty-first century. After World War II, the US Department of Defense established the Internet with the goal of creating a network that could function in the event of a disaster or war and securely transmit information. In India, internet services were launched by the state-owned Videsh Sanchar Nigam Limited in 1995, and the government ended VSNL's monopoly in 1998, opening the market to private operators. At the time, internet users in India constituted 0.1% of the total population; today, India ranks second only to China in terms of internet users, with 33.22% of the population using the internet.

"In the case of computer crime, legislators grew increasingly attentive in the 1980s as businesses became more dependent on computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations," Abraham and Seymour explained. Criminals can now easily encrypt information representing evidence of their criminal acts, store it, and even transmit it without fear of law enforcement detection." "Because of the Internet's extraordinary impact, a computer crime scene can now span from the geographical point of victimization to any other point on the planet, further complicating criminal investigative efforts." A commonality among these types of crimes is that the offender relies heavily on law enforcement's lack of technological skills to successfully commit the offenses and escape undetected.

Based on the empirical evidence available on investigators' self-assessed skills in this area, computer criminals have good reason to be optimistic about their chances of evading detection." As we move into the twenty-first century, it is clear that "technological innovations have paved the way for the entire population using computer technology today to experience new and wonderful conveniences in their daily lives ranging from how to educate, shop, entertain, to availing the understanding of business strategies and work flow." But it's also true that the technological marvels that have improved our quality of life come with some risks. While computer technology has provided many people with increased convenience, it has also provided thieves with new entry points.

Cybercrime as we know it today began on November 2, 1988, when Robert Tappan Morris unleashed the Morris Worm, named after him, on the world, wreaking havoc on business. Morris

was unaware of his creation's capabilities. Outside of a research lab, this type of self-replicating program had never been seen before, and the worm quickly transformed itself into the world's first large-scale distributed denial of service (DDoS) attack. Despite the fact that this worm was not intended to be malicious, it caused significant damage. The program overwhelmed computers all over the world, and servers came to a halt. Although Morris quickly issued the protocol for terminating the program, the damage had already been done. Morris was the first person to be prosecuted and charged under the Computer Fraud and Abuse Act in 1989.

The first known ransomware attack, which targeted the healthcare industry, occurred in 1989. Ransomware is a type of malicious software that encrypts and locks a user's data until a small ransom is paid, at which point a cryptographic unlock key is sent. An evolutionary researcher named Joseph Popp distributed 20,000 floppy discs across 90 countries, claiming that the discs contained software that could be used to analyze an individual's risk factors for developing the AIDS virus. The disc, on the other hand, contained malware that, when activated, displayed a message demanding payment for a software license. Ransomware attacks have grown in sophistication over time, with the healthcare industry remaining a major target. The historical evolution of cybercrime threats is presented chronologically:

1971 - Telephone phreak John Draper discovers that a whistle given out as a prize in boxes of Cap'n Crunch Cereal produced the same tones as telephone switching computers of the time. Phone phreaks are computer programmers who are obsessed with phone networks, which are the foundation of modern computer networking. He created a "blue box" with a whistle that allowed him to make free long-distance phone calls and then published the instructions for making it. Wire fraud has increased significantly.

1973 - A teller at a local New York bank embezzled over $2 million dollars using a computer.

1978 - The first electronic bulletin board system went live, quickly becoming the preferred method of communication in the cyber world. It enabled the quick and free exchange of knowledge, including hacking tips and tricks for computer networks.

1981 - Ian Murphy, known to his fans as Captain Zap, was the first person to be convicted of a cyber crime. He gained access to the AT&T network and altered the internal clock to charge off-hours rates during peak hours. In comparison to today's penalties, he received 1,000 hours of community service and 2.5 years of probation, a mere slap on the wrist, and was the inspiration for the film Sneakers

1982 – A 15-year-old kid created the virus Elk Cloner as a joke. It is one of the first viruses known to have escaped from its original operating system and spread in the "wild." It was designed to attack Apple II operating systems and spread via floppy disk.

1983 – The film War Games is released, bringing hacking into the mainstream. The film depicts a teenage boy who hacks into a government computer system via a back door and nearly causes World War III.

1990 – Two cyber-based gangs, Legion Of Doom and Masters Of Deception, engage in online warfare. They actively interfere with each other's connections, hack into computers, and steal data. These two organizations were large-scale phone phreaks who were well-known for numerous hacks into telephone mainframe infrastructure. The growth of these two groups, along with other cyber gangs, prompted an FBI sting targeting BBSs that promoted credit card theft and wire fraud.

1993 – Kevin Poulson is apprehended and convicted of hacking into phone systems. He took over all phone lines connecting to a LA radio station in order to win a call-in contest. He was featured on America's Most Wanted at one point, but the phone lines for that show mysteriously went silent. When the FBI began their investigation, he fled but was eventually apprehended. He was sentenced to 5 years in federal prison and was the first to have an Internet ban imposed as part of his sentence.

1994 – The World Wide Web is launched, allowing black hat hackers to transfer product information from old bulletin board systems to their own websites. A student in the United Kingdom uses the information to hack into Korea's nuclear program, NASA, and other US agencies using only a Commodore Amiga computer and an online "blueboxing" program.

1995 – Macro-viruses emerge. Macro-viruses are viruses that are written in computer languages and are embedded in applications. When an application, such as word processing or spreadsheet documents, is opened, macros run and are an easy way for hackers to deliver malware. This is why opening unknown email attachments can be extremely dangerous. Macro-viruses are still difficult to detect and are a major source of computer infection.

1996 – According to CIA Director John Deutsch, foreign-based organized crime rings were actively attempting to hack into US government and corporate networks. The US GAO announced that its files had been attacked at least 650,000 times by hackers, with at least 60% of them succeeding.

1997 – According to the FBI, over 85% of US companies have been hacked, and the majority are unaware. The Chaos Computer Club has hacked Quicken software and is able to make financial transfers without informing the bank or account holder.

1999 - The Melissa virus had been released. It infiltrated the user's computer through a Word document before sending copies of itself to the first 50 email addresses in Microsoft Outlook. It is still one of the most rapidly spreading viruses, and the damage cost around $80 million to repair.

2000 – The number and variety of online attacks are increasing at an alarming rate. After the credit card information of its customers was published online, music retailer CD Universe was extorted for millions of dollars. DoS attacks have been launched numerous times against AOL, Yahoo!, Ebay, and others. Emulex stock drops nearly 50% as a result of fake news. The infamous I Love You Virus infected 50 million computers across the Internet, corrupting data and self-propagating by exploiting a user's email contacts.

2002 – The Shadow Crew website has gone live. The website served as a forum and message board for black hat hackers. Members could post, share, and learn how to commit a variety of cyber crimes while avoiding arrest. The Secret Service shut down the site after it had been up for two years. In the United States and six other countries, 28 people were arrested.

2003 – SQL Slammer becomes the world's fastest spreading worm. It infected SQL servers and launched a denial of service attack that slowed Internet speeds for quite some time. In terms of infection speed, it infected nearly 75,000 machines in less than 10 minutes.

2007 – Hacking, data theft, and malware infections are on the rise. The number of stolen records and infected machines is in the millions, and the amount of damage caused is in the billions. The Chinese government is accused of hacking into government systems in the United States and elsewhere.

WHY IS CYBERCRIME SUCH A BIG DEAL?

While it may appear that hostile governments are the primary perpetrators of online Internet attacks, this is not the case. According to United Nations cyber security experts, sophisticated gangs of criminals engaged in highly organized operations commit roughly 80% of all cyber-based crime. The gangs operated like legitimate businesses, with regular work hours and a hierarchy of members working together to create, operate, and maintain whatever fraud they were focused on.

Crime lurks just beneath the Internet's surface. It's like an invisible fungus spreading through the web one breach at a time. A variety of factors contribute to its ability to spread so rapidly. First, criminals can easily hide behind their terminals far from regulators, operating with impunity by masking their locations and misdirecting any prying eyes with the latest high-tech software and networking techniques. Second, almost everyone on the planet has easy access to the Internet, and when it comes down to it, anyone with money or information to steal is probably connected and not difficult to find. Third, you don't have to be a programmer to run a scam; all you need to know is where to buy one. The Internet is multilayered; there is the surface layer, which anyone can access, but there are deeper layers that are much more difficult to find, such as the Deep Web and the TOR network, and then there is the Deep Dark Web, where illegal activities occur on a daily basis. Everything imaginable can be found on these websites, from innocent chat rooms where users prefer to remain completely anonymous to sites where you can purchase your very own malware.

TYPES OF CYBER CRIME

The cybercrimes are classified as follows:

1. Cybercrime against Individuals
2. Crime against Organizations
3. Crime against society

Cybercrime against Individuals

These types of crimes are committed against an individual or his property. The following are examples of the major offenses covered by it.

A. Unauthorized Access

B. Online fraud

C. Cyber Stalking

D. Hacking

E. Phishing and Vishing

F. Spoofing

G. Identity theft

Cyber Crime against Organizations

In the modern era, almost all large corporations and organizations are scaling back their online growth. They must also deal with cybercrime in this situation. The following are some of the most common cybercrimes committed against institutions or organizations:

H. Data breach

I. Cyber terrorism

J. Denial of service (DoS) attack

K. Cyber espionage

Cyber Crime against Society

These types of cybercrimes have a societal impact, with young men and women and children being particularly vulnerable. Also, which are prohibited websites and products in society, as well as illegal materials, are made available to the public via the internet. The following are examples of cybercrime against society.

A. Child pornography

B. Online gambling

C. Selling illegal article

D. Forgery

E. Spamming

FUTURE THREATS

The report considers how cybercrime may evolve in the next five to ten years, as determined by an expert panel, and what threats organizations should be prepared for:

• Destructive attacks may become even more damaging - As organizations embrace digital transformation and IoT, attackers will likely exploit the increased attack surface. Extortion attacks based on the threat of data destruction could increase in sectors that rely on IoT devices, particularly those that rely on infrastructure in time-sensitive and critical ways.

• Professionalized and targeted intrusions - To maximize the value of their intrusions, cybercriminals will continue to use APT tactics, such as spending more time on target reconnaissance and establishing long-term access within networks.

• Emerging technologies that can function as both a weapon and a shield - Technologies in their infancy, such as Web3, could create new opportunities for creating reputation systems that support the cybercrime economy, making it more difficult for authorities to shut down. Quantum computing could be used to boost decryption efforts.

• Attackers will concentrate on making attacks more efficient - As cybercrime is reduced to repeatable, procedural steps, opportunities for automation and efficiency will emerge. Cybercriminals may use AI to automate their post-exploitation activities, such as selecting targets from a victim's address book and building persuasive spear-phishing attacks based on previous communication.

CONCEPT OF CYBER SECURITY

Because of the complex and ever-changing nature of information and communication technology at the global and national levels, the term "cyber security" has yet to be comprehensively defined. Cyber security as we know it today began in 1972 with a research project on ARPANET (The Advanced Research Projects Agency Network), the internet's precursor. The concept of cyber-security was maturing by the mid-1970s. "Security has become an important and challenging goal in the design of computer systems," stated Operating System Structures to Support Security and Reliable Software in 1976. The term cyber security encompasses both the physical security of devices and the information stored within them. It addresses "security against unauthorized access, use, disclosure, disruption, modification, and destruction." The Information Technology Act of 2000 defines cyber security as "protecting information, equipment, devices, computers, computer resources, communication devices, and information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction."

INDIA'S REQUIREMENTS FOR CYBER LAW

To begin with, India's legal system is extensive and well-defined. The Constitution of India is the most important of the many laws that have been passed and implemented. Among the laws we share are the Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, the Companies Act, and others. As a result, the introduction of the Internet introduced a number of delicate legal difficulties and challenges, necessitating the adoption of Cyber laws.

Second, "even with the most benevolent and liberal interpretation, the existing laws of India could not be interpreted in the light of the emerging cyberspace to include all aspects relating to various activities in cyberspace." Indeed, practical experience and judgment have revealed that "interpreting existing laws in the context of emerging cyberspace" without enacting new cyber laws will not be without major risks and pitfalls.

Third, "none of the existing laws gave any legal validity or sanction to cyberspace activities." The Internet, for example, is used by the vast majority of users for email. Even so, email is not "legal" in our country. There is no law in the country that gives email legal validity and sanction. In the absence of a specific law enacted by Parliament, our courts and judiciary have been hesitant to grant judicial recognition to the legality of email." As a result, the need for Cyber law has arisen.

Fourth, "the Internet necessitates a modern, enabling, and supportive legal infrastructure." Because traditional laws have failed to provide this legal infrastructure, the enactment of relevant Cyber laws is the only way to provide it. E-commerce, the Internet's most promising future, can only be realized if the necessary legal infrastructure is in place to support its vibrant growth."

Other cyber historians and cyber security experts argue that "Cyber laws in India or cyber-crime law in India are important for the simple reason that the cybercrime act in India encompasses and covers all of the aspects that occur on or with the internet - transactions, and activities involving the internet and cyberspace." With the Information Technology Act, 2000, the rise of the twenty-first century marked the evolution of cyber law in India. The first recorded cybercrime occurred in 1820. The Information Technology Act is the result of a resolution passed by the United Nations General Assembly on January 30, 1997, which adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, among other things, that

all states give the Model Law favorable consideration when revising and enacting new laws, so that uniformity can be observed in the laws of the various cyber-nations applicable to alternatives to paper-based methods of communication and information storage.

Information Technology Act, 2000

Although cybercrime is not defined in the Information Technology Act of 2000 ("IT Act") or the IT Amendment Act of 2008, the IT Act has the authority to address it because it contains provisions relating to cyber-offenses or crimes. Because cybercrime involves the targeting or assault of a computer or computer network, the IT Act's definitions of terms like computer, computer network, computer resource, data, and information are critical. It primarily:

1. recognizes electronic records and electronic signatures as valid;

2. recognizes electronic signatures and digital signatures; and recognizes electronic records and electronic signatures as valid.

3. Handles computer-related offenses and other offenses committed via electronic means, as well as violations.

Constant criticisms, evaluations, and harsh interpretations of certain sections resulted in the IT Amendment Act, 2008 ("IT Amendment Act"), which went into effect in 2008.

Cyber Crimes under the IT Act, 2000

Section 65 - Tampering with computer source documents.

Section 66 - Hacking with computer systems.

Section 67 - Publishing obscene information

Section 70 - Unauthorized access to a secure system

Section 72 -Breach of confidentiality and privacy.

Section-73: Publication of false digital signature certificates

The IT Amendment Act, 2008 made some notable changes, including:

1. Concentrate on data privacy.

2. Information security practices are introduced,

3. The term cybercafé is defined, and

4. Companies must implement reasonable security practices to safeguard information against unauthorized access, damage, use, modification, disclosure, or impairment.

Section 43 of the IT Act gives a computer or computer system owner recourse in the form of compensation if a person or entity damages or destroys the computer or computer system.

Section 43A of the IT Act compensates a person if a company dealing with or handling the person's sensitive personal information in its computer resource fails to protect the information.

Section 66 of the IT Act punishes the person who commits the act referred to in Section 43 with imprisonment for a term of up to three years or a fine of up to Rs. five lakh, or both.

Section 66B: receives or retains stolen computer resource knowingly by deception, punishable by imprisonment for up to three years or a fine of up to Rs. one lakh, or both.

Section 66C: uses another person's electronic signature or password fraudulently or dishonestly, punishable by imprisonment for up to three years and a fine of up to Rs. one lakh.

Section 66D: cheats by impersonation using any communication device or computer, punishable by imprisonment for up to three years and a fine of up to Rs. one lakh.

Section 66F punishes anyone who: (a) intends to jeopardize India's unity, integrity, security, or sovereignty; (b) denies access to any person authorized to access a computer; (c) attempts to penetrate or access a computer without authorization; or (d) introduces a computer contaminant such as a virus, Trojan, malware, etc. and causes death or injury to a person or damage to or destruction of property, etc. with life imprisonment.

POCSO Act of 2012

The Protection of Children from Sexual Offenses Act , 2012 (the "POCSO Act") makes it illegal to exploit a child or children for pornographic purposes, including using a child for sexual pleasure on the internet. Persons convicted of the aforementioned offenses face up to 5 years in prison, and if convicted a second time, they face up to 7 years in prison and a fine. The POCSO Act also allows for up to three years in prison, a fine, or both for anyone who keeps pornographic information involving a child with the intent of profiting from it.

The Indian Penal Code, 1860 (IPC)

It punishes those who commit crimes such as identity theft or cyber fraud. Sections 464 (Creating a false document or false electronic record), 465 (Forgery Punishment), 468 (Forgery for the Purpose of Cheating i.e. forged electronic record), 469 (Forgery for the Purpose of Harming Reputation i.e. forged electronic record), and 471 (Forgery for the Purpose of Harming Reputation i.e. forged electronic record) of the IPC are all applicable. Some other sections include

Sending threatening emails- Section 503 IPC

Emailing defamatory messages- Section 499 IPC

Electronic record forgery- Section 463 IPC

False websites and cyber fraud- Section 420 IPC

Web-Jacking- IPC Section 383

Email spoofing - Section 463 IPC

E-mail Abuse- Section 500 IPC

CONCLUSION

Cybercrime is out of control; it occurs every day and in every location. Estimates of how much cyber criminals make vary, but nearly $450 billion was made last year alone, and this figure is

only expected to rise. To put it into context, the number of records stolen last year was over 2 billion, including at least 100 million health insurance files, mostly from the United States. Today's technological age, in which human civilization has achieved limitless facilities and security in every field, has made it easier to develop cyber technology. However, anti-humanitarian and anti-nationalist individuals gave birth to cybercrime. Cybercrime endangers both human security and national security. Cyber criminals directly harm the socioeconomic, political, and cultural spheres. India has surpassed the United States as the world's second largest internet user country. The Indian government is also constantly enacting new laws to prevent and punish cybercrime. In addition, the government agreed to collaborate on the international convention for the prevention of cybercrime. The government's Ministry of Information Technology and Ministry of Law collaborated to create laws and policies to combat cybercriminals. In which the Information Technology Act of 2000, the National Policy on Information Technology of 2012, the National Cyber Security Policy of 2013, the Indian Computer Emergency Response Team (CERT-In) of 2022, and other important laws were enacted. The entire world is united in its fight against cyber terrorism. There is also an anti-crime campaign in which women and children are harassed. To combat cybercrime, civil society and the government must collaborate. The government should enact additional legislation, amend sections of the IPC, and enact new legislation. So that cybercriminals can be stopped. The nation's society is intertwined with cyber security in the age of modern technology. As a result, without it, no nation's national security is possible. The following recommendations may be helpful in dealing with India's cyber security challenges:

1. Citizen participation can be extremely beneficial in combating cybercrime and cyber-security.

2. A special cyber security Cell Station should be established to handle cases involving computer crimes.

3. To detect computer-related crimes, a "Cyber Forensic Laboratory with all updated technologies" should be approved.

4. Public Awareness Programs should be implemented to educate the public, especially police officers, about the "National Cyber Security Policy, 2013, National Cyber Security Policy Mission 2020, Indian Computer Emergency Response Team (CERT-In) 2022."

5. The security expert in educational institutions to raise student awareness about computer abuse.