Cyber Crimes: An Overview

Muragendra Tubake
Asst.Prof.of Law, Karnataka State Law University's Law School Navanagar, Hubli, India

Abstract

In the recent days With the advent of the Internet, there is an infinite expansion in the field of Electronics and Communications.. The Internet is a worldwide electronic computer network that connects people and information. But every technology has its own advantages and disadvantages. Internet has several advantages but it is considered as a heaven for cyber criminals. The anonymity over the internet and the jurisdictional issues has given rise to cyber crimes where crime is committed with the aid assistance of computer.

KEYWORDS: Internet, Electronics and Communications, cyber criminals, cyber crimes and computer

Introduction

Cybercrime, computer crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, and targetpoor place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more category. Cyber crime is broadly used term to describe criminal activity committed on computers or the Internet. Cyber crime is a criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, system interference, misuse of devices and electronic fraud. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which causes breach of rules of lans and counter balanced by the sanction of the state.

Objective:

The research article attempts to explain the meaning, nature and definitions of the term 'Cyber crime'. It also focuses on classification of different kinds of Cyber crimes into four groups i.e. Cyber crimes against Individual, Cyber crimes against Property, Cyber crimes against Organization and Cyber crimes against Society

Research Methodology:

The paper is based on the Doctrinal method of primary research.

Meaning of Crime

The word 'Crime' is derived from Greek expression '*Krimos*' which means social order and it is applied 'to those acts that go against social order and are worthy of serious condemnation'.

According to Kenny "Crimes are wrongs whose sanction is punitive, and are in no way remissible by any private person, but are remissible by the Crown alone, if remissible at all".

Halsbury's Laws of England provides, "A crime is an unlawful act or default which is an offence against the public and renders the person guilty of the act or default liable to legal punishment".

Definition and Nature of Cyber Crime

Cybercrime may say to be those species of which genus is the conventional crime and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

Cybercrime simply describes the criminal use of computer technology. The amazing advances have transformed the world in which we live. These technologies have helped to create a truly global market place, characterized by a constant team of information that flows through networks and websites. In the light of these facts, cyber crimes can often take the form of computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

Donn Parker defines computer crime as, "a crime in which the preparatory uses special knowledge about computer technology"

Computer crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of crime.

Encyclopedia Britannica defines cybercrime as, "any use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing, identity or violating the piracy."

Nature of Cybercrimes

The peculiar characteristics of cybercrimes are as follows.

- The weapon with which cybercrime are committed is technology. Cybercrimes are the work of technology and thus cyber criminals are technocrats who have deep understanding of the Internet and Computers.
- Cybercrime is extremely efficient i.e., it takes place in real time. It may take seconds or a few minutes to hack websites or do cyber frauds.
- Cybercrime knows no geographical limitations, boundaries or distances. A cyber criminal in the one corner of the world can commit hacking on a system in other corner of the world.
- The act of cyber crime takes place in cyberspace which makes the cybercriminal being physically outside cyberspace. All the components of cyber criminality from preparation to execution, take place in the cyber space.
- Cybercrime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into websites of backs and the defence department's websites. The amount of loss which may cause is easy to be imagined.
- It is extremely difficult to collect evidence of cybercrime and prove the same in the court of law, due to the anonymity and invisibility of cybercriminal

and its potential to affect in several countries at the same time, which are different from the place of operation of the cyber criminal.

Classification of Cyber Crimes

Cybercrimes are normally related to computers. But it is better to classify them on the basis person so affected by these crimes. It may affect an individual, or an organization, or property or society as a whole. Some time it may happen crime classified under one category may fall under another category at the same time. It is also one of the difficulties in classifying the cybercrimes. For example, hacking may affect both individual and organization at the same time. Following is the broader classification of cyber crimes.

- Cyber crimes against Individual
- Cyber crimes against Property
- Cyber crimes against Organization
- Cyber crimes against Society

I. Cybercrimes against Individual

Cybercriminals may attack individual persons through computers or computer networks Individuals may be the target for cyber criminals. Cybercrimes may affect individuals in different manners like e-mail spoofing, spamming, cyber defamation, phishing, cyber stalking.

E-Mail Spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source.

E.g.: Raju has an e-mail address raju25@gmail.com. His enemy Sanju spoofs his email and sends obscene message to all his acquaintances. Since e-mail appears to have originated from Raju, his friends could take offence and relationships could be spoiled for life.

It involves the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed e-mails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost lot of money.

Spamming

Spam is unsolicited commercial sent electronically, usually to many people at once, often through mail. Spam generally contains advertising in one or more forms

such as offers to sell prescription drugs, stock tips, links to online dating services or pornography web sites, or various business opportunities often of questionable legitimacy. A person who sends spam is called a spammer. Spam is also associated with distribution of malware such as viruses and Trojans. So it is not only an annoyance to the victim but it may also carry malicious code with it by which the computer or computer network of a victim may get corrupted or damaged.

Phishing

Webopedia defines phishing as "the act of sending an e-mail to user falsely claiming to be established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a web site where they asked to update personal information, such as passwords and credit card, social security and bank account number that the legitimate organization already has. The web-site however is bogus and set up only to steal user's information.

The term phishing arises from the use of increasingly sophiscated lures to "fish" for users finished information and passwords.

The term "phishing" is commonly believed to have been derived from the old expression "let's go fishing to see what's biting!" In the technological world of cybercrime, phishing (pronounced the same as "fishing") by analogy means to cast "digital bait" onto the internet to see who bill bite. Thus phishing is a type of social engineering that cybercriminals use when attempting to clause potential victims into revealing private information about themselves or their computer accounts, such as usernames, passwords and financial or bank account numbers.

The damage caused by phishing ranges from loss of access to e-mail to substantial financial loss. This style of identity theft is becoming more popular, because of the ease with which unsuspecting people often divulge personal information to phishers, including credit card numbers and social security numbers.

Cyber Stalking

Stalking in general terns can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously.

Cyber stalking can be defined on the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services.

The majority of victims are female. Cyber stalking prevalent to be highest among victims with a relatively low household income. Stalking victims are more frequently fraud among single persons although married person and those in other partners are not exempt from stalking victimization.

In cyber stalking cybercriminals targets victims in three areas:

1. Live chat or Internet Relay Chat (IRT): in which a user talks live with other users.

2. Message boards and newsgroups: a user interacts with others by posting messages, conversing back and forth.
3. E-mail boxes: a user has the ability to write anything on even attach files to the e-mail. Sending electronic viruses, sending unsolicited e-mail and electronic identity theft are quite common manifestations of cyberstalking.

Cyber Defamation

The defamation is an injury done to the reputation of a person. The essentials of defamation are defamatory statement, the plaintiff must be published in some manner. Cyber defamation may be carried out through e-mail, spread of malicious gossip on discussion groups or posting of offensive content against a person on a website.

Voyeurism

The Oxford English Dictionary defines a 'voyeur' as someone 'whose sexual desires are stimulated or satisfied by covert observation of the sex organs or sexual activities of the others.'

Voyeurism means recording a video or capturing a photograph of victims body normally places like sex organs or in other words known as private place. Normally dressing rooms, bathrooms in hotels, toilets etc are the major places where voyeurism can take place. After filming or photographing, the offender uploads them to the internet or he may transfer those films or photographs to his friends or to somebody else.

II. Cyber Crime against Property

Cyber crimes may affect a property of a person. These crimes are also known as crimes affecting economy. It involves credit card skimming, Intellectual Property Crimes, Internet Time Theft, Identity theft etc.

Credit Card Skimming

Credit Card skimming is the process by which legitimate credit card data is actually captured or copied, usually by electronic means. This technique exploits the vulnerabilities of magnetic-stripe technology, present on much credit, debit and other transactions cards. While allowing cards to be programmed with data quickly and easily, it also means that the data can easily copied.

Intellectual Property Crimes

It mainly involves software piracy and crimes related to domain names.

Software Piracy

It includes illegal use or distribution of software, copying or distributing copyrighted software without license is one kind of piracy. Software piracy includes End-user piracy, Manufacturer piracy, Internet piracy, Counterfeiting, Online auction piracy, Online distributor piracy.

Internet piracy includes offer to unauthorized copies of software for download over internet. It software is available on the Internet one has to make sure that the software publisher has authorized the distribution.

Domain Name Disputes

Domain name very simple is the address of a particular site on the internet not much different from a particular telephone number on the web to communicate with or access a simple specific site; each site must have an address. Internet protocol address act as such address. Cyber squatting is another kind of a cybercrime related to domain names.The term cyber squatter refers to someone who has speculatively registered or has acquired the domain name primarily for the purpose of selling, renting or otherwise transferring the domain name registration to the complainant who is the owner of a mark or service mark. As long as a cyber squatter owns the domain name, the trademark owner cannot register his own trademark as a domain name. Thereby, a cyber squatter breaches the right of a trademark owner to utilize his own trademark.

Internet Time Theft

This connotes the usage by an unauthorized person of the internet hours paid for by another person. In May 200, the Delhi police arrested an engineer who had misused the login name and password of a customer whose internet connection he had set up.

Identity Theft

Identity theft also referred to as identity fraud, is a criminal act where one individual misrepresents himself by pretending to be someone else. This is typically done by illegally using the victims personal information to open new financial accounts, use existing financial accounts, or do some combination of the two. Identity theft may be committed during the course single incident, or it may occur over a long period of time.

There are many ways in which the offender can obtain personal information about a person in order to commit identity theft. Some of these are “offline” through physical means, such as when an offender goes through the victim’s trash to find discarded documents such as credit applications and pay stubs. Other methods are “online” via computer or the Internet such as when victims respond to phishing ploys and enter personal information on dummy websites set up to look like legitimate ones, or when they volunteer personal information to blogs, chat rooms or social Networking Websites.

III. Cybercrime against Organisation

Cybercrimes also affect organization. Organization includes banks, service sectors, government agencies, companies and other association of persons. These involve Hacking, Denial of Service, Virus and Worms, E-mail bombing, Salami Attack, Logic Bomb, Spywares etc.

Hacking

Hacking means unauthorized access to a computer system. It is the most common type of cyber crime being committed across the world. Commonly used definition of hacking is breaking into computer systems. Hacking as a cybercrime is the most dangerous to the Internet because it has effect of eroding the credibility of

the Internet. Hacking creates a perception in the minds of citizens that internet is vulnerable and weak.

There are four types of hacking which are most prevalent today:

1. For fun as a hobby, mostly by teenagers obsessed with the internet.
2. To damage the business of competitors.
3. With the intention of committing a further offence such as fraud and misappropriation.
4. By internet security companies to test their client

Denial of Service Attack (Dos Attack)

Denial of Service (Dos)attacks are cybercrimes in which the primary goal is to deny users of computers or other types of electronic devices access to an information system or its resources. Dos attack often involve flooding a computer network with massive amounts of data in a short period of time so that servers cannot keep up with the amount of data being transmitted. The effect is prevention, disruption and for minimization of legitimate network traffic. Dos attacks may also inhibit users from accessing network related applications or services needed.

Another kind of Dos attack is D Dos also known as Distributed Denial of Service Attack wherein multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

E-mail Bombing

An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to address in an attempt to overflow the mail box or overwhelm the server.

There are two ways of e-mail bombing, mass mailing and list linking. Mass mailing consists of sending numerous duplicate mails to the same e-mail ID list linking consisting of signing a particular e-mail ID upto several subscription. This type of bombing is effective as the person has to unsubscribe from all the services manually.

Salami Attacks

These attacks are used for committing financial crimes. The key here is to make the attention so insignificant that in a single case it would go completely unnoticed. This attack is called “salami attack” as it is analogous to slicing the data thinly, like salami. For instance, a bank employee inserts a program, into the banks servers, that deducts a small amount of money (say Rs 1 a month) from the account of every customer. No account holder will probably employee will make a sizeable amount of money every month.

Logic Bomb:

A logic bomb is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. ‘Logic Bomb is that code of a virus, which waits for some event to occur. When that particular time comes, it bursts and cause complete damage. It may erase the complete hard disk.’ In this way, a logic bomb is very analogous to a real-world land mine. The most common activator for a

logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code.

Data Diddling:

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable. For example, a person entering accounting may change data to show their account, or that or a friend or family member, is paid in full. By changing or failing to enter the information, they are able to steal from the company.

IV. Cyber Crimes against Society:

Society has a whole is also affected by cyber crimes. Pornographic websites, sale of illegal articles, illegal auctions on the internet are contributing to the decline of social morals. Terrorist activities are also taking place using computer or computer networks in the name of cyber terrorism. Cyber space is also helping the criminals in manufacturing fake currency notes, revenue stamps which is affecting society at large. Following is the brief discussion about cyber crimes affecting the society.

Cyber Pornography:

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit in India may not well be considered obscene in United States of America. There have been many attempts to limit the availability of pornographic content on the internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Due to torrent websites, Bit torrent, extra torrent, also known as files sharing networks it is very easy to anybody who has an internet connection to download sexual videos, images and all other related contents.

Another noticeable thing in pornography is ‘child pornography’. The Cybercrime Convention define ‘child pornography’ to include ‘pornographic material’ that visually depicts:

a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct; or,
c) Realistic images representing a minor engaged in sexually explicit conduct.

The easy access to the pornographic contents readily and freely available over the internet lowers the inhibitions of the children. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Cyber criminals are taking advantage of innocence of children and engage them into cyber pornographic industries without their explicit consent.

Sale of Illegal Articles:

It is becoming increasingly common to find cases where sale of narcotics drugs, weapons and wildlife is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc. Internet is a very easiest way on the planet where criminals communicate with each other without any barriers.

Online Gambling:

Internet gambling is now easily available to anyone with access to a computer hooked up to the Internet. Traditional gambling can be controlled, police can inspect the places where gambling is being carried out. But it is highly impossible in case of internet based gambling. Because internet has no border, no jurisdictions, highly anonymous and it is a virtual space where anything can be happen.

The U.S. General Accounting Office has defined Internet gambling as "any activity that takes place via the Internet and that includes placing a bet or wager". Many types of gambling activity take place online, including casino-style games like blackjack, poker, or roulette, pari-mutuel wagering such as wagering on horse races, dog races, lotteries, sports wagering, and bingo.

Cyber Terrorism:

The general meaning of Terrorism involves the use or threat of violence and seeks to create fear, not just within the direct victims but among a wide audience. Federal Bureau of Investigation (US) describes terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

Cyber terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large- scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

The National Infrastructure Protection Center (NIPC) is a group of over 100 special agents, analysts, and others from the FBI, the Department of Defense, the CIA, the National Security Agency, and other federal departments. The NIPC's Analysis and Information Sharing Unit has proposed the following definition:

- Cyber-terrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Cyber terrorism can be dangerous than traditional terrorism activities. It can be as destructive as a nuclear weapon if executed in a proper manner. Carrying out terrorist activities is also very easy just by the use of computers. And physical presence is also not necessary as it can be done from sitting anywhere in the world through internet and computers.

As described by Barry C. Collin, who takes credit for coining the term "cyber terrorism" in themed 1980s, says, "This enemy does not attack us with truckloads of explosives, or with brief cases of Sarin gas, nor with dynamite strapped to the bodies of fanatics. This enemy attacks us with ones and zeros".

Speaking about the effect of the cyber terrorism on a particular country Collins says that: "In effect, the cyber-terrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live. In addition, the people charged with the protection of their nation will not have warning, and will not be able to shut down the terrorist, since that cyber-terrorist is most likely on the other side of the world."

Conclusion

The nature of cyber crimes requires that there should be an International Co operation among the countries to tackle the cyber criminals. Until now the Internet Community has only one cyber convention. Not all the countries are party to that convention. Even India is also not a party to the convention. There is no unity among the nations itself in combating cyber crimes. Further it can be said that, not only should the co operation exist at the international level it should exist among different states of a particular country also. Every police officer should be trained accordingly; every country should have proper technology to beat the cyber criminals in all aspects.

References

Alexander P.J. (2002) "Policing India in the New Millennium", Allied Publication, New Delhi

Bidgoli Hussein (2004) "The Internet Encyclopedia, Vol.1", John Wiley & Sons Publication, New Jersey

Clough J. (2010) "Principles of Cybercrime", Cambridge University Press, New York

Grabosky Peter & Roderic Broadhurst. (2005) "Cybercrime: The Challenge in Asia",Hong Kong University Press, Hong Kong

Kamath Nandan. (2009) "Law relating to Computers, Internet and E-commerce", Universal Law Publication, Delhi

Gaur K. D. (1992) "A Textbook on the Indian Penal Code", Oxford and IBH Publication, New Delhi

Pardesi Jigisha. (2007) "Emerging Trends in Information Technology", Nirali Prakashan, Pune

S. Ghosh and E. Turrini. (2010) "Cybercrimes: A Multidisciplinary Analysis", Springer-Verlag Heidelberg Publication, Berlin

Singh Justice Yatindra (2010) “Cyber Laws”, Universal Law Publication, Delhi

Sood Vivek (2001) “Cyber Law Simplified”, Tata McGraw-Hill Publication, New Delhi

Waelde, Lilian Edwards and Charlotte (2009), “Law and the Internet”, Hard Publication, Portland

Wall David (2001) “Crime and the Internet-Cyber crimes and Cyber fears” Routledge Publications, London