By Rahul Kr. Verma
Advocate

Types of Cyber Crime

Thank you so much for inviting me at this platform for this session. Today we are going to discuss in brief that how many cyber crimes use to commit with us in general in these days.

First of all, we need to understand that what is the object of the cyber-crime.

So, The objects of the cyber crime are hacking, phishing, spamming or its used as a tool to commit an offence like child pornography, hate crimes etc.

Cyber crime is defined as a crime in which the cyber criminals may use computer technology to access your personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and documents or data storage. And the Criminals who perform these illegal activities are often referred to as hackers.

So, There are various crimes where computer or mobile phone is a tool for these unlawful activities such as:-

1. **Cyber Stalking:** Black law dictionary defines cyber stalking as " the act of threatening, harassing or annoying someone through multiple e-mail address, as through the internet, especially with the intent of placing the recipient in fear that an illegal act or injury will be inflicted on the recipient or a member of the recipient's family or household".

   Although there is no universally accepted definition of cyber stalking, it is generally defined as the repeated acts of harassment or threatening behaviour of the cyber-criminal towards the victim by using internet services. Stalking in general terms can be referred to as the repeated acts of harassment targeting victim such as follow the victim, making harassing phone calls, killing the victim pet, vandalizing victim property, leaving written massages or objects. Stalking may be followed by series of violent acts such as physical harm to the victim. It all depends on the course of conduct of the stalker.

   Basically, Cyber stalking is a crime against a person, as opposed to other internet enabled crimes such as data theft or hacking, which are crimes are against the property. The prevalence of cyber stalking has

increased with the increased use of social media such as Facebook, Twitter, Whatsapp, Myspace, Tumblr, Telegram, Instagram etc.., which give easy access to your photos, personal information and whereabouts of a person and also act as medium of communication. Cyber Stalking is often accompanied by realtime or offline stalking. It is motivated by a desire to control, intimidate or influence a victim.

A stalker may be an online stranger or a person whom the victim knows. He may be anonymous and solicit involvement of other people online who do not even know the victim. Typically, the cyber stalker's victim is new on the web and inexperienced with the rules of internet safety. Their main targets are mostly females, children, emotionally weak or unstable persons. It is believed that over 75% of the victims are female.

As far as the Law on Cyber Staking in India.

Before the Criminal Law Amendment Act 2013, which came on the recommendations of Justice Verma Committee Report on women law, there was no separate offence of stalking. However, it was covered under section 509 IPC. Justice Verma committee proposed the inclusion of laws regulating stalking including cyber stalking and voyeurism in our criminal law. It was observed by the Justice Verma Committee that the **Priyadarshini Matoo case** is a stark reminder of what stalking can lead to if it left ignored. It was further observed that stalking incidents have in the past led to gruesome rapes and acid attacks and therefore, the need arises to provide for a law which creates a strong deterrence. Accordingly, our legislator made certain amendments to the IPC by bringing Criminal Law Amendment Act 2013 and inserted section 354C and 354D and made voyeurism and stalking punishable.

2. **PORNOGRAPHY:** Pornography can be defined as any media basically construed as intended to entertain or arouse erotic desire. This is the most common definition used by researchers and the courts. Among some persons and groups, the pornography and its associated materials have negative connotations and they wish to express the sentiments in the definition. For others pornography is viewed positively.

The rapid growth of the internet has raised concern about how internet use affects the prevalence of sex crimes. On the one hand, the internet provides meeting points for potential offenders and victims, both in chat rooms and on internet dating sites. On the other hand, a vast supply of extreme sexual content has triggered renewed interest in the impact of pornography on sex related crimes such as rape and child sex abuse.

There are Several theories relate the consumption of pornographic material to sex crimes. One theory argues that pornography increases the likelihood of sex crimes because it triggers sexual arousal and aggression, degrades women or children to objects and affects social and individual norms. A second, opposing theory highlights the potential cathartic effects of pornography consumption, because it leads to sexual relief and thereby potentially offsets sexual aggression.

But it leads to cybercrime such as Online Obscenity & Pornography: meaning thereby publishing of information which is obscene in electronic form. Whoever publishes or transmits or cause to be published in the electronic form, any material which is lascivious or appeal to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, as per section 67 of Information Technology Act, 2000, it shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to Rupees One Lakh and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to 10 years and also with fine which may extend to Two Lakh Rupees. As per section 66E of Information Technology Act 2000, violation of privacy of an individual is also punishable up to three years or with fine up to Rupees two lakh or both.

Among the cyber crimes, obscenity and pornography in the internet poses a major challenge, especially in societies where moral standards are held as the core of value of culture and reinforced by religious values. The standard of such morals vary from society to society and in a given society undergoes substantial changes. But for the moment the law

relating to obscenity and pornography of a given system holds steadfast and attempts to regulate the same. Regulating obscenity in a physical world itself is fraught with many difficulties and in internet it becomes very porous due to its nature of operation. The whole gamut of obscenity and pornography also becomes a lucrative business in internet as it is banned in most part of the world and hence a huge market. But unfortunately, there is no proper check and balance by the concerned authorities, therefore it porn sites are easily available on the internet.

Child Pornography:

Children being weak, gentle and meek should be protected from the world of criminals, shady people and negative people and so on. They being the most voiceless and defenceless group, requires special attention for protection of their human rights. It is indeed the duty of the society at large, including the legal and judicial authorities, to protect those who are helpless to protect themselves and this is especially true for children. But, at time, these vulnerable kids fall prey to the predators of child abuse, child trafficking, child pornography and begging etc. they find themselves entangled in the world of disgrace, inhumanity and disrespectfulness from which they hardly escape or look for a shine of hope. With the introduction of the modern information technology they get entrapped into new modes of crime especially child abuse, child labour and child pornography.

However, our legislature brought certain provisions in the Information Technology Act, 2000 like section 67-A, 67-B and 67-C, to deal with the child pornography. There are certain provisions have also provided in The Protection of children from sexual offences Act, 2012 (POCSO ACT) to protect the children from the pornography apart from section 292 and 293 of Indian Penal Code.

3. CYBER TERRORISM.

Before we can discuss the possibilities of “cyber terrorism”, we must have some working definition of it. The word “cyber terrorism” refers to two elements i.e. cyber space and terrorism.

Another word for cyber space is the “virtual world” i.e. a place in which computer programs function and data moves. Terrorism is a much-used term, with many definitions.

For the purposes of this session, we will use the combine definition given by United States Department of state i.e. “The term ‘terrorism’ means premediated, politically motivated violence perpetrated against non-combatant targets by sub national groups or clandestine agents.”

If we combined these definitions, we construct a working definition i.e. “Cyber terrorism is the premediated, politically motivated attack against information, computer systems, computer programs and data which results in violence against combatant targets by sub national groups or clandestine agents”.

The basic definition of cyber terrorism subsumed over time to encompass such things as simply defacing a web site or server or attacking non-critical systems, resulting in the term becoming less useful. There is also a train of thought that says cyber terrorism does not exist and is really a matter of hacking or information warfare. Some may disagree with labelling it terrorism proper because of the unlikelihood of the certain of fear of significant physical harm or death in a population using electronic means, considering current attack and protective technologies.

Who are Cyber Terrorists?

From American point of view the most dangerous terrorist group is Al-Qaeda which is considered the first enemy for the US. According to US official’s data from computer seized in Afghanistan indicate that the group has scouted systems that control American energy facilities, water distribution, communication systems and other critical infrastructure.

After April 2001 collision of US Navy spy plane and Chinese fighter jet, Chinese hackers launched Denial of Service (DOS) attack against American Web Sites.

A study that covered that the most dangerous nation for originating malicious cyber-attack are the United States, South Korea, China, Germany, France, UK and Israel.

One group called World’s Fantabulas Defacers (WFD) attacked many Indian sites. Also there is another pro Pakistan group called Anti India Crew (AIC) who launched many cyber attacks against India.

Why do they use Cyber Attacks?

Cyber terrorist prefer using the cyber attack methods because of many advantages for it.

I,e. It is cheaper than traditional methods.
The action is very difficult to be tracked.
They can hide their personalities and location.
There are no physical barriers or check points to cross.
They can do it remotely from anywhere in the world.
They can use this method to attack a big number of targets.
They can affect a large number of people at a time.

Forms of Cyber Terrorism.

A. Privacy violation.
B. Secret Information appropriation and data theft.
C. Demolition of e-governance base.
D. Distributed denial of services attack.
E. Network damage and disruptions.

Through these form of cyber-attacks, cyber terrorists can destroy the economy of the country by attacking the critical infrastructure of the country like attacking the banks and financial institutions and play with their computer systems. These cyber terrorists have tried number of times to target the electric power grids, transportation systems and other international websites. These cyber terrorists are endangered the security of the nation by targeting the sensitive and secret information by stealing, disclosing or destroying it.

4. CYBER DEFAMATION

Under this, wrongdoer can publish defamatory statements against you at cyber space to defame you at public at large. It is a civil as well as criminal wrong. Under civil law the wrongdoer is liable to pay compensations and damages to the victim and in criminal wrong it is punishable under section 499 and 500 of IPC.

There are several areas on the internet where there is a real risk of liability for defamation. The fact that a user is alone with his computer and distanced from other users creates a sense of intimacy. There is no spoken/ telephonic conversation or dictated correspondence that would normally in still some caution. In addition, the notion that the internet is a ‘free for all’ cyber space where there are no limits or

boundaries results in a user's sense of social norms and propriety getting blurred.

Cyber defamation need not be necessarily be directed an individual victim but it could be harmful to the whole society. Similarly, it is also an offence, which affects the country's economy and not merely the wealth of an individual victim. It is also affect the corporate houses, so its share value be adversely affect.

5. CYBER CRIMES- FINANCIAL FRAUDS.

I. Money Loundering: There are may ways in which a criminal can illegally acquire money electronically. Whether it's through malicious malware, phishing, vishing and smishing scams, account takeovers or other vectors, a commonality across all these attack methods is that fraudster will need to move the illicit funds fast to avoid being caught and have the sum confiscated.

In traditional money laundering schemes, the placement of funds begins when tainted money is put into a financial institution. When funds are stolen online through digital transactions at financial institutions, the process immediately jumps to layering.

Basically, Money laundering is used to be done in three ways i.e. 1. Moving funds within the financial system. 2. Moving funds into unregulated financial e-cash systems and 3. Removing funds from the financial system altogether.

1. **Moving funds within the financial system.** Moving funds within the financial system generally only occurs with very large sums of money. Some of the most common methods for this include of use offshore accounts, Anonymous shell accounts, money mules and unregulated financial services.

   A. offshore accounts.

   Individuals can transfer stolen money funds into offshore account in a locale where bank secrecy laws are very strict. For example Swiss Bank at Switzerland. These countries are often referred to as tax heavens.

   Financial institutions, trusts, shell corporation and other financial groups in these regions may welcome money from

almost everywhere and often do not require disclosure of information regarding where the money originated from. In these institutions do not file any reporting back to the country in which the funds were generated.

B. **Anonymous Shell Accounts.** A shell company, bank, account or corporation is an entity that conducts no real business. It is essentially a cover used to hide and move funds. The purpose of these accounts is to deceive others into thinking the business is legitimate while laundering money and evading taxes. It is basically conceal the identity of the beneficial owner of the funds and the company records are often more difficult for law enforcement to access because they are offshore, held by professionals who claim secrecy or the professionals who run the company may act on remote and anonymous instructions.

C. **Money Mules.** A money mule is a person who receives and transfers funds acquired illegally for others. Most mules receive commission for their efforts.

2. **Unregulated Financial Services.** Unregulated entities may offer a variety of services that can be applied for criminal purposes. Many things fit into this category, such as:-
   A. **Electronic Money.** Stored value cards allow electronic money to put onto the card directly and then used to purchase goods and services.
   B. **Casinos.** In recent years, the financial crimes enforcement network placed regulatory requirements on casinos due to large sum of money and high frequency of transactions at these establishment. In casinos savvy criminals use it to move their illicit funds.
   C. **Underground networks of money dealers.** This refer to conduits through which money is transferred via informal methods. Which is used for money laundering, criminal activity and terrorist financing.

3. **Removing funds from the financial system altogether.**

Credit Card Frauds: Credit card or debit card fraud is a form of identity theft that involves an unauthorised taking of another's card information for the purpose of charging purchases to the account or removing funds from it. It is committed when a person fraudulently obtains, takes, signs, sells, buys or forges someone else's credit or debit card or card information.
Credit fraud is a broad term for the use of a credit card to buy goods or services with the intention of evading payments.

There are many ways that credit card thieves gather your personal information i.e.
like using your lost or stolen credit cards,
stealing from your mailbox,
looking over your shoulder during transactions,
going through your trash,
sending you unsolicited email,
making you false telephone solicitations and
looking at your personal records, etc. etc..

Stolen Cards:
When a credit card is lost or stolen, it may used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Most banks have free 24 hours telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorised purchases on a card before the card is cancelled. Without other security measures, a thief could potentially spend thousands of rupees.
Credit card frauds can be broadly classified into three categories, i.e. Card related frauds, merchant related frauds and internet related frauds.

There are different card frauds such as:-

A. **Application Fraud:** this type of fraud occurs when a person falsifies an application to acquire a credit card. Application fraud can be committed in three ways: Such as (1) **Assumed identity,** in this case an individual illegally obtains personal information of another individual and open accounts in his or

her name, using partially legitimate information. (2) **Financial Fraud**, in this case an individual provides false information about his or her financial status to acquire credit card. (3) **Non-received items,** it is also called as postal intercepts, it occurs when the card is stolen from postal services before it reaches to its owner's destination.

B. **Lost/Stolen Cards:** This type of fraud occurs when a legitimate cardholder loses the card or someone steals the card for criminal purpose.

C. **Amount Takeover:** this type of fraud occurs when a fraudster illegally obtains all the personal confidential information of any bonafide person. Ten being impersonate as genuine cardholder, he or she inform the bank that his residential or office address is changed. Or He or She reports that his credit card is lost and request for mailing of a new card to his new address. He or she receives the card and thus the criminal is able to successfully takeover the account.

D. **Counterfeit Card Fraud (It is also known as Skimming):** A counterfeit, cloned or skimmed card is one that has been printed, embossed or encoded without permission from the card company or one that has been validly issued and then altered or recorded. In most of the cases of counterfeit fraud involve skimming a process where the genuine data on a card's magnetic strips is electronically copied on to another card, without the knowledge of the legitimate cardholder. Skimming can occur at retail outlets, particularly at bars, restaurants and petrol pumps.

E. **Card not Present Fraud:** this type of fraud is conducted over the internet, by telephone, fax and mail order. It occurs when criminals obtain card details by the theft of card details of any individual from discarded receipt or by copying down details of cardholder during a transaction without the legitimate cardholder's knowledge. In this type of fraud neither the card nor the cardholder is present at the time of use of said card.

F. Triangulation: It occurs when a fraudster acts as a bogus intermediary to connect legitimate customer and the merchant. He advertises and sells an item, receives the payment and then fulfils the order by using stolen credit card details.

G. Mail Non-receipt Fraud: It occurs when a criminal intercepts a replacement card sent to a legitimate cardholder and uses it.

H. Identity Fraud: It occurs when someone illegally obtains personal information and repeatedly uses it to open new account or to initiate transaction in the name of legitimate customer. Majority of identity thefts occur offline like stealing the wallets/ intercepting the mail or rummaging through the trash.

D. Hacking:

Hacking is the most common type of cyber crime committed across the world. Hacking is defied in section 66 of the Information Technology Act, 2000 as "Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in the computer resources or diminishes its value or utility or affects it injuriously by any means, committing hacking." In simple words, hacking is a crime which entails cracking systems and gaining unauthorised access to the data stored in them. Hacker is a person who breaks in or trespass a computer system.

E. Virus Dissemination:

Virus are the programs which attach themselves to the computer or file and then circulate themselves to other files and to other components on a network. They usually affect the data on the computer, either by altering or deleting it.

F. Email Bombing:

An email bombing is more a form of internet abuse. Email bombing is an overload of emails directed to one particular email address, this will cause the person receiving the emails server to become sluggish or even crash. The email bombers may not necessarily be stealing anything from you but having a sluggish server can be a real pain and hard work to fix.

G. Forgery:

Sometimes counterfeit currency notes, postage and revenue stamps, mark-sheets etc can be forged using sophisticated computers, printers and scanners.

H. Data diddling:

It is altering a raw data before the computer processes it and then changing it back after the processing is completed. It may lead to huge losses to the organisations.

I. Salami Attacks:

It is a kind of cyber crime which is generally done to commit financial crimes. The key here is to make the alterations so insignificant that in a single case it would go completely.

J. Internet time thefts:

It is a kind of theft in which the internet surfing hours of the victims are used by some another person by gaining access to their ID and password.

K. Logic Bomb:

These are dependent programs i.e. these programs are created to do something only when certain event occurs. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

L. Electronic Money Laundering.

Money generated in large volumes illegally must be laundered before it can be spent or invested. One way to launder money is to transfer it electronically through messages between banks which is known as a "wire transfer". It had previously seemed impossible to monitor or screen wire transfers as they occur due to the tremendous volumes on transactions going through on a day to day to basis, however, banks are clamping down on the issue and filing away any suspicious activity.

So, with this note I would like to conclude this session now. Thank you so much to all of you.