Introduction to Cybercrime

INTRODUCTION

- "Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber-attacks".
- "Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
- Almost everyone is aware of the rapid growth of the Internet.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomenon; the first recorded cybercrime took place in the year 1820.It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend.

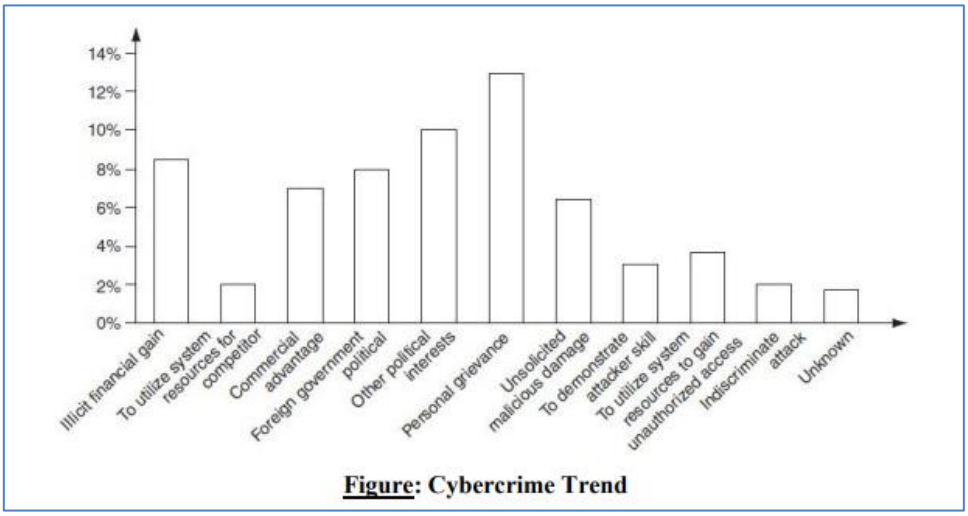

Figure: Cybercrime Trend

- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

✳CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD:

"A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime."

"As the name says, "cyber" means computer and "crime" means something unfair and illegal, which collectively means a crime executed using computer technologies. It could be that the computer may be involved in the crime or a target of a big one. This could harm someone's privacy and finances."

It comprises a wide range of crimes such as cyber fraud, financial scams, cybersex trafficking, ad scams, etc. Many privacy concerns refer to cyber crime when the privacy is intercepted and disclosed. The World Economic Forum 2020 Global Risk Report confirmed that organized cybercrime bodies are joining forces to execute criminal activities online. This also affects global GDP and the world economy as financial scams related activities are more notable and popular in the cyber world.

✳Types of attacks are prevalent

the legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:

1. Techno-crime: A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, “finger prints”.

2. Techno-vandalism: These acts of “brainless” defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

✳Types of Cybercrime:

1.Cyberterrorism

The act of terrorism is executed using computer technologies such as cyberspace or other computer resources. Acts of large-scale disruption mainly of computer networks connected to the internet using computer viruses and malware software. Government and IT specialists have recorded much increase in cyber terrorism since the early 2000s.

This could include-

- Phishing
- Hardware methods
- Programming scripts
- Threats such as
- Rape threats
- Death threats
- Harm to Mental health threats
- Malicious software.

2. Cyberpunk

The term, combining "cyber" and punk, possibly originated in 1980 with Bruce Bethke's short story, "Cyberpunk." The

people who are specialized in cryptography and crackers are those people who crack into computer security system.

Several categories of groups associated with cyberpunk:

- Hacker, who represent the best kind of cyberpunk
- Cracker, who attempt to break into computer systems
- Phreaker, who attempt to break into telephone systems
- Cyber-punks, who attempt to break codes and foil security systems

3.Cyber Fraud

This refers to an act of stealing E-data or gaining unlawful use of another computer system. This usually involves accessing a computer without permission or authorization.

The forms of computer fraud involve

- Hacking of a computer
- Sending malicious codes such as viruses
- Installing malware, suspicious software or spyware to steal data
- Phishing to perform scams on finance or banking details
- Identity Theft
- Sending hoax (seems to be good but, in reality, aren't) emails
- Data Mining
- This could usually cause monetary or identity harm.

4.Cyberwarfare:

Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying and paralyzing nations. This perception seems to be correct as the term's cyberwarfare and

Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. These types of Cyber-attacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare.

5.Cybersquatting:

Cybersquatting is registering, selling or using a domain name with the intent of profiting from the good will of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.

6.Drug Trafficking

Dark web or darknet markets are used to buy and sell drugs online. Some criminals use encrypted messaging software to communicate with drug mules. The dark web site "silk road" was the first major online marketplace of drugs. It was permanently shut down by the FBI in 2014. These markets got a major rise in recent years. There are many ways in which darknet markets can financially drain individuals-

- Virtual Private Networks (VPN)
- Tails
- Tor browser
- To hide their online presence.

⚜How to Prevent Being the Victims of These Crimes?

- Use strong passwords
- Keep your software updated
- Manage your social media settings
- Be aware of scams and online fraud
- The right use of a VPN
- Be updated on major security suits
- Know what to do when you become a victim.

✳Cybersecurity:

Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- Cybersecurity includes both the physical security of devices and the information stored in that. It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.
- Where financial losses to the organization due to insider crimes are concerned for example, leaking customer data, often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft.
- Cybercrimes take up a vital space in information security domain because of their impact. For anyone trying to compile data on business impact of cybercrime, there are number of challenges.

✳Cyber Security Goals

Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks.

This principle is called the **CIA** triad. The **CIA** model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

We can break the CIA model into three parts: Confidentiality, Integrity, and Availability.

Confidentiality

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others.

Integrity

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event.

Availability

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

⚜WHO ARE CYBERCRIMINALS?

Cybercrime involves such activities

- credit card fraud;
- cyberstalking;
- defaming another online;
- gaining unauthorized access to computer systems;
- ignoring copyright, software licensing and trademark protection;
- overriding encryption to make illegal copies;
- software piracy and stealing another's identity (known as identity theft) to perform criminal acts

Types of Cybercriminals:

1. Type I: Cybercriminals – hungry for recognition:

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threats)
- Politically motivated hackers;
- Terrorist organizations.

2. Type II: Cybercriminals – not interested in recognition:

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage)
- organized criminals

3. Type III: Cybercriminals – the insiders:

- Disgruntled or former employees seeking revenge;
- Competing companies using employees to gain economic advantage through damage and/or theft.

Classifications of Cybercrime:

Generally, almost all cyber-crimes can be classified under heads, depending on the groups they are targeted at. The heads are:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society
- Crimes emanating from Usenet newsgroup

1 Cyber-crimes against individuals:

Generally, ordinary individuals are the most vulnerable targets of cybercriminals. This is due to various reasons like lack of information, guidance, and cyber-security. As per a recent report published by Norton, 44% of individuals consider themselves as 'worthwhile targets' for hackers.

The following are some of the main cyber-crimes committed targeting individuals.

Email spoofing:

A spoofed email is one in which e-mail header is forged so that mail appears to originate from one source but actually has been 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. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life.

Phishing

Phishing refers to the fraudulent practice of sending emails under the pretext of reputable companies to induce individuals to reveal personal information, such as passwords, credit card numbers, etc., online. Phishing refers to the impersonation of a legitimate person and fraudulently stealing someone's data. Through phishing attacks, cybercriminals not only exploit innocent individuals but also spoil the reputation of well-known companies.

Section 66C of the IT Act penalizes any offender committing phishing-related activities. It provides that anyone who fraudulently uses an electronic signature, password or any other unique identification feature of any other person is punishable with imprisonment of up to three years and a fine of up to rupees one lakh.

Spamming:

People who create electronic Spam are called spammers. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, video sharing sites, etc.

Cyber defamation

Cyber defamation means injuring the other person's reputation via the internet through social media, Emails etc. There are two types of Cyber defamation: libel and slander.

Libel: It refers to any defamatory statement which is in written form. For instance, writing defamatory comments on posts, forwarding defamatory messages on social media groups, etc. are a part of cyber defamation in the form of libel.

Slander: It refers to any defamatory statement published in oral form. For instance, uploading videos defaming someone on YouTube is a part of cyber defamation in the form of slander.

Punishment for Cyber defamation is provided under Section 67 of the IT Act; whoever publishes or transmits a defamatory statement about a person shall be punished with 2 years imprisonment and a fine up to ₹25000.

Cyberbullying

The term cyberbullying is not defined under any Indian law. However, in general parlance, cyberbullying refers to bullying someone by threatening, harassing or embarrassing the victim using technology digital device. Generally, cyberbullying includes the following activities on the internet:

- Humiliating/embarrassing content posted online about the victim of online bullying,
- Hacking social media accounts
- Posting vulgar messages on social media
- Threatening the victim to commit any violent activity
- Child pornography or threatening someone with child pornography

In India, a whopping amount of almost 85% of children experiences cyberbullying. There are no specific provisions that deal with cyberbullying. Section 67 of the IT Act is the closest legal provision relating to cyberbullying. It penalizes anyone who transmits obscene materials in electronic form. The punishment for such transmission is imprisonment for a term which may extend to five years and a fine which may extend to ten lakh rupees.

Cyberstalking and harassment:

The dictionary meaning of “stalking” is an “act or process of following prey stealthily – trying to approach somebody or something.” Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization. The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

As the internet has become an integral part of our personal & professional lives, cyberstalks take advantage of ease of communication & an increased access to personal information available with a few mouse clicks or keystrokes. They are 2 types of stalkers: Online Stalkers: aim to start the interaction with the victim directly with the help of the internet. Offline Stalkers: the stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim.

Pornographic Offenses: Child pornography means any visual depiction, including but not limited to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

2.Cybercrime against property:

Credit card frauds

- Credit card fraud is when someone uses your credit card or credit account to make a purchase you didn't authorize. This activity can happen in different ways.
- If you lose your credit card or have it stolen, it can be used to make purchases or other transactions, either in person or online.
- Fraudsters can also steal your credit card account number, PIN and security code to make unauthorized transactions, without needing your physical credit card. (Unlawful transactions like these are known as card-not-present fraud.)

Intellectual Property (IP) Crimes:

With the growth in the use of internet these days the cyber-crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers. Copyrights and trade secrets are the two forms of IP that is frequently stolen. For example, stealing of software, business strategies etc. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it. Another major cyber theft of IP faced by India is piracy. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.

Internet time theft:

Internet time theft is a crime where the internet connection of one person is used by an unauthorized person. This is usually done by getting access to the user’s internet account details, such as user name and password, given by internet service provider. This access can be given voluntarily by the user for a stipulated time period, or it can be gained fraudulently. Wireless internet has made this theft more prevalent. It is easy to commit this crime if the victim is using an open Wi-Fi connection for internet access.

3.Cybercrime against Organization:

The cyber-crimes mainly targeting individuals may help cybercriminals get only a meagre amount of ransom, depending on the financial status of the targeted individuals. On the other hand, cyber-attacking large companies or organizations can help them get their hands on extremely confidential data of both private and public institutions or entities. Cyber-attacks on organizations are generally launched on a large scale to get a lump sum amount of ransom. Since such attacks drastically damage the companies' daily operations, most companies try to resolve them as fast as possible. The following are the kinds of cyber-crimes launched targeting organizations.

Unauthorized accessing of computer

o Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access.

Password sniffing

o Password sniffing is a technique used to gain knowledge of passwords that involves monitoring traffic on a network to pull out information. There are several software's available for automatic password sniffing.

Virus attacks/dissemination of Viruses:

Computer virus is a program that can "infect" legitimate (valid) programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. A computer virus passes from computer to computer in a similar manner as a biological virus passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. Viruses can take some typical actions:

- Display a message to prompt an action which may set of the virus
- Delete files inside the system into which viruses enter
- Scramble data on a hard disk
- Cause erratic screen behaviour
- Halt the system (PC)
- Just replicate themselves to propagate further harm.

E**-mail bombing/mail bombs:**

Email bombing is characterized by an abuser sending huge volumes of e-mail to a target address resulting in the victim's e-mail account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. o If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. E-mail bombing is commonly carried out using botnets (private internet-connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. o This type of attack is more difficult to control due to multiple source addresses and the bots, which are programmed to send different messages to defeat spam filters.

Data diddling

It is a illegal or unauthorized data alteration. These changes can occur before and during data input or before output. It has affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other form of data processing know.

Logic Bomb:

A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

Trojan Horse:

A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.

Salami attack/salami technique:

Salami Attack (also known as Salami Slicing) refers to as fraudulent action by alternation of systems either by modification or insertion of malicious program and the main purpose of this for financial gain. A salami attack is considered a minor attack that can be repeated many times, a simple example is referred to as stealing of specific small amount of money from every customer's bank account in a particular bank.

o It is very hard for such attack to be notice by customers and such attack are reportedly mostly conducted by crime minded bank's officials.

This cyber-crime usually goes undetected and unnoticed because of nature and form of the crime, because only small amounts are deducted severally in a specific period of time.

4.Cybercrime against society:

Forgery:

Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates. These are made using computers and high-quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

Cyberterrorism

Cyberterrorism is committed and planned activity in cyberspace via computer networks. It consists of the usage of e-mail for communications among co-conspirators to communicate records for use in violent activities as well as recruiting terrorist institution individuals through internet sites. It also includes:

a) Air visitors control computer systems which reason the planes to collide or crash.
b) Infiltrating water treatment plant computer structures to reason infection of water supplies.
c) Hacking into medical institution databases and changing or deleting facts that could result in incorrect, risky remedy of a patient or sufferers.
d) Disrupting the electric power grid, this will motive lack of air conditioning in summer and warmth in iciness or result in the dying of folks.

Web Jacking:

Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves "password sniffing". The actual owner of the website does not have any more control over what appears on that website.

5.Crimes emanating from Usenet newsgroup:

By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabelled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk. Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

🔰Cybercrime and the Indian ITA 2000:

The Information Technology Act, 2000 also Known as an IT Act is an act proposed by the Indian Parliament reported on 17th October 2000. This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997. It is the most important law in India dealing with Cybercrime and E-Commerce.

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

- First Schedule – Deals with documents to which the Act shall not apply.
- Second Schedule – Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

- Tampering with the computer source documents.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Publishing of information which is obscene in electronic form.
- Penalty for breach of confidentiality and privacy.
- Hacking for malicious purposes.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Penalty for misrepresentation.
- Confiscation.
- Power to investigate offences.
- Protected System.
- Penalties for confiscation not to interfere with other punishments.
- Act to apply for offence or contravention committed outside India.
- Publication for fraud purposes.
- Power of Controller to give directions.

Sections and Punishments under Information Technology Act, 2000 are as follows :

Section	Offence	Punishment
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70.	Imprisonment of either description up to 10 years and fine.

71	Misrepresentation to the controller to the certifying authority.	Imprisonment up to 2 years and/or fine up to₹ 1 lakh.
72	Breach of confidentiality and privacy.	Imprisonment up to 2 years and/or fine up to ₹1 lakh.

72-A	Disclosure of information in breach of lawful contract.	Imprisonment up to 3 years and/or fine up to ₹ 5 lakh.
73	Publishing electronic signature certificate false in certain particulars.	Imprisonment up to 2 years and/or fine up to ₹ 1 lakh.
74	Publication for fraudulent purpose.	Imprisonment up to 2 years and/or fine up to ₹ 1 lakh.

Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.

✅ A Global Perspective on Cybercrimes

- In Australia, cybercrime has a slender legal meaning as used in the Cyber Crime Act 2001, which details offenses against computer data and systems.
- At international level cybercrime has a broad meaning.
- One example of cybercrime is, cyber criminals tried to celebrate the valentine 's day in advance in the year 2000 so they chose the dates 6, 7 and 8 February to greet the e-commerce site happy valentine's day in advance that is before the 14th of February, the e-commerce sites buy.com, Yahoo, eBay, and amazon.com were slow and shut down for hours.
- At that time the cyber criminals also send one virus called "I love you" this virus spread very rapidly and results in great loss.
- In year 1999 Melissa virus spread around, this virus affects the e-mail system and results in a huge loss.
- In recent time some hackers group were also active. One group from Pakistan called 'G' hacked and defeated more than 40 Indian websites.
- The websites they hacked were: Agricultural University of Maharashtra, National Research Centre Asian Age newspaper, Indian Science Congress, Indian Institute of Management Ahmadabad, the Gujarat government Indian Institute of Technology Madras Centre for electronics design and Technology, Glaxo welcome, the Gujarat government and some other websites.
- The second group called 'Doctor Nuker' which is founder of Pakistan hackers club hacked sites of Indian Parliament, Ahmadabad telephone exchange, engineering export, Promotion Council, and United Nations (India).
- The third group called 'nightman' hacked websites owned by government and website set up by the Indian companies.
- Some of the sites this group has ruined are Blue Star InfoTech, Lal Bahadur Shastri National Academy of Administration and Mahindra and Mahindra.
- Every year indian government is spending lots of money on e-security. Actions are taken against the cybercrime but still day by day it is growing.
- The Council of Europe's (CoE's) cybercrime treaty, includes the cyber-criminal activity like copyright offenses, computer-related offenses, offenses against computer data and systems, and content offenses.

- Cybercrimes wide definition is divided into white-collar crime and economic crime.
- There are countries like Argentina, Australia, Brazil, and Canada etc which are taking action against spam. These countries are restricting the use of email spam.

Cyber Terrorism/Cyber Crime

In India, cyber terrorism has become new era in the cyber world. Let us discuss cyber terrorism (the name used by media first time after 26/11) in detail; Indian government got considerable evidences against 2008 serial blasts in cities like Mumbai, Ahmedabad, Delhi, Jaipur, and Bangalore.

I remember the day 26/11 when I was in Mumbai for pursuing my Master of Engineering we listen the news there are dozens of terrorist attacked on Hotel Taj, C.S.T. station and hotels at Nariman points.

Even have seen and received all the videos of attacks on these places. During these attacks terrorist used all the latest digital technology like satellite phones even they used all type of network attacks fake IP address etc and all.

The day onwards Indian government feels where we are in terms of technology and security of the country.

So, they tighten the physical security and made the provision of Information Technology Act 2000 we will discuss all these IT acts in next point.

In spite of doing all these effort towards implementing security in July 2011, the use of digital technology was further used for bomb blasts in a crowded city market in Jhaveri Bazaar, Mumbai.

Without discussing more on background history of Cyber terrorism we will start directly from definition of cyber terrorism/ crime which will vary from author to author :

"The crime which shows illegal behaviour of the person targeted on the security of the different popular places, population of the country by sending threatening emails on government sites and hacking or cracking government servers through denial of service attacks".

Currently many people instead of normal usage of Internet they are using it for creating online banking frauds, unauthorized access of resource, damage to computer data or programs, unauthorized interception of communications, online share trading fraud, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common, Do you thing that we need a strong cyber laws to tackle all these cybercrimes of extensive and misuse of computer systems connected to Internet ?