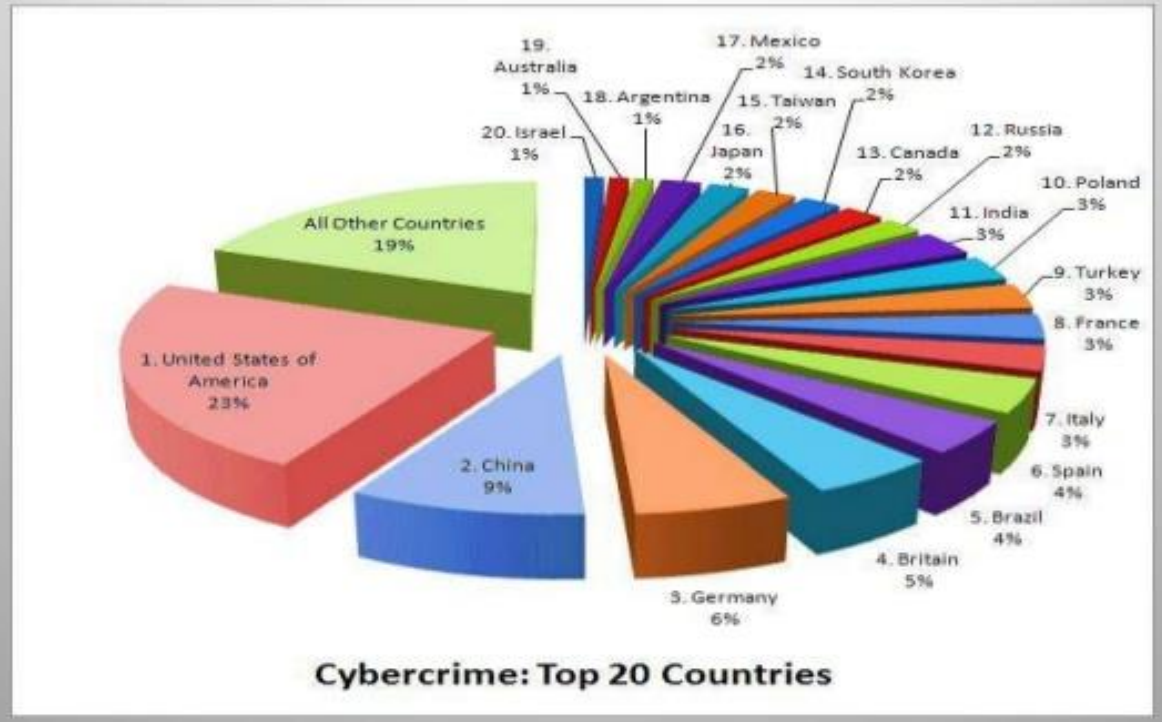
INTRODUCTION TO CYBER CRIME & LAW

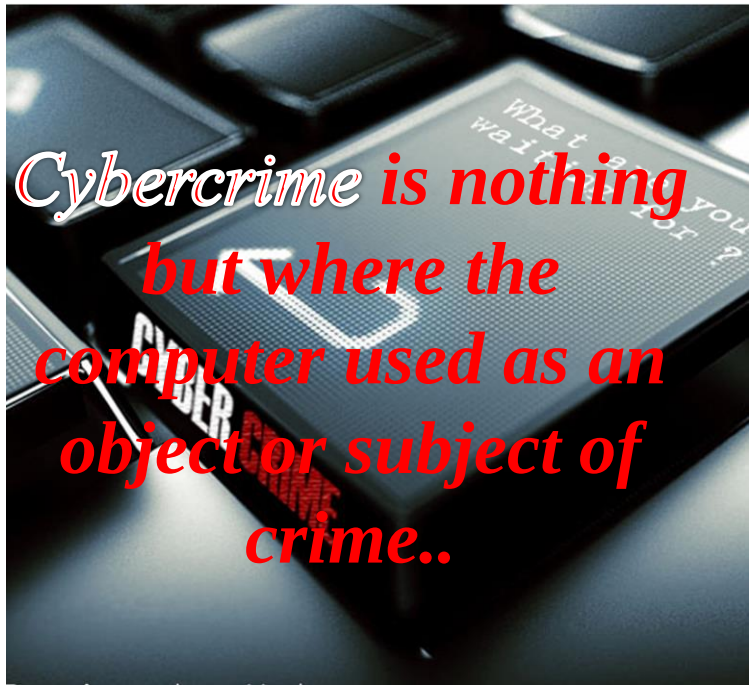
Cybercrime



India stands 11th in the ranking for Cyber Crime in the World, constituting 3% of the Global Cyber Crime.

Cyber Crime

- The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education.
- There're two sides to a coin. Internet also has it's own disadvantages is Cyber crime- illegal activity committed on the internet.



Cyber Crimes

- Criminal activities carried out by means of computers or the Internet.
- Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone.
- The first recorded cyber crime took place in the year 1820
- The Department of Justice divides cybercrime into three categories:

1) crimes in which the computing device is the target, for example, to gain network access;

2) crimes in which the computer is used as a weapon, for example, to launch a denial of service (DOS) attack;

3) crimes in which the computer is used as an accessory to a , for example, using a computer to store illegally-obtained data.

- At the onset, let us satisfactorily define "cyber crime" and differentiate it from "conventional Crime". Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a scope of new age crimes that are addressed by the Information Technology Act, 2000.
- Defining cyber crimes, as "acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be "unlawful acts wherein the computer is either a tool or a target or both".

Let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

- **Financial crimes:** This would include cheating, credit card frauds, money laundering etc.
- **Sale of illegal articles:** This would include sale of downers, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.
- **Online gambling (internet gambling) :** There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.
  - **Gambling** can be **defined** as risking money or anything of material value for unsure results. The initial intent is to win additional money or material goods. **Online gambling**, more commonly known as Internet **gambling**, is typically **betting** on casino or sports type games over the Internet.

- **Intellectual Property crimes :** These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.
- **Email spoofing :** A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Pooja has an e-mail address pooja@asianlaws.org. Her enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life.

Frequently Used Cyber Crimes

- **Unauthorized access to computer systems or networks :** This activity is commonly referred to as hacking. The Indian law has however given a different meaning to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking".
- **Theft of information contained in electronic form :** This includes information stored in computer hard disks, removable storage media etc.
- **Email bombing :** Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
  - In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the schemes was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

- **Data diddling :** This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.
  - **Data diddling** (also called false **data** entry) is. “ [t]he unauthorized changing of **data** before or during their input to a computer system. Examples are forging or counterfeiting documents and ex- changing valid computer tapes or cards with prepared replacements.
- **Salami attacks :** These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

- **Virus / worm attacks :** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.
- **Logic bombs :** These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because their story hidden all through the year and become active only on a particular date.

- **Trojan attacks :** A Trojan as this program is properly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing. There are many simple ways of installing a Trojan in someone's computer.
- **Trojans** are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, **Trojans** do not reproduce by infecting other files nor do they self-replicate.

Types of Cyber crime

- **Hacking:** In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.
- **Theft:** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
- **Cyber Stalking:** This is a kind of online harassment
- **Identity Theft:** This has become a major problem with people using the Internet for cash transactions and banking services.
- **Attack Vector**: An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Eg: malicious email, attachments, worms, web pages, downloads

continue

- **COMPUTER VANDALISM:** Damaging or destroying data rather than stealing.& Transmitting virus
- **CYBER TERRORISM:** Use of Internet based attacks in terrorist activities.

Traditional Crime Associated with Computer Crime

- The only difference between a traditional crime and a cyber-crime is that the cyber-crime involves in a crime related to computers. Let us see the following example to understand it better:
- Traditional Theft: A thief breaks into Ram’s house and steals an object kept in the house.
- Hacking: A Cyber Criminal/Hacker sitting in his own house, through his computer, hacks the computer of Ram and steals the data saved in Ram’s computer without physically touching the computer or entering in Ram’s house.

Cyber Hacking

- **Computer hacking** refers to the practice of modifying or altering **computer** software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in **computer hacking** activities are typically referred to as “**hackers**.”

Cyberspace & Criminal Behavior

- **Cyberspace** is "the imaginary environment in which communication over computer networks occurs.
- Cyberspace can be defined as an complex environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.
- **Criminal behavior** is defined as an act or failure to act in a way that interrupts public law. Public law is most often established by a governing body, and will therefore vary between countries and states.

Cyber Law

- Cyber Law is the law governing cyber space.
- Cyber space is a very wide term and includes computers, networks, software, data storage devices. (Such as hard disks, USB disks etc.), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.
- Law includes the rules of conduct:
  - 1. That have been approved by the government,
  - 2. Which are in force over a certain territory,
  - 3. Which must be obeyed by all persons on that territory?
- Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation.
- Cyber law encompasses laws relating to:
  - 1. Cyber Crimes
  - 2. Electronic and Digital Signatures
  - 3. Intellectual Property
  - 4. Data Protection and Privacy

- **Cybercrimes** are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a remarkable shot in incidents of cybercrime.
- **Electronic signatures** are used to authenticate electronic records. **Digital signatures** are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

- **Intellectual property** is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The faces of intellectual property that relate to cyber space are covered by cyber law. These include:
  - Copyright law in relation to computer software, computer source code, websites, cell phone content etc.
  - Software and source code licenses
  - Trademark law with relation to domain names, Meta tags, mirroring, framing, linking etc.
  - Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts,
  - Patent law in relation to computer hardware and software.

- **Data protection and privacy laws** aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Need for Cyber Law

- There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below.
- 1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
- 2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank's electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

- 3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

- 4. Cyberspace offers enormous potential for privacy to its members. Readily available encryption software and stenographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

- 5. Cyberspace offers never-seen-before economic efficiency. Billions of dollars‖ worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty.

- 6. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds.

- 7. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

- 8. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities. Here the ‘original‘ information, so to say, remains in the possession‘ of the owner‘ and yet information gets stolen.

Incident Response

- **Incident response** is an organized approach to addressing and managing the result of a security attack (also known as an **incident**). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
- Incident response plans are just as important as disaster recovery plans.
- Incidents are situations that could turn into a disaster if not handled properly, and are often the first step in detecting a disaster.

Digital Forensics

- Computer **forensics** is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.
- **Digital forensics** (sometimes known as **digital forensic** science) is a branch of **forensic** science encompassing the recovery and investigation of material found in **digital** devices, often in relation to **computer** crime.

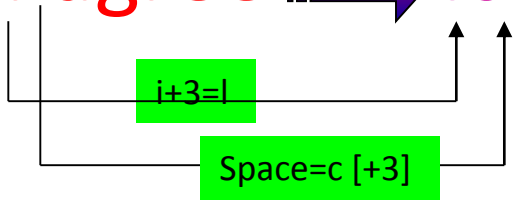
Digital Signatures

- Electronic Record

1. Very easy to make copies
2. Very fast distribution
3. Easy retrieval
4. Copies are as good as original
5. Easily modifiable
6. Environmental Friendly

Encryption

- Caesar Cipher
- The shift is linear and equidistributed 3 changes
- I agree → lcdjuhh



ENCRYPTION

Message 1

Central to the growth of e-commerce and e-governance [illegible] the issue of trust in electronic environment.

Encrypted Messa[illegible]

9a46894335be49f0b9
71b275bbb0adb405e
dd135285482

Same Key
SYMMETRIC

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encrypted Message 2

a[illegible]b61a770f947ca856cd675463f1c95
a9a[illegible]71f80830c87f5715f5f593348[illegible]
8dd7e[illegible]
67c3[illegible]

Different Keys
[Keys of a pair – Public and Private]
ASYMMETRIC
[PKI]

DECRYPTION

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd98571b
275bbb0adb405e6931e856ca3e5e569edd13528
5482

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95a9a2b
8d4e6a71f80830c87f5715f5f59334978dd7e97da
0707b48a1138d77ced56feba2b467c398683c7db
eb86b854f120606a7ae1ed934f5703672adab0d7
be66dccde1a763c736cb9001d0731d541106f50b
b7e54240c40ba780b7a553bea570b99c9ab3df13
d75f8ccfdddeaaf3a749fd1411

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

What is Digital Signature?

- **Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document**
  - **Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.**
  - **As the public key of the signer is known, anybody can verify the message and the digital signature**

Digital Signatures

Each individual generates his own key pair
[Public key known to everyone & Private key only to the owner]

Private Key – Used for making digital signature

Public Key – Used to verify the digital signature