# CYBER LAW AND ETHICS

Faculty:
MOHAMMED RAHMAT ALI,
Asst. Professor, Dept of CSE.

# UNIT-I

- **Cyber laws and rights in today's digital age**; IT Act, Intellectual Property Issues connected with use and management of Digital Data The similar Acts of other countries

- **Information Warfare**: Nature of information warfare, including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information How, electronic bombs, and sops and perception management.

# What is 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 encompasses the rules of conduct:

1. that have been approved by the government, and
2. which are in force over a certain territory, and
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

# Cyber crimes

- Cyber crimes 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 phenomenal spurt in incidents of cyber crime.
- These crimes are discussed in detail further in this chapter.
- A comprehensive discussion on the Indian law relating to cyber crimes and digital evidence is provided in the ASCL publication titled “Cyber Crimes & Digital Evidence – Indian Perspective”

# Electronic signatures

- 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. These issues are discussed in detail in the ASCL publication titled “Ecommerce – Legal Issues”.

# Intellectual property

- Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets 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 licences

• 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.

These issues are discussed in detail in the ASCL publication titled "IPR & Cyberspace - the Indian Perspective".

# Data protection and privacy

- 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.

# Categories of cyber crime

- Cyber crime against persons
- Cyber crimes against property
- Cyber crimes against government

**Against a person**

* Cyber stalking
* Impersonation
* Loss of privacy
* Transmission of obscene material
* Harassment with the use of computer

# Against Property

- Un authorized computer trespassing
- Computer vandalism
- Transmission of harmful programmes
- Stealing secret information & data
- Copy rights Against Property

**Against government**

- * Hacking government website
- * Cyber extortion
- * Cyber terrorism
- * Computer viruses

**Some other crimes:**

- Logic bombs -virus, worms, Trojan horse, email bombing
- Spamming - E-mail abuse

# 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.

- Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
- 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.

# Need for Cyber Law(cont'd)

- 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.
- Cyberspace is absolutely open to participation by all. A ten year-old in Bhutan can have a live chat session with an eight year-old in Bali without any regard for the distance or the anonymity between them.
- Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

# Need for Cyber Law(cont'd)

- 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.
- Electronic information has become the main object of cyber crime. 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.

# Need for Cyber Law(cont'd)

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

# Cyber Laws of India

- In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

- **We can categorize Cyber crimes in two ways**
- The Computer as a Target :-using a computer to attack other computers.
  e.g. Hacking,Virus/Worm attacks,DOS attack etc.
- The computer as a weapon :-using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

# Cyber Law in INDIA

- **Why Cyberlaw in India ?**

- When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be are many disturbing things happening in cyberspace. misused for criminal activities and which required regulation. Today, there Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

- **What is the importance of Cyberlaw ?**

- Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

- **Does Cyberlaw concern me ?**

- Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit

# Advantages of Cyber Laws

- The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
- Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

- The Act now allows Government to issue notification on the web thus heralding e-governance.
- The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
- Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

# INFORMATION WARFARE

Information is not a new component to conflict.

The Information Age, however, has ushered in extraordinary improvements in collection, storage, analysis, and transmission of information.

# Defining Information Warfare

**Information Warfare**: Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

# Direct and Indirect Information Warfare

Direct Information Warfare changes the adversary's information without involving the intervening perceptive and analytical functions.

Indirect Information Warfare changes the adversary's information by creating phenomena that the adversary must then observe and analyze.

# Information Warfare: Past and Present

Information warfare is not a new phenomenon.

*For centuries, cryptography has been used to conceal and reveal messages. The word cipher is derived from the seventh century Arabic word sifr, meaning "nothing."*

Two of the more famous information warfare examples include the German Enigma machine and the use of Native American "codetalkers."

*Since the 1970s, extraordinary improvements in the technical means of collecting, storing, analyzing, and transmitting information have contributed to codemaking and codebreaking as well as begun the shift toward a "Revolution in Military Affairs."*

# Information Warfare

- Definition:

  "..actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems"

  Source: U.S Defense Information Systems Agency DISA

# Information Warfare

- Three General Categories:
- Offensive
  - To deny, corrupt, destroy, or exploit adversary's information
- Defensive
  - To safeguard ourselves and allies from similar actions
- Exploitation
  - To exploit information in a timely fashion, to enhance our decision/action cycle and disrupt the adversary's cycle

# Information Warfare

- Operation Desert Storm
  - Knocked out communications systems
  - Attempted to disrupt economy prior to the operation
- UN in Bosnia
  - Knocked out communications
  - Disrupt the economy
  - Propaganda and Misinformation

# What Constitutes Information Warfare?

Traditional forms of Information Warfare

1. Psychological Operations
2. Electronic Warfare
3. Physical Destruction
4. Security Measures
5. Information Attack

# Psychological Ops

Psychological operations use information to affect the enemy's reasoning.

*"We can be sure that the global battlefield of the 21st century will be over information -- the dissemination or withholding of facts, the interpretation of events, the presentation or distortion of ideas and ideologies, and the communication of messages and symbols carefully prepared to provoke a particular reaction, either conscious or unconscious, from a target audience."*

# Electronic Warfare

Electronic Warfare denies accurate information to the enemy.

Any military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and the action which retains friendly use of the electromagnetic spectrum. The three divisions within EW include electronic countermeasures, electronic counter-countermeasures, and electronic warfare support measures.

# Military Deception

Military deception misleads the enemy about our capabilities or intentions.

*Successful deception causes enemies to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives.*

# Physical Destruction

Physical destruction can assist information warfare by affecting information system elements through destructive power.

*The means of physical attack range from conventional bombs to electromagnetic pulse weapons. This is one of the most important areas where the United States may be vulnerable to attack.*

# Security Measures

Security measures seek to keep the adversary from learning about our military capabilities and intentions.

# Cyberterrorism and Other Potenial Attacks

What types of information are at risk?

1. Power delivery
2. Communications
3. Aviation
4. Financial services
5. Medical records
6. Criminal records
7. Business plans

# New Ways of Conceiving the Global World

- Incredibly powerful and vastly expanding communications technologies have forced us to consider the world as a smaller environment.

- Multinational corporations and communications networks have also helped to diminish the importance of national borders.

# Cyber security threats

- Cyber security threats reflect the risk of experiencing a cyber attack. A cyber attack is an intentional and malicious effort by an organization or an individual to breach the systems of another organization or individual. The attacker's motives may include information theft, financial gain, espionage, or sabotage.

# What are the main types of cyber security threats?

- The main types of cyber threats are:
- Distributed denial of service (DDoS)
- Man in the Middle (MitM)
- Social engineering
- Malware and spyware
- Password attacks
- Advanced persistent threats (APT)

# Distributed denial of service (DDoS)

- The objective of a denial of service (DoS) attack is to overwhelm the resources of a target system and cause it to stop functioning, denying access to its users. Distributed denial of service (DDoS) is a variant of DoS in which attackers compromise a large number of computers or other devices, and use them in a coordinated attack against the target system.
- DDoS attacks are often used in combination with other cyber threats. These attacks may launch a denial of service to capture the attention of security staff and create confusion, while they carry out more subtle attacks aimed at stealing data or causing other damage.

# Methods of DDoS attacks include:

- **Botnets**—systems under hacker control that have been infected with malware. Attackers use these bots to carry out DDoS attacks. Large botnets can include millions of devices and can launch attacks at devastating scale.
- **Smurf attack**—sends Internet Control Message Protocol (ICMP) echo requests to the victim's IP address. The ICMP requests are generated from 'spoofed' IP addresses. Attackers automate this process and perform it at scale to overwhelm a target system.
- **TCP SYN flood attack**—attacks flood the target system with connection requests. When the target system attempts to complete the connection, the attacker's device does not respond, forcing the target system to time out. This quickly fills the connection queue, preventing legitimate users from connecting.

# Man-in-the-middle attack (MitM)

- When users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system. In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server.
- Once the attacker has intercepted communications, they may be able to compromise a user's credentials, steal sensitive data and return different responses to the user.

# MitM attacks include:

- **Session hijacking**—an attacker hijacks a session between a network server and a client. The attacking computer substitutes its IP address for the IP address of the client. The server believes it is corresponding with the client and continues the session.
- **Replay attack**—a cybercriminal eavesdrops on network communication and replays messages at a later time, pretending to be the user. Replay attacks have been largely mitigated by adding timestamps to network communications.
- **IP spoofing**—an attacker convinces a system that it is corresponding with a trusted, known entity. The system thus provides the attacker with access. The attacker forges its packet with the IP source address of a trusted host, rather than its own IP address.
- **Eavesdropping attack**—attackers leverage insecure network communication to access information transmitted between client and server. These attacks are difficult to detect because network transmissions appear to act normally.

# Social engineering attacks

- Social engineering attacks work by psychologically manipulating users into performing actions desirable to an attacker, or divulging sensitive information.

# Social engineering attacks include:

- **Phishing**—attackers send fraudulent correspondence that seems to come from legitimate sources, usually via email. The email may urge the user to perform an important action or click on a link to a malicious website, leading them to hand over sensitive information to the attacker, or expose themselves to malicious downloads. Phishing emails may include an email attachment infected with malware.
- **Spear phishing**—a variant of phishing in which attackers specifically target individuals with security privileges or influence, such as system administrators or senior executives.
- **Homograph attacks**—attackers create fake websites with very similar web addresses to a legitimate website. Users access these fake websites without noticing the slight difference in URL, and may submit their credentials or other sensitive information to an attacker.

# Malware and spyware attack

- Attacks use many methods to get malware into a user's device. Users may be asked to take an action, such as clicking a link or opening an attachment. In other cases malware uses vulnerabilities in browsers or operating systems to install themselves without the user's knowledge or consent.
- Once malware is installed, it can monitor user activities, send confidential data to the attacker, assist the attacker in penetrating other targets within the network, and even cause the user's device to participate in a botnet leveraged by the attacker for malicious intent.

# Malware and spyware attacks include:

- **Trojan virus**—tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.
- **Ransomware**—prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid.
- **Malvertising**—online advertising controlled by hackers, which contains malicious code that infects a user's computer when they click, or even just view the ad. Malvertising has been found on many leading online publications.
- **Wiper malware**—intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.
- **Drive-by downloads**—attackers can hack websites and insert malicious scripts into PHP or HTTP code on a page. When users visit the page, malware is directly installed on their computer; or the attacker's script redirects users to a malicious site, which performs the download. Drive-by downloads rely on vulnerabilities in browsers or operating systems.
- **Rogue security software**—pretend to scan for malware and then regularly show the user fake warnings and detections. Attackers may ask the user to pay to remove the fake threats from their computer or to register the software. Users who comply transfer their financial details to an attacker.

# Password attacks

- A hacker can gain access to the password information of an individual by ‘sniffing’ the connection to the network, using social engineering, guessing, or gaining access to a password database. An attacker can ‘guess’ a password in a random or systematic way.

# Passwords attacks include:

- **Brute-force password guessing**—an attacker uses software to try many different passwords, in the hope of guessing the correct one. The software can use some logic to trying passwords related to the name of the individual, their job, their family, etc.
- **Dictionary attack**—a dictionary of common passwords is used to gain access to the computer and network of the victim. One method is to copy an encrypted file that has the passwords, apply the same encryption to a dictionary of regularly used passwords, and contrast the findings.

# Top Cyber security Challenges

- In addition to the more specific issues covered above, there are also broader challenges faced by many cyber security teams. Below are a few of the most common current challenges.

# Mobile devices are difficult to manage and secure

- Even if people haven't fully embraced smart technologies, nearly everyone has a mobile device of some sort. Smartphones, laptops, and tablets are common. These devices are often multipurpose, used for both work and personal activities, and users may connect devices to multiple networks throughout the day.
- This abundance and widespread use make mobile devices an appealing target for attackers. Targeting is not new but the real challenge comes from security teams not having full control over devices. Bring your own device (BYOD) policies are common but these policies often do not include internal control or management.
- Often, security teams are only able to control what happens with these devices within the network perimeter. Devices may be out of date, already infected with malware, or have insufficient protections. The only way security teams may have to block these threats is to refuse connectivity which isn't practical.

# The complexity of cloud environment

- With businesses moving to cloud resources daily, many environments are growing more complex. This is particularly true in the case of hybrid and multi-cloud environments, which require extensive monitoring and integration.
- With every cloud service and resource that is included in an environment, the number of endpoints and the chances for misconfiguration increase. Additionally, since resources are in the cloud, most if not all endpoints are Internet-facing, granting access to attackers on a global scale.
- To secure these environments, cybersecurity teams need advanced, centralized tooling and often more resources. This includes resources for 24/7 protection and monitoring since resources are running and potentially vulnerable even when the workday is over.

# Sophisticated phishing exploits

- Phishing is an old but still common tactic used by attackers to gain sensitive data, including credentials and financial information. In the past, phishing emails were vague, often posing as authority figures with wide user bases. For example, Facebook or Netflix. Now, however, phishing often leverages social engineering.
- Many people willingly make large amounts of information about themselves public, including where they live and work, their hobbies, and their brand loyalties. Attackers can use this information to send targeted messages, increasing the likelihood that users will fall for their tricks.

# State-sponsored attacks

- As more of the world moves to the digital realm, the number of large-scale and state-sponsored attacks are increasing. Networks of hackers can now be leveraged and bought by opposing nation,states and interest groups to cripple governmental and organizational systems.
- For some of these attacks, the results are readily apparent. For example, numerous attacks have been identified that involved tampering with elections. Others, however, may go unnoticed, silently gathering sensitive information, such as military strategies or business intelligence. In either case, the resources funding these attacks enables criminals to use advanced and distributed strategies that are difficult to detect and prevent