# Introduction to Cyber Law

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.

Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data Protection and Privacy

**Need for Cyber Law:**

**TACKLING CYBER CRIMES**

**INTELLECTUAL PROPERTY RIGHTS AND COPYRIGHTS PROTECTION ACT**

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 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

**Hacking:**

- role of an ethical hacker
- legally as an ethical hacker

Ethical hackers

- Employed by companies to perform penetration tests

Penetration test

- Legal attempt to break into a company's network to find its weakest link
- Tester only reports findings, does not solve problems

Security test

- More than an attempt to break in; also includes analyzing company's security policy and procedures
- Tester offers solutions to secure or protect the network

**Role of Security & Penetration Testers:**

- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission

Tiger box

Collection of OSs and hacking tools

Usually on a laptop

Helps penetration testers and security testers conduct vulnerabilities assessments and attacks

**Penetration Testing Methodologies:**

White box model

Tester is told everything about the network topology and technology

- Network diagram

Tester is authorized to interview IT personnel and company employees

Makes tester's job a little easier

- Black box model
  - Company staff does not know about the test
  - Tester is not given details about the network
    - Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

Gray box model

Hybrid of the white and black box models

Company gives tester partial information

**Overview – Software Piracy**

- Software piracy is illegal copying of computer software, and it is a prevalent and serious problem or sale of saleable software without a license.
- Major software companies are losing 35-40% of their potential retail revenue to software pirates around the world

**The Concept of privacy**

- Unreasonable intrusion upon a person's seclusion
- Public disclosure of private facts
- Publicity that places a person in false light
- Appropriation of a person's name or likeness invoked

**Right to privacy in India**

- Article 21 of the Constitution of India-Right to life and personal liberty by necessary implication confers right to privacy –
- Kharak singh v State of U.P AIR 1963 SC 1295
- Gobind v State of M.P 1975 SCC 468
- PUCL v UOI (1997) 1 SCC 318
- R.Rajagopal v State of Tamil Nadu (1994)6 SC 632-autoshanker case
- Article 19-freedom of speech and expression
- Article 19(2) –Reasonable restrictions
- One of the restrictions/conditions is National Security

- Privacy vs national security balancing competing interests

**Threats to privacy**



- Hacking
- Cookies
- HTTP
- Information provided voluntarily
- Browsers
- E-mail
- Websites
- Spam
- Software's to check employee behavior
- Satellite vigilance

**Protecting privacy**

- Encryption
- Trust mark-webtrust, truste,etc
- Anonymity
- Cookie guards-cookie cop, siemen's webwasher, cookie crush,etc
- Privacy policy of website-p3p-platform for privacy preference
- Secure system for electronic money transfer- e.g SSL
- Need for legislation and enforcement
- Establish effective dispute resolution

What is a Mobile Device/Wireless?

- Mobile Device: a device that is easy to use, enables remote access to business networks and the internet, and enables quick transfer of data.
- Wireless Communication: the transfer of *information* over a distance without the us of electrical conductors or wires

Examples of Mobile Devices

- Laptops

- Cell Phones
- PDAs
- Flash Drives
- Bluetooth
- Mouse/Keyboard
- Mp3 Players

How does Wireless Work?

- Wireless networks use electromagnetic radiation as their means of transmitting data through space.
- An access point (AP) device is physically connected to the LAN (typically a router)
- The AP has an antenna and sends and receives data packets through space
- A wireless device then connects to the WLAN using its transmitter to connect to the AP, and then to the LAN.

What are the Advantages?

- Enhanced productivity
- Portability: Stay connected even away from home or office, resulting in a more flexible work life

**Risk: Physical theft/loss of device**

- Laptop theft accounted for 50% of reported security attacks.
  CSI, The 12th Annual Computer Crime and Security Survey, 2007
- Lost or stolen laptops and mobile devices are the most frequent cause of a data breach, accounting for 49% of data breaches in 2007.
  Ponemon Institute, U.S. Costs of a Data Breach, November 2007

**Mitigation**

- Cable Locks
- Never leave hardware unattended
- Make hardware as inconspicuous as possible
- Invest in tracking/recovery software
- Encryption
- Authentication

**Risk: Data loss/leakage**

- 7 out of 10 government mobile devices are unencrypted.

  Government Accountability Office (GAO), IT Security: Federal Agency efforts to encrypt sensitive information are under way, but work remains, June 2008
- The cost of recovering from a single data breach now averages $6.3M - that's up 31 percent since 2006 and nearly 90 percent since 2005.

  Ponemon Institute, U.S. Costs of a Data Breach, November 2007



**Wireless networks**

- Infrastructure Mode
- Ad-hoc mode

Specific Threats to Wireless Networks

- Unauthorized use of service
- Jamming
  - Constant Jamming
  - Deceptive Jamming

**Auditing Wireless Networks**

- Access control, transmission control, viruses, and monitoring access points are important risks to consider
- Firewall generally secures information but WLAN creates new challenges because it easier to access. Therefore, control is more important.
  - (Ex) If an employee were to bring in an unauthorized router in to work, unauthorized users could potentially access the network from outside the building
- Access Point (AP) – security of APs is crucial for wireless network auditing, consider unauthorized access, unauthorized APs, improperly configured APs, and Ad Hoc networks
- An Auditor might walk around the building looking for markings left on the ground by hackers indicating a spot in range of a wireless network
- Wireless auditor – an automated system that detects anomalies

**Tools and Methods used in Cybercrime**

Various types of Cybercrime attack modes are

1) Hacking

2) Denial Of Service Attack

3) Software Piracy

4) Phishing

5) Spoofing.

Some important tool use for preventing cyber-attack is

1)Kali Linux

2) Ophcrack

3) EnCase

4) SafeBack

5) Data Dumber

**Purpose of Proxy Server**

- Improve Performance
- Filter Requests
- Keep system behind the curtain
- Used as IP address multiplexer
- Its Cache memory can serve all users
- The attacker first connects to a proxy server – establishes connection with the target through existing connection with the proxy.

**An Anonymizer**

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.

It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.

It accesses the Internet on the user's behalf protecting personal information by hiding the client computer's identifying information.

**Phishing and Identify theft:**

Stealing personal and financial data with virus infected system as a method of online ID theft

Phishing works with planning, setup, attack and collection of information recorded from the online communication.

# UNIT II

## Cybercrime – An Introduction

Computer Crime, E-Crime, Hi-Tech Crime or Electronic Crime is where a computer is the target of a crime or is the means adopted to commit a crime.

Most of these crimes are not new. Criminals simply devise different ways to undertake standard criminal activities such as fraud, theft, blackmail, forgery, and embezzlement using the new medium, often involving the Internet

**Computer vulnerability**

- Computers store huge amounts of data in small spaces
- Ease of access
- Complexity of technology
- Human error
- One of the key elements that keeps most members of any society honest is fear of being caught — the deterrence factor. Cyberspace changes two of those rules. First, it offers the criminal an opportunity of attacking his victims from the remoteness of a different continent and secondly, the results of the crime are not immediately apparent.
- Need new laws and upgraded technology to combat cyber crimes

**Types of Cyber crimes**

- Credit card frauds
- Cyber pornography
- Sale of illegal articles-narcotics, weapons, wildlife
- Online gambling
- Intellectual Property crimes- software piracy, copyright infringement, trademarks violations, theft of computer source code
- Email spoofing
- Forgery
- Defamation
- Cyber stalking (section 509 IPC)
- Phishing

- Cyber terrorism

## TYPES OF CYBER CRIMES

**E-Mail bombing:** Email bombing refers to sending a large number of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

**Data diddling:** This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

**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 bank's servers, that deducts a small amount from the account of every customer

**Denial of Service:** This involves flooding computer resources with more requests than it can handle. This causes the resources to crash thereby denying authorized users the service offered by the resources.

### Cyber Crime Data in Regional Context

Carding:

Carding is a serious threat to India, as it does not require a high degree of sophistication and is considered particularly pernicious by international financial institutions and e-commerce providers.

Bots:

Bots, compromised servers that may be launching cyber-attacks or sending Spam, were detected in the India IP space, including servers with the domain name.

Phishing:

ISPs were able to point to a few examples of phishing capture sites being located on their servers, one targeting eBay (a frequent attack point for phishers).

### Constitutional & Human Rights issues in Cyberspace

The right includes freedom to receive and impart information and ideas and to hold opinions without any state interference. It also includes the right to express oneself in any medium including exchanging ideas and thoughts through Internet platforms or social networks.

### Issues in Cyberspace

Cyberspace has been faced many security challenges like identity tracing, identity theft, cyberspace terrorism and cyberspace warfare. In this paper, we focus on analysis these security challenges, and give some possible solutions offered by law and technology.

**Right to use Cyberspace**

Accordingly, the Internet has become a major vehicle for the exercise of the right to freedom of expression and information. The International Covenant on Civil and Political Rights (ICCPR)3 states (in article 19(2))

**Freedom of expression in Cyberspace**

Freedom of speech and expression is broadly understood as the notion that every person has the natural right to freely express themselves through any media and frontier without outside interference, such as censorship, and without fear of reprisal, such as threats and persecutions.

**Freedom Of Speech in Cyberspace**

Freedom of speech is one of the human rights inherit by human in the world as stated in Article 19 of the UDHR (Universal Declaration of Human Rights), the article states that everyone has the right to freedom of opinion and speech, including the right to hold opinions without interference and to seek, receive and convey information and ideas through any media regardless of boundaries (region).

The freedom of speech rights in regard of speaking and giving opinion which associated with IT is often leads to victim suspected of breaking these limits. Actually, the freedom of speech rights itself is regulated in the article 28 of the 1945

**Right to access in Cyberspace – an Internet**

Right to internet under **Article 21**

The court took the view that the right to be able to access the internet has been read into the fundamental right to life and liberty, as well as privacy under Article 21. The court added that it constitutes an essential part of the infrastructure of freedom of speech and expression.

Internet plays a significant role with the escalation of technology, so a primitive question arises that:

Whether or not Internet access should be considered a civil right?

In 2016, the UNHRC General Assembly expressed an important human right to Internet access.

The Internet is the undiscovered ocean of information, and the biggest supplier in the world.

Technology is, in his opinion, an enabling agent of rights and not a privilege of its own. India has legislation which deals with cyberspace crimes.

**Right to privacy**

What is privacy?

Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.

Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps to establish boundaries to limit with the access for information sharing and communication.

Privacy is an essential way to protect against society with arbitrary and unjustified usage of power. Privacy International envisions, protects the right to access the information. Individual can participate in the modern development of technologies with ability to freely enjoy the rights. Privacy is a qualifies, fundamental human right with articulated management instruments.

**Right to data protection**

Personal data is any information related to privacy, professional or public. In the recent environment, vast amount of personal data are shared and transferred around the globe instantaneously. Data protection refers to the practices, safeguards and binding rules with protection of personal information.

**Data Protection Laws:**

- Laws need to be updated to address today's reality

- Corporate co- and self-regulation is not working to protect the data

**Cybercrime and Legal frameworks**

Cybercrime is defined as a crime in which a computer can commit with hacking, phishing and spamming as a tool to work as offense. Cybercriminals use computer technology to access personal information, business trade for exploitative purposes. Criminals can perform illegal activities referred as hackers.

Cybercrime include online bank information theft, identity theft, unauthorized computer access.

**Types of Cybercrime**

- DDoS Attacks
- Botnets
- Identity Theft
- Cyberstalking
- Social Engineering
- PUPs
- Phishing
- Prohibited/Illegal Content

Cybercrimes against Individuals, Institution and State

- Individual
- Property
- Government

Individual: This type of Cybercrime can be in the form of Cyberstalking, distributing pornography, trafficking and "grooming".

Institutions: It includes, financial institutions, banks with highly affected event of cyber-attacks such as data breaches. The institutions have to pay fines and penalties for losing personal identifiable information.

**Hacking**

It can be worked out with identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Hacking causes computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data.

**Digital Forgery**

Forgery has been defined as the crime of falsely altering document with intension to mislead others. It includes the production of counterfeited items. Digital Forgery involve electronic forgery and identity theft. The majority of digital forgery occurs because of digitally altering pictures. Digital techniques are notoriously more precise than conventional retouching because any area of the photo can be changed pixel by pixel. The three types of image forgery include image retouching, splicing forgery and copy-move image forgery.

**Cyberstalking**

- Cyberstalking is a new concept with agreed-upon definition such as
- Stalking is done with the assistance of technology
- It is done to make a person feel afraid, threatened or worried about their safety
- It invades a person's privacy
- The stalker monitors the victim's behaviour, threatens them with unwanted access.

**Cyber pornography**

It is defined as the act of using cyberspace to create, display, distribute, import or publish pornography. The traditional pornographic content has been largely replaced by online/digital pornographic content.

**Cyber Defamation**

The term defamation is used to define the injury caused by the reputation of a person. The intention of the person causes defamatory statement which lowers the reputation of the person against whom the statement has been made in the eyes of general public. Defamation is the application to Cyber defamation which involves defamation of a person through a new and a virtual medium. Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.

Medium by which offense of cyber defamation can be caused:

- World Wide Web
- Discussion groups
- Intranets
- Mailing lists and bulletin boards
- E-mail