UNIT-I
SYLLABUS

UNIT 1: CYBERCRIME

Cybercrime and information security, Cybercriminals, Classifications of cybercrimes, Need for Cyberlaws in Indian context, Legal perspectives of cybercrime, Indian perspective of cybercrimes, Cybercrime and the Indian ITA 2000, Positive aspects and weak areas of ITA 2000, Amendments made in Indian ITA 2000 for admissibility of e-records, Amendments to the Indian IT Act, Global perspective on cybercrimes, Intellectual property in cyberspace, Ethical dimension of cybercrimes.

Introduction to cybercrime:

- First recorded cybercrime place in year 1820.
- Indian corporate and government websites attacked or defaced more than 780 times between February 2000 and December 2002.
- Third December 2009,286 Indian websites rare hacked in 5 months between January and June 2009.
- Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge underlines this.
- Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.
- Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.
- Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.
- Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy.
- In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.
- At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.
- At the regional and international level, this entails cooperation and coordination with relevant partners.

- The formulation and implementation of a national framework and strategy for cyber security thus requires a comprehensive approach.
- Cyber security strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime.
- The development and support of cyber security strategies are a vital element in the fight against cybercrime.
- The legal, technical and institutional challenges posed by the issue of cyber security are global and far- reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation.
- In this regard, the World Summit on the Information Society (WSIS) recognized the real and significant risks posed by inadequate cyber security and the proliferation of cybercrime describing the multi stakeholder implementation process according to eleven action lines and allocating responsibilities for facilitating implementation of the different action lines.
- At WSIS, world leaders and governments designated ITU to facilitate the implementation of WSIS Action Line C5, dedicated to building confidence and security in the use of ICTs.
- In this regard, the ITU Secretary-General launched the Global Cyber security Agenda (GCA) on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions.
- The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cyber security and to enhance confidence and security in the information society.
- It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Within ITU, the GCA complements existing ITU work programmes by facilitating the implementation of the three ITU Sectors' cyber security activities, within a framework of international cooperation.
- The Global Cyber security Agenda has seven main strategic goals, built on five work areas:
  1) Legal measures
  2) Technical and procedural measures
  3) Organizational structures
  4) Capacity building
  5) International cooperation.
- The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

- Among the GCA work areas, “Legal measures” focuses on how to address the legislative challenges posed by criminal activities committed over ICT networks in an internationally compatible manner.
- “Technical and procedural measures” focuses on key measures to promote adoption of enhanced approaches to improve security and risk management in cyberspace, including accreditation schemes, protocols and standards.
- “Organizational structures” focuses on the prevention, detection, response to and crisis management of cyber attacks, including the protection of critical information infrastructure systems.
- “Capacity building” focuses on elaborating strategies for capacity-building mechanisms to raise awareness, transfer know-how and boost cyber security on the national policy agenda.
- Finally, “International cooperation” focuses on international cooperation, dialogue and coordination in dealing with cyber threats.
- The development of adequate legislation and within this approach the development of a cybercrime- related legal framework is an essential part of a cyber security strategy.
- This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.
- The fact that provisions exist in the criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the Internet as well.
- Therefore, a thorough analysis of current national laws is vital to identify any possible gaps.
- Apart from substantive criminal law provisions, the law-enforcement agencies need the necessary tools and instruments to investigate cybercrime.
- Such investigations themselves present a number of challenges.60 Perpetrators can act from nearly any location

Cybercrime definition:

- A crime conducted to which a computer was directly and significantly instrumented
- Cybercrime is any illegal behaviour directed by needs of electronics operations that targets security of computer system and the data processed by them.
- A crime commit using a computer and the internet to send a person (identity theft-particular person theft) or send contra band or stalk victims or distracts operations with programs.

Cyber security:

- There are 2 types of attack are prevalent
    1. Techno-crime
    2. Techno- vandalism

1. **Techno-crime:**

- In the techno crime consists of data theft, data delete, copy, preventions, corrupt, deface or damage

2. **Techno-vandalism:**

- These acts of brainless defacement.
- These acts of brainless defacement of website and are others activities such as copying files and publishing their contents.
- Publically are mutually in nature.

Who are Cybercrimes?

- Cybercrime involves such activities as credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer systems; ignoring copyright. Software licensing and trade mark protecting; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts
- Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one major challenge underlines this.
- Cyber security plays an important role in the ongoing development of information technology, as well as Internet services.
- Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being.
- Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy.
- Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy.
- In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.
- At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of

3 types

Type1: Cyber criminals- Hungry for recognition

- Hobby hackers
- It professionals
- Politically motivated hackers
- Terrorist or organization

Type2:

- Not interested in recognition
- Psychological perverts
- Financially motivated hackers

State- sponsored

Type3:

- The insiders(employee)
- Disgruntled or former employees seeking revenge
- Competing companies using employees to gain economic advantage through data and or theft.
- Thus, the typical "motives" behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mind set and desire to sell network security services

Classification of cybercrimes:

- Crime is defines as " an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the offender liable to punishment by the law"
- Cybercrimes are classified as follows:

1. **Cybercrime against individuals:**
    - Electronic mail- spoofing and another frauds
    - Phishing, Spear Phishing and its various others form such as Vishing and Smishing
    - Computer-related fraud is one of the most popular crimes on the Internet, as it enables the offender to use automation and software tools to mask criminals' identities.
    - Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit.
    - With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes.504 One example of such a scam is the Nigeria Advanced Fee Fraud.
    - Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.
    - The main distinction between computer- related and traditional fraud is the target of the fraud.
    - If offenders try to influence a person, the offence is generally recognized as fraud.
    - Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences.
    - The most common fraud offences include online auction fraud and advanced fee fraud.
2. **Email spoofing:**
    - Hacking the mail.

- A spoofed email is one that appears to originate from one source but actually has been sent from another source
- Comparing different regional approaches (such as the CoE Convention on Cybercrime , the EU Framework Decision on Attacks against Information Systems, the Draft African Union Convention on Cyber Security and HIPSS, HIPCAR and ICB4PAC) to addressing concrete offences (e.g. illegal access) shows a large degree of consistency in the prescribed approach and methodology.
- All follow international best practices and it was therefore possible to use the model law developed by Caribbean experts as basis for the development of the HIPSSA and ICB4PAC model framework.
- In advance fee fraud, offenders send out e-mails asking for recipients' help in transferring large amounts of money to third parties and promise them a percentage, if they agree to process the transfer using their personal accounts.
- The offenders then ask them to transfer a small amount to validate their bank account data (based on a similar perception as lotteries – respondents may be willing to incur a small but certain loss, in exchange for a large but unlikely gain) or just send bank account data directly.
- Once they transfer the money, they will never hear from the offenders again. If they send their bank account information, offenders may use this information for fraudulent activities. Evidence suggests that thousands of targets reply to e-mails.
- Current researches show that, despite various information campaigns and initiatives, advance fee frauds are still growing – in terms of both the number of victims and total losses.

3. Spamming:

- Junk files anonomous
- People who create electronic spam are called spammers.
- Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately
- Although the most widely recognized from of spam is email spam, the team 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, video sharing sites.
- Spamming is difficult to control because it has economic viability- advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings.
- Spammers are numerous; the volume of unsolicited mail has become very high because the barrier to entry is low

- The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, who are forced to add extra capacity to cope with the deluge
- Spamming is widely detested, and has been the subject of legislation in many jurisdictions- for example , the CAN-SPAM Act of 2003
- Another definition of spamming is in the context of "search engine spamming". In this context, spamming is alteration or creation of a document with the intent to device an electronic catalog or a filling systems.
- Those who continually attempt to subvert or spam the search engines may be permanently excluded from the search index.
- Therefore, the following web publishing techniques should be avoided:
  1. Repeating key words
  2. Use of keywords that do not relate to the content on the site
  3. Use of fast meta refresh
  4. Redirection
  5. IP Cloaking
  6. Use of colored text on the same colour background
  7. Tiny text usage
  8. Duplication of pages with different URL's
  9. Hidden links
  10. Use of different pages that bridge to the same URL

4. Cyber defacement:

- Fake news(rumours),rollel type of activity
- Cyber defamation happens when the above takes place in an electronic form.
- Cyber defacement occurs when defamation takes place with the help of computers and/or the internet, for example someone publishes defamatory matter about someone on a website or sends an email containing defamatory information to all friends of that person.
  1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives
  2. It many amount to defamation to make an imputation concerning a company or an association or collection of persons such as
  3. An imputation in the form of an alternative or expressed ironically, may amount to defamation
  4. No imputation is said to harm a person's reputation unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character person, or lowers the character of that person in respect, or lower the credit of that person, or causes it to believed that the body of that person is in a loathsome state or in state generally considered as disgraceful

- Libel is written defamation and slander is oral defamation. When determining whether or not defamation has taken place, the only issue to consider is whether a person of ordinary intelligence in society would believe that the words would indeed injure the person's reputation
- Even if there is no damage to a person's reputation, the person who made the allegations may still be held responsible for defamation

5. **Internet time theft:**
    - Banner's
    - Such a theft occurs when an unauthorized person uses the internet hours paid for by another person
    - Basically, internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and passwords, either by hacking or by hacking or by gaining access to it by illegal means, uses it to access the internet without the other person's knowledge
    - However, one can identity time theft if the internet time has to be recharged often, even when one's own use of the internet is not frequent
    - The issue of internet time theft is related to the crimes conducted through "identity theft"
6. **Salami attack:**
    - Fully related to financial transaction.
    - Small changes to financial transaction do some problems may be occurred.
    - The attacks are used for committing financial crime. The idea here is to make alteration so insignificant that in a single case it would go completely unnoticed
    - For example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money from the account of every customer
    - No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month
7. **Data diddling:**
    - Small changes.
    - A data diddling 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 computerize their systems
8. **Forgery:**
    - To theft the data.
    - Counterfeit currency notes, postage and revenue stamps, mark sheets, 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 certificates

9. Web jacking:

- To control other parties.
- Web jacking occurs when someone forcefully takes control of a website
- 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

10. News group spam:

- Fake news to spread other resources
- The word "spam" was usually taken to mean excessive multiple posting
- The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever
- Spamming of Usenet newsgroups actually predates email spam
- The newsgroups posting Bot Serdar Argic also appeared in early 1994, posting tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide

11. Industrial Spying/ Industrial Espionage:

- Spying is not limited governments. Corporations, like governments, often spy on the enemy
- The internet and privately networked systems provide new and better opportunities for espionage
- Industrial spying is not new; in fact it is as old as industries themselves
- The use of the internet to achieve this is probably as old as the internet itself. Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of escrow organizations
- With the growing public availability of Trojans and spyware material , even low-skilled individuals are now inclined to generate high volume profit out of industrial spying
- This is referred to as "targeted attacks". This aspects of industrial spying is the one to be addressed in the fight against cybercrime
- Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them
- There are also the email worms automating similar "data exfiltration features". Such files are uploaded on an FTP server owned by the cyber crooks, with the aim of stealing as much IP as possible wherever it can be and then selling it to people who are ready to pay it.

- There are two distinct business models for cybercrime applied to industrial spying: Selling Trojan-ware and Selling Stolen Intellectual Property

12. Hacking:

- Hack the user's details
- Although the purpose of hacking are many, the main ones are as follows:
  1. Greed
  2. Power
  3. Publicity
  4. Revenge
  5. Adventure
  6. Desire to access forbidden information
  7. Destructive mind set
     - Every act committed toward breaking into a computer and/or network is hacking and it is an offences.
     - Hackers, write or use ready-made computer programs to attack the target computer
     - They possess the desire to destruct and they get enjoyment out of such destruction
     - Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money
     - They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature
     - Hackers, crackers and phrackers are some of the oft-heard teams. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT

13. Online frauds:

- Online theft.
- Spoofing websites and emails security alerts, hoax mails about virus threats lottery frauds and spoofing
- In spoofing websites and email security threats, fraudsters create authentic looking websites that are actually nothing but a spoof
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank account
- Fraudsters are increasingly turning to email to generate traffic to these websites. This king of online fraud is common in banking and financial sector
- It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate

- Online auctions are now one of the most popular e-commerce services. Already back in 2006, goods worth more than USD 20 billion were sold on eBay, the world's largest online auction marketplace.
- Buyers can access varied or specialist niche goods from around the world. Sellers enjoy a worldwide audience, stimulating demand and boosting prices.
- Offenders committing crimes over auction platforms can exploit the absence of face-to-face contact between sellers and buyers.
- The difficulty of distinguishing between genuine users and offenders has resulted in auction fraud being among the most popular of cybercrimes.
- The two most common methods include offering non-existent goods for sale and requesting buyers to pay prior to delivery and buying goods and asking for delivery, with no intention of paying.
- In response, auction providers have developed protection systems such as the feedback/comments system.
- After each transaction, buyer and sellers leave feedback for use by other users513 as neutral information about the reliability of sellers/buyers. In this case, "reputation is everything" and without an adequate number of positive comments, it is harder for offenders to persuade targets to either pay for non-existent goods or, conversely, to send out goods without receiving payment first.
- However, criminals have responded and circumvented this protection through using accounts from third parties.
- In this scam called "account takeover",offenders try to get hold of user names and passwords of legitimate users to buy or sell goods fraudulently, making identification of offenders more difficult.

14. Use net groups:

- Sharing of particular message.
- Usenet is a popular means of sharing and distributing information on the web with respect to specific topic or subjects
- It is feasible to block specific news-groups, however, this cannot be considered as a definitive solution to illegal or harmful content.
- It is possible to put Usenet to following criminals use:
  1. distribution
  2. distribution/ sale of pirated software package
  3. distribution of hacking software
  4. sale of stolen credit card numbers
  5. sale of stolen data/ stolen property

15. Password sniffing:

- To product our password
- Password sniffers are programs that monitor and record the name and password of network users as they login, jeopardizing security at a site

- Whoever installs the sniffer can then impersonate an authorized user and login to access restricted documents
- Laws are not yet setup adequately prosecute a person for impersonating another person online
- Laws designed to prevent unauthorized access to information may be effective in apprehending cracker using sniffer programs

15. Credit card frauds:

- Through fraud using credit card
- Information security requirements for anyone handling credit cards have been increased dramatically recently
- Millions of dollars may be lost annually by consumers who have credit card and calling cards numbers stolen from online database
- Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information
- Such attacks usually result in the implementation of stronger security systems

16. Identity theft:

- Information theft after that the hacker use the information in on use.
- The term identity theft – which is neither consistently defined nor consistently used – describes the criminal act of fraudulently obtaining and using another person's identity.
- These acts can be carried out without the help of technical means as well as online by using Internet technology.
- Wide media coverage, the results of various surveys analysing the extent of and loss caused by identity theft, as well as numerous legal and technical analyses published in recent years could easily lead to the conclusion, that identity-related offences are a 21st-century phenomenon.
- But this is not the case, as offences related to impersonation and the falsification and misuse of identity documents have existed for more than a century.
- Already back in the 1980s, the press intensively reported on the misuse of identity-related information.
- The emerging use of digital identities and information technology only changed the methods and targets of the offenders.
- Increasing use of digital information opened up new possibilities for offenders to gain access to identity-related information.
- Thus, the transformation process from industrialized nations to information societies has had a big influence on the development of identity-theft offences.
- Nonetheless, despite the large number of Internet-related identity-theft cases, digitization did not fundamentally change the offence itself, but merely created new targets and facilitated the development of new methods.

- The impact of the increasing use of Internet technology seems to be overestimated.
- Based on the results of a method analysis of identity-related offences, identity theft to a large degree remains an offline crime.
- In 2007, 20 per cent of the offences in the US542 were online scams and data breaches.
- Despite recent developments the offline identity theft remains highly relevant. The persisting importance of offline crimes is surprising, insofar as the digitization and moreover the globalization of network-based services has led to increasing use of digital identity- related information.
- Identity-related information is of growing importance, both in the economy and in social interaction. In the past, a "good name" and good personal relations dominated business as well as daily transactions.
- With the transfer to electronic commerce, face-to-face identification is hardly possible, and as a consequence identity-related information has become much more important for people participating in social and economic interaction.
- This process can be described as instrumentalization, whereby an identity is translated into quantifiable identity-related information.
- This process, along with the distinction between the more philosophical aspect of the term "identity" and the quantifiable identity-related information that enables the recognition of a person, is of great importance.
- The transformation process is not just relevant to Internet-related features of identity theft, as the impact of the development goes far beyond computer networks.
- Nowadays, the requirements of non-face-to-face transactions, such as trust and security, dominate the economy in general and not just e-commerce businesses.
- An example is the use of payment cards with a PIN (personal identification number) for purchasing goods in a supermarket.
- In general, the offence described as identity theft contains three different phases.
- In the first phase the offender obtains identity-related information. This part of the offence can for example be carried out by using malicious software or phishing attacks.
- The second phase is characterized by interaction with identity-related information prior to the use of the information within criminal offences.
- An example is the sale of identity-related information. Credit-card records are for example sold for up to USD
- The third phase is the use of the identity-related information in relation with a criminal offence. In most cases, the access to identity-related data enables the perpetrator to commit further crimes.
- The perpetrators are therefore not focusing on the set of data itself but the ability to use the data in criminal activities.

- Examples for such offence can be the falsification of identification documents or credit-card fraud.

Legal perspectives:

- First criminals justies resource manual 1978
- Computer related crimes any illegal for which knowledge of computer technology is essential for a successful proetution.
- International aspect for computer crime study in1983.
- Proper legislation is the foundation for the investigation and prosecution of cybercrime.
- However, law- makers must continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology.
- Historically, the introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced.
- One example is the development of computer networks in the 1970s – the first unauthorized access to computer networks occurred shortly afterwards.
- Similarly, the first software offences appeared soon after the introduction of personal computers in the 1980s, when these systems were used to copy software products.
- It takes time to update national criminal law to prosecute new forms of online cybercrime.
- Indeed, some countries have not yet finished with this adjustment process. Offences that have been criminalized under national criminal law need to be reviewed and updated.
- For example, digital information must have equivalent status as traditional signatures and printouts.
- Without the integration of cybercrime-related offences, violations cannot be prosecuted.
- The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law.
- This challenge remains as relevant and topical as ever as the speed of network innovation accelerates.
- Many countries are working hard to catch up with legislative adjustments. In general, the adjustment process has three steps: adjustment to national law, identification of gaps in the penal code, and drafting of new legislation.
- Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes.
- The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

- To ensure effective legislative foundations, it is necessary to compare the status of criminal legal provisions in the national law with requirements arising from the new kinds of criminal offences.
- In many cases, existing laws may be able to cover new varieties of existing crimes (e.g. laws addressing forgery may just as easily be applied to electronic documents).
- The need for legislative amendments is limited to those offences that are omitted or insufficiently covered by the national law.
- Based on experience, it may be difficult for national authorities to execute the drafting process for cybercrime without international cooperation, due to the rapid development of network technologies and their complex structures.
- Drafting cybercrime legislation separately may result in significant duplication and waste of resources, and it is also necessary to monitor the development of international standards and strategies.
- Without the international harmonization of national criminal legal provisions, the fight against transnational cybercrime will run into serious difficulties, due to inconsistent or incompatible national legislations.
- Consequently, international attempts to harmonize different national penal laws are increasingly important.
- National law can greatly benefit from the experience of other countries and international expert legal advice.
- he second situation in which law-enforcement agencies are allowed to access stored computer data outside their territory is when the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorization is heavily criticized.2508
- One main concern is the fact that the provision in its current wording probably contradicts fundamental principles of international law.
- Based on international law, investigators have to respect national sovereignty during an investigation.
- They are especially not allowed to carry out investigations in another state without the consent of the competent authorities in that state.
- The decision whether such permission should be granted is not in the hands of an individual, but of the state authorities, since interference with national sovereignty does not only affect the rights of the individual, but also state concerns.
- By ratifying the Convention on Cybercrime, countries partly dismiss the principle and allow other countries to carry out investigations affecting their territory.
- Another concern is the fact that does not define procedures for the investigation.
- Based on the text of the provision, it is not necessary for the same limitations to be applied that exist in domestic law with regard to comparable domestic investigations. Interestingly enough, such a restriction was included in the draft text of the Convention on Cybercrime presented in the beginning of 2000

Globalization:

- Globalized information is done an interesting number of Transe national offences

Cybercrime Indian perspectives:

- Fourth highest number of internet users in the world.
- There are 45 billion internet resources in India.
- 37% cyber café-browsing center-remaining 1990's internet not is usually. 57%(18 to 35 years old)
- Mobile internet used only
- Information technology act recorded the cybercrime 50% in the year 2007 recorded.
- Related in 46% to cyber pornography followed by hacking.
- In over 60% of the layers affentere between 18 to 30 of the years according to the crime in 2007 report of the national crime record.

Cybercrime and Indian ITA 2000:

- ITA 2000 in acted after the united nation journal assembly resolution in January 30,1997 by adopting the model law electronic commerce adopted by united nations commission on international trade law.
- It was enacted into consideration UNICITRAL modes of law on electronic commerce in year 1996.

Hacking and Indian law:

- Cybercrime are punishable under the 2 categories
- ITA 2000 and the IPC
- A total of 207 the cases of cybercrimes were registered under the ITA 2007 compared to cases registered in 2006 under the IPC to 339 where recorded in 2007 compare with 3x11 cases in 2006.
- The identification of illegal content is a challenge for the hosting provider. Especially for popular providers with many websites, manual searches for illegal content on such a great number of websites would be impossible. As a result, the drafters of the Directive decided to limit the liability of hosting providers.
- However, unlike in the case of the access provider, the liability of the host provider is not excluded.
- As long as the host provider has no actual knowledge of illegal activities or illegal content stored on its servers, it is not liable.
- Here, an assumption that illegal content could be stored on the servers is not considered equivalent to actually having knowledge of the matter.
- If the provider obtains concrete knowledge about illegal activities or illegal content, it can only avoid liability if it immediately removes the illegal information. Failure to react immediately will lead to liability of the hosting provider.

- Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews.
- Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.
- Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues
- Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.
- Examine national participation in international efforts to combat cybercrime, such as the round-the- clock Cybercrime Point of Contact Network.
- Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

1. Sec -43 (penalty for damage to computer system etc.)	Punishment fine Rs.1 core
2. Sec-66 (hacking with computer system)	fine 62 lakh imprisonment for 3 years
3. Sec-67(publishing of information which is electronic form)	fine 1 lakh imprisonment of 5 years and double conviction on second offences
4. Sec-68(power of controller to give directory)	Fine up to 20 lakh and imprisonment of 3 years.
5. Sec-70(product systems) attempting or security access to computer of another person without their knowledge.	Imprisonment of up to 10 years.

6. Sec-72(penalty reach of confidentiality and privacy attempting or securing access for computer for breaking confidentiality of the information of computer)	Five up to 1 lakh and imprisonment of up to 2 years.
7. Sec-73(penalty for publishing digital signature certificate false in certain particulars(publishing false digital signature false in certain particular))	Fine 1 lakh imprisonment of 2 years
8. Sec-74(publication for fraud purpose)	Imprisonment of term 2 years and fine 1 lakh.

The intensity of the protection of religions and their symbols differs between countries.

- A number of concerns are expressed with regard to criminalization. It is pointed out in the 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression that in "many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues"
- The 2008 Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should resist from the further adoption of statements supporting the idea of criminalizing defamation of religions.
- The question whether this requires criminalization of defamation is controversial.
- Concerns regarding the criminalization of defamation are especially related to potential conflict with the principle of "freedom of speech".
- Thus, a number of organizations have called for a replacement of criminal defamation laws.
- The UN Special Rapporteur on Freedom of Opinion and Expression and the OSCE Representative on Freedom of the Media have stated: "Criminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".
- Despite these concerns, some countries1826 have implemented criminal law provisions that criminalize libel, as well as the publication of false information.
- It is important to highlight that even in the countries that criminalize defamation the number of cases varies considerably.

While in the United Kingdom nobody in 2004 and just one suspect in 2005 was charged with libel, the German crime statistics record defamation offences for 2006.The Council of Europe Convention on Cybercrime, the Commonwealth Model Law and the Stanford Draft do not contain any provisions directly addressing these acts.

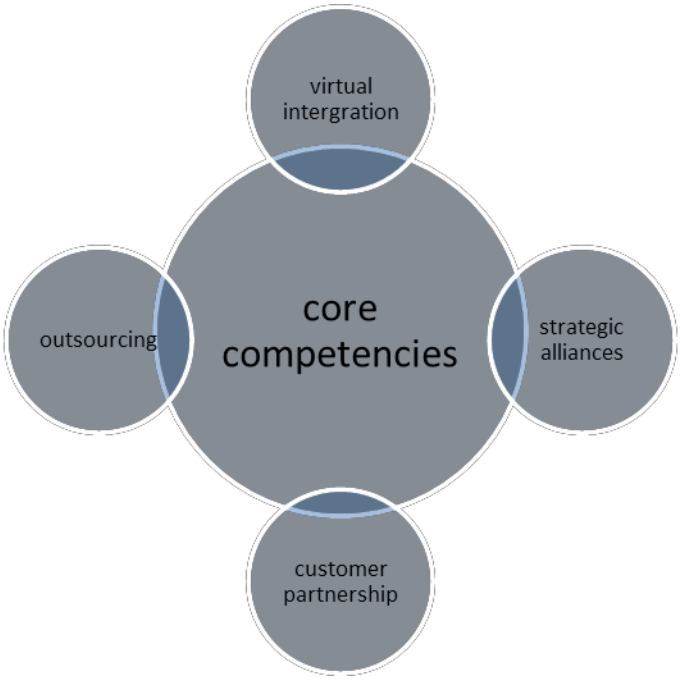
A global perspective of cybercrimes:

- In Australia cybercrime as narrow statutory meaning as used in the cybercrime ad 2001 which detail against computer data and system.
- COE's (council of eruopes)cybercrime treaty is used as a umbrella term to refer to a array of criminal activity including data and system related content and copyright offences
- Countries taking actions against spam although this status is form the ITU (International Telecommunication version) conducted in 2005.
- After intensive discussions1098 about topics and methodology of a comprehensive UNODC study related to cybercrime, the UN Member States received a questionnaire in early 2012.
- At the same time an online portal was developed. The complex questionnaire contains various questions related to different fields of cybercrime legislation such as definitions, criminalization and procedural instruments.
- Member states were requested to provide information about the status of their legislation as well as the implementation of different regional standards (such as the Convention on Cybercrime).
- In 2013 these results were submitted to the Commission on Crime Prevention and Criminal Justice
- In 2013 UNODC published the first results of the study.
- The study is the most complex so far and contains results from 69 Member States that responded.
- In addition to responses from the member states the study includes the results of the review of 500 publicly available documents and information submitted by more than 40 companies and 16 academic institutions.
- The study highlights that the reach of regional harmonization instruments – such as the Council of Europe Convention on Cybercrime – is limited. In addition the study shows that other regional instruments are equally important.
- The expert working group met in February 2013 and submitted the matter to the Commission on Crime Prevention and Criminal Justice.
- In April 2013 the Commission on Crime Prevention and Criminal Justice for the first time discussed the results of the study.
- Resolution 22/7 discusses the work done without going into detail.
- Instead the Commission calls upon the member states to review the results, asks the expert group to continue the work and requests the secretariat to translate the study into all UN languages.
- During the 23rd meeting the topic Cybercrime was addressed by various speakers.

- Despite various calls for a global harmonization the Commission did not take a decision in this regard. Instead it focusses more on capacity building by underlining the global Capacity Building Program run by UNODC

Cybercrime the extended enterprise:

- It is a continuing of that the airline user is not adquiatly educated to understanding thread and how to product one self.
- It is the responsibility of each user to become of the thread as well as the operations that connectivity and presents with the concept of extended enterprise.
- The extended enterprise can only successful if all of the component and individual have the information they need in order to business effectively and extended enterprise is a loosely coupled self organization network that combine a economic output to provide and service to the market.
- The interconnected feature of information and communication technologies security overall can only way fully promoted when the users can fully awareness of the existing thread and dangerous.
- Government and business and the international community must therefore proactively help users access information on how to product themselves.
- International co operations of the levels of government industry and consumers, business and technical throws to allow a global and co-ordinate approach to archiving global cyber security is the key.



Survival mantra for the Netizens:

- Netizens are the internet users netizes is some one whose spends considerable time online and also has a considerable presents online.
- The term "netizen" was coined by Michael Hauben. Quite simply, "Netizens" are the internet users
- Therefore, by corollary, "Netizen" is someone who spends considerable time online and also has a considerable presence online
- The 5P Netizen matra for online security is:
  1. Precaution
  2. Prevention
  3. Protection
  4. Preservation
  5. Perseverance
- Some agencies have been advocating for the need to address protection of the Rights of Netizens.
- There are agencies that are trying to provide guidance to innocent victims of cyber crimes
- There are also a few incidents where police have pursued false cases on innocent IT professionals
- More importantly, users must try and save any electronic information trail on their computers
  1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.
  2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime.
  3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.

     1. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries.

     2. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

     7 Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

     - Cybercrime can be committed using only fairly basic equipment.

- Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools.
- The tools needed to commit complex offences are widely available over the Internet often without charge. More sophisticated tools cost several thousand dollars.
- Using these software tools, offenders can attack other computer systems at the press of a button.
- Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks.
- High-profile attacks are often individually designed for specific targets.585 Software tools are available that enable the offender to carry out DoS attacks, design computer viruses, decrypt encrypted communication or illegally access computer systems.
- A second generation of software tools has now automated many cyber scams and enables offenders to carry out multiple attacks within a short time. Software tools also simplify attacks, allowing less
- In the early days of computer technology, the ability of law enforcement to carry out investigations involving digital data was limited by a lack of computer forensic equipment and expertise.
- The growing importance of digital evidence has spawned an increasing number of computer forensic laboratories.
- Yet, while the logistical aspects of the issue can be solved fairly easily, a number of challenges remain.
- The underlying reason for these challenges is the fact that, despite a number of similarities between digital evidence and other categories of evidence, there are major differences.
- Some of the general principles, such as the requirement that the evidence be authentic, complete, reliable and accurate and that the process of obtaining the evidence take place in line with the legal requirements, still hold good.
- Alongside the similarities, however, there are a number of aspects that make digital evidence unique and therefore require special attention when dealing with digital evidence in criminal investigations.
- Analysing and evaluating digital evidence requires special skills and technical understanding which is not necessarily covered in the education received by judges, prosecutors and lawyers.
- They therefore rely increasingly on the support of experts in the recovery of digital evidence.

Intellectual Property in Cyberspace

Introduction:

Intellectual Property (IP) refers to creations of the mind, such as inventions, literary and artistic works, symbols, names, images, and designs used in commerce. With the growth of the internet and digital technologies, the cyberspace has become a critical platform for creating, sharing, and distributing intellectual property. However, this rapid digital expansion has also raised challenges in protecting IP rights.

What is Intellectual Property (IP)?

IP includes:

- Copyright – Protects creative works (books, music, software, etc.)
- Patents – Protect inventions or new processes
- Trademarks – Protect brand names, logos, and slogans
- Trade Secrets – Protect confidential business information

Cyberspace and Its Role in IP

Cyberspace refers to the virtual environment of the internet where digital interactions occur. It enables: easy creation and sharing of content

- Instant global distribution
- Anonymity of users
- Difficulty in tracing sources of content

These characteristics make it both a boon for creators and a challenge for protecting IP.

Challenges of IP in Cyberspace

Digital Piracy:

- Unauthorized downloading or sharing of music, movies, software, eBooks, etc.
- Torrent sites and illegal streaming services contribute to this problem.
- Copyright Infringement:
- Content (text, images, and videos) is often copied and used without permission.
- Social media platforms, blogs, and websites are common places for misuse.

Trademark Misuse:

- Fake or counterfeit products sold online using popular brand names.
- Domain name squatting (registering domain names similar to famous trademarks to resell at a profit).

Software Piracy:

- Use of cracked software versions without licenses.
- A major concern for software companies and developers.
- Difficulty in Enforcement:
- Jurisdictional issues: IP laws differ from country to country.
- Difficulty in identifying offenders due to anonymity on the internet.
- Legal Frameworks and Protection Mechanisms

International Laws and Treaties:

- WIPO (World Intellectual Property Organization) – Promotes IP protection globally.
- TRIPS Agreement (by WTO) – Sets minimum standards for IP regulation.

- National Laws:
- Countries have specific IP laws (e.g., Copyright Act, Patent Act, Trademark Act).
- Cyber laws like IT Acts (in India, the IT Act 2000) address digital crimes and IP theft**.**

Technological Solutions:

- Digital Rights Management (DRM): Restricts unauthorized copying or distribution.
- Watermarking: Identifies content ownership.
- Encryption and secure coding practices.
- Organizations & Tools:
- CERT and Cybercrime Cells: Investigate cybercrimes including IP violations.
- Content ID systems (used by YouTube): Automatically detect copyright violations.
- Best Practices for IP Protection in Cyberspace
- Always register copyrights, patents, and trademarks.
- Use licensing and clear terms for digital distribution.
- Monitor online platforms regularly for infringement.
- Educate users and employees about IP laws and cyber ethics.
- Use legal notices and takedown procedures (e.g., DMCA notice in the U.S.)

Ethical Dimensions of Cybercrimes

Introduction

Cybercrime refers to illegal activities conducted through computers or the internet. These crimes include hacking, identity theft, cyberbullying, digital piracy, and financial fraud. While laws define cybercrimes legally, the ethical dimension explores the moral implications of such actions — what is right or wrong, fair or unjust — in the context of technology use.

Understanding the Ethical Dimension

- Ethics is the study of what is morally right and wrong. In cyberspace, users often face ethical dilemmas, especially where behavior may not be illegal but still morally questionable. The ethical dimension of cybercrime deals with:
- Responsibility for one's digital actions
- Respecting privacy and intellectual property
- Using technological power fairly and honestly

Key Ethical Issues in Cybercrime

1. Privacy Violation

Cybercrime Example: Unauthorized access to emails, surveillance, or data leaks.

Ethical Concern: It is ethically wrong to invade someone's personal space or misuse their private data without consent.

2**. Digital Piracy**

Cybercrime Example: Downloading software, music, or movies illegally.

Ethical Concern: Although widely practiced, piracy disrespects the creator's rights and discourages innovation and hard work.

3. Hacking and Unauthorized Access

Cybercrime Example: Bypassing security systems to access restricted systems or networks.

Ethical Concern: It breaches trust, causes harm, and disrupts systems that others rely on, even if not done for profit.

4. Cyberbullying and Harassment

Cybercrime Example: Threats, trolling, and spreading false information online.

Ethical Concern: Such acts damage mental health, violate human dignity, and reflect a lack of empathy.

5. Spreading Misinformation

Cybercrime Example: Deliberately sharing fake news, especially on social media.

Ethical Concern: It manipulates public opinion, causes panic, and undermines truth and trust in society.

6. Identity Theft

Cybercrime Example: Using someone's personal data to impersonate them or commit fraud.

Ethical Concern: It violates personal autonomy and may cause serious harm to victims' financial and personal lives.