RV College of Engineering®

Go, change the world

22EM1C07-Introduction to Cyber Security

UNIT- I

Chapter-2: Introduction to Cyber Crime

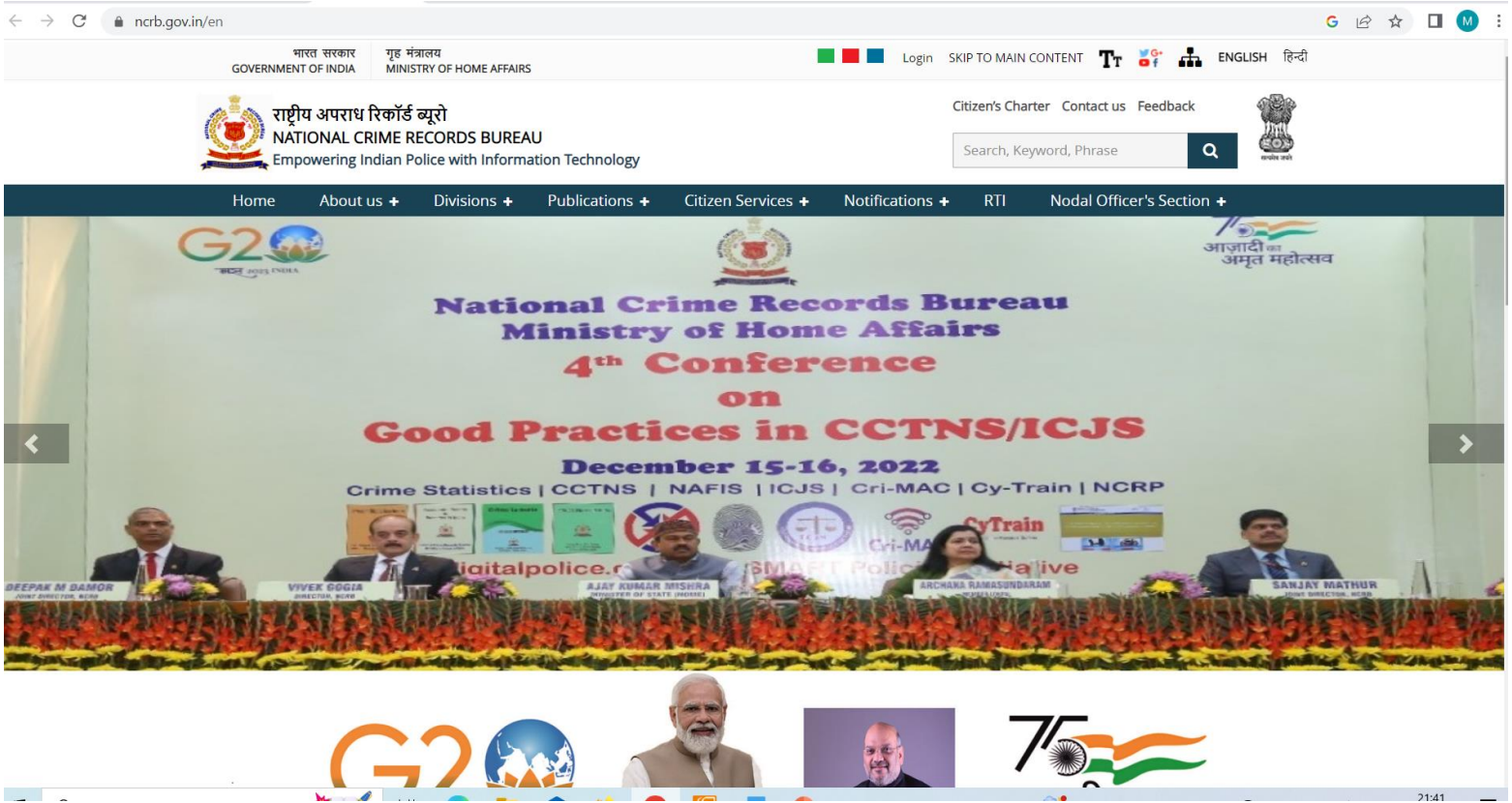
Text Book:

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011,Reprint 2022, ISBN:978-81-265-2179-1.

Course Incharge: Dr.Mohana
Department of Computer Science & Engineering (Cyber Security)
RV College of Engineering, Bangalore-560059

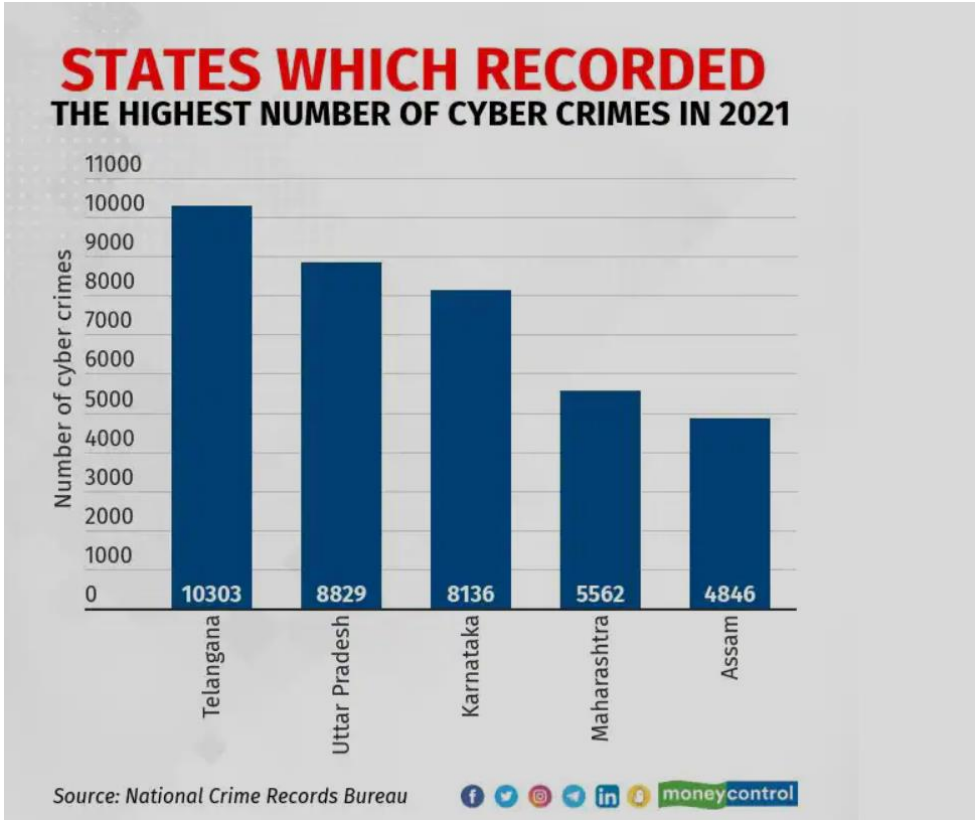
Unit - I Syllabus

Unit-I	8 Hrs
Introduction to Cyber Space History of Internet, History and evolution of Information Security and cyber-Security, introduction to cyber space and information security, computer ethics and security policies. **Introduction to Cybercrime** Definition and Origins of the Word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives. Different Types of Cyber Crimes, Scams and Frauds	



Source: https://ncrb.gov.in/en

Cyber Crimes in India



https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

Cyber attacks in India

medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/#:~:text=The%20Indian%20Computer%20Emergency%20Response,Parliament%20on%20December...

REPORTS DONATE CAREERS EVENTS CUSTOMER SUPPORT LOG IN

MEDIANAMA Latest Free Reads Focus Discover Subscribe

Discover more: Cyber Attack, MeitY, Parliament, Rajeev Chandrasekhar

12.67 Lakh Cyber Attacks Reported In India By November 2022: IT Ministry In Parliament

Rajeev Chandrasekhar gave the data for 2022 while responding to a questions in Parliament, and also said dealing with cyber attacks is for States

By Vallari Sanzgiri Published December 15, 2022

Search SEARCH

LATEST HEADLINES

US military devices with biometric data sold online at $68,

https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/#:~:text=The%20Indian%20Computer%20Emergency%20Response,Parliament%20on%20December%2014%2C%202022.

Cyber crime on the rise

- As per the cyber crime data maintained by the **National Crime Records Bureau (NCRB)** https://ncrb.gov.in/en
- According to NCRB, the police have recorded under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC).
- 58.6% of the offenders were in the age group 18–30 years, 31.7% of the offenders were in the age group 30-45 years and **remaining reported offenders whose age was below 18 years.**
- Awareness and education, labs, research centres

CYBER CRIMES / CYBER FRAUDS

- Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping.
- Fraud is the intentional deception of a person or group.
- Internet fraud includes any scheme using Web sites, chat rooms, and email to offer nonexistent goods and services to consumers or to communicate false information to consumers.
- Most scams are done by **e-mail**- critical information like usernames, passwords, credit card information, or other types of account information.

- hindering the economic and **social development of any nation**.
- Cyber fraud can also destroy our good and morally sound culture.

Definition of cyber crime

- Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

- Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

- Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data.

Types of cyber frauds

- A wide variety of scams operate in the online environment, ranging from fraudulent lottery schemes, travel and credit-related ploys, modem and web page hijacking, and identity theft (ID theft)
- Many online scams originate in spam messages.
- the "advance fee fraud" format of requiring up-front payment or investment on the promise of high returns thatare never forthcoming.
- Spam is a key tool for the spread of ID theft

- "look alike" websites where users are tricked into divulging personal information which can be used to access and illegally transfer money out of the victim's bank account(s)
- These attacks are continually becoming more sophisticated.
- Other variants of fraud rely on the use of identity stolen through technological methods.
- "**key stroke" loggers** and other programs to steal information stored on, entered into, or received by these devices.

Cyber frauds in India

According to the survey,

- 66% of Indian online adults have been a victim of cyber fraud in their lifetime. In the past 12 months, 56% of online adults in India have experienced cyber fraud.
- As per the report, at least 1,15,000 people fall prey to cyber fraud every day, while 80 per minute and more than one per second leading to a rise in the average direct financial cost per victim to around Rs10,500.
- The cybercriminals have now shifted their focus to the increasingly popular social platforms. One in three adults online Indians (32%) have been either social or mobile cybercrime victims.

- While most internet users delete suspicious emails and are careful with their personal details online.
- 25% don't use complex passwords or change their passwords frequently and 38% do not check for the padlock symbol in the browser before entering sensitive personal information.
- Online adults are also unaware of the evolution of most common forms of cybercrime. In fact, 68% of adults do not know that malware can operate in a discreet fashion, making it hard to know if a computer has been compromised

Preventive measures

- Setup an e-security program for your business.
- Ensure your security program facilitates confidentiality, integrity and availability.
- Identify the sources of threats to your data from both internal and external sources.
- must have provisions to maintenance and upgrades of your systems.
- Administrators have access to all files and data.
- Roles for security should be defined, documented, and implemented for both your company and external contractors.
- Establish a security awareness program for all users.
- **Maintain logs** of all possible activities that may occur on your system.
- User accounts should **not be shared.**

- Employee user accounts **must be disabled or removed** when no longer needed.
- Ensure network security from external sources by installing **firewalls and intrusion detection** systems.
- Allow remote access to employees only through **secure communication channels like SSL or VPN.**
- Install **antivirus software** on all desktops and servers.
- Create a **data backup and disaster recovery plan** in case of unforeseen natural calamities.
- Ensure back-up procedures are in place and tested.
- Ensure back-up procedures include all the critical as well as back office data such as finance, payroll etc.
- **Incident response** is the ability to identify, evaluate, raise and address negative computer related security events.
- In case of an incident, do not panic, and continue to save logs.
- **Incident response -** Take a backup of the affected system and notify theauthorities.

Cyber crimes

1. Cyber pornography
2. Sale of illegal articles
3. Online gambling
4. Intellectual Property crimes
5. Email spoofing
6. Forgery
7. Cyber Defamation:
8. Cyber stalking
9. Unauthorized access to computer systems or networks
10. Theft of information contained in electronic form
11. Email bombing

12. Data diddling
13. Salami attacks
14. Denial of Service attack
15. Virus / worm attacks
16. Logic bombs
17. Trojan attacks
18. Internet time theft
19. Web jacking
20. Theft of computer system
21. Physically damaging a computer system

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

Ex. (Delhi Public School case)

https://timesofindia.indiatimes.com/home/sunday-times/what-the-dps-mms-tells-us-about-consent-in-the-digital-age/articleshow/64238647.cms

2. Sale of illegal articles

- sale of narcotics, weapons and wildlife etc.,
- by posting information on websites, auction websites, and bulletin boards or simply by using email communication.
- E.g. many of the auction sites even in India are believed to be selling cocaine in the name of ‘honey’.

3. Online gambling

- There are millions of websites; all hosted on servers abroad, that offer online gambling.
- money laundering.

Ex. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound.

After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

4. Intellectual Property crimes

- These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.
- In other words this is also referred to as cyber squatting.
- Ex. Satyam Vs. Siffy is the most widely known case.

5. Email spoofing

- A spoofed email is one that appears to originate from one source but actually has been sent from another source.

E.g. Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances.

Email spoofing can also cause monetary damage.

Ex. Recently, a branch of the **Global Trust Bank** experienced a run on the bank.

Numerous customers decided to withdraw all their money and close their accounts.

6. Forgery

- Counterfeit currency notes, postage and revenue stamps, mark sheetsetc can be forged using sophisticated computers, printers and scanners.
- These are made using computers, and high quality scanners and printers.
- In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

7. Cyber Defamation

- This occurs when defamation takes place with the help of computers and / or the Internet.

E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

8. Cyber stalking

- The Oxford dictionary defines stalking as “pursuing stealthily”.
- Cyber stalking involves following a person’s movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

9. Unauthorized access to computer systems or networks

- This activity is commonly referred to as hacking.
- “unauthorized access” interchangeably with the term “hacking”.

10. Theft of information contained in electronic form

- This includes information stored in computer hard disks, removable storage media etc.

11. Email bombing

- Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
- sending e-mailstill their servers crashed.

12. Data diddling

- This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
- Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

13. Salami attacks

- These attacks are used for the commission of financial crimes.
- The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.
- E.g. a **bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5a month)** from the account of every customer.
- sizeable amount of money being transferred into his account every Saturday.

14. Denial of Service attack

- This involves flooding a computer resource with more requests than it can handle.
- This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.
- sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash.
- Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

15. Virus / worm attacks

- Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on anetwork.
- They usually affect the data on a computer, either by altering or deleting it.

16. Logic bombs

- These are event dependent programs.
- This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs.
- E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only ona particular date (like the Chernobyl virus).

17. Trojan attacks

- A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

18. Internet time theft

- This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

19. Web jacking

- This occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
- The actual owner of the website does not have any more control over what appears on that website.

20. Theft of computer system

- This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system

- This crime is committed by physically damaging a computer or its peripherals.

- This is just a list of the known crimes in the cyber world.
- The unknown crimes might be far ahead of these, since the lawbreakers are always one-step aheadof lawmakers.

Who commits cyber crimes?

i. **Insiders -** Disgruntled employees and ex-employees, spouses, lovers

ii. **Hackers -** Crack into networks with malicious intent

iii. **Virus Writers -** Pose serious threats to networks and systems worldwide

iv. **Foreign Intelligence -** Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country

v. **Terrorists -** Use to formulate plans, to raise funds, propaganda

Need for Cyber law

- world is becoming **more and more digitally sophisticated** and so are the crimes.
- Transactional with e-business, e-commerce, e-governance and e-procurement etc.
- All legal issues related to internet crime are dealt with through cyber laws.
- In today's highly digitalized world, almost everyone is affected by cyber law.

Examples

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages forcommunication.
- Even in "**non-cyber crime" cases**, important evidence is found incomputers / cell phones.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.

Important terms related to cyber law [IT Act, 2000]

- Access
- Addressee
- Affixing Electronic Signature
- Asymmetric Crypto System
- Certifying Authority
- Communication Device
- Computer
- Computer Network
- Computer Resource
- Computer System
- Cyber café
- Cyber Security
- Data

- Digital Signature
- Electronic Form
- Electronic Record
- Electronic signature
- Function
- Information
- Intermediary
- Key Pair
- Originator
- Private Key
- Public Key
- Secure System
- Subscriber

Access

- Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Addressee

- Person who is intended by the originator to receive the electronic record but does not include any intermediary.

Affixing Electronic Signature

- adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature.

Asymmetric Crypto System

- secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Certifying Authority

- Person who has been **granted a license to issue** a Electronic Signature Certificate

Communication Device

- Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

Computer

- any electronic, magnetic, optical or other high-speed data processing device or system

Computer Network

- interconnection of **one or more Computers** or Computer systems or Communication device

Computer Resource

- computer, communication device, computer system, **computer network, data, computer database or software.**

Computer System

- Device or collection of devices, including input and output support devices

Cyber café

- Facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

Cyber Security

- Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Data

- Representation of information, knowledge, facts, concepts prepared in a formalized manner

Digital Signature

- Authentication of any electronic record by a subscriber by means of an electronic method or procedure.

Electronic Form

- Any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

Electronic Record

- data, **record or data generated**, image or sound stored, received or sent in an electronic form.

Electronic signature –

- Authentication of **any electronic record by asubscriber** by means of the electronic technique

Function

- in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer

Information

- includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

Intermediary

- Any particular electronic records, means any person who on behalf of another person receives, stores or transmits

Key Pair

- An asymmetric crypto system

Originator

- Person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated,stored or transmitted to any other person but does not include an intermediary.

Private Key

- key pair used to create a digital signature.

Public Key

- key pair used to **verify a digital signature** and listed in the Digital Signature

Secure System

- computer hardware, software, and procedure
- secure from unauthorized access and misuse
- provide a reasonable level of reliability and correct operation;
- reasonably suited to performing the intended functions; and
- adhere to generally accepted security procedures.

Subscriber

- Means a person in whose name the Electronic SignatureCertificate is issued.

CYBER LAW IN INDIA

- In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000.
- purpose of the Actis to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Act, Rules and Regulations are covered under cyber laws:

1. Information Technology Act, 2000
2. Information Technology (Certifying Authorities) Rules, 2000
3. Information Technology (Security Procedure) Rules, 2004
4. Information Technology (Certifying Authority) Regulations, 2001

Need for cyber law in India

- India has an extremely **detailed and well-defined legal system** in place.
- The existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace.
- None of the existing laws gave any legal validity or sanction to the activities in Cyberspace.
- Internet requires an enabling and supportive legal infrastructure in tune with the times.

Salient features of the Information Technology (Amendment) Act, 2008

- The term **'digital signature'** has been replaced with **'electronic signature'** to make the Act more technology neutral.
- A new section has been inserted to define **'communication device'** to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.
- A new section has been added to **define cyber cafe** as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- A new definitions has been **inserted for intermediary**.

a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

b) The Information Technology (Electronic Service Delivery) Rules, 2011

c) The Information Technology (Intermediaries guidelines) Rules, 2011

d) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011

e) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009

f) The Cyber Appellate Tribunal (Procedure for investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009

g) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009

h) The Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009

i) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

j) The Information Technology (Use of electronic records and digital signatures) Rules, 2004

k) The Information Technology (Security Procedure) Rules, 2004

l) The Information Technology (Other Standards) Rules, 2003

m) The Information Technology (Certifying Authority) Regulations, 2001

n) Information Technology (Certifying Authorities) Rules, 2000