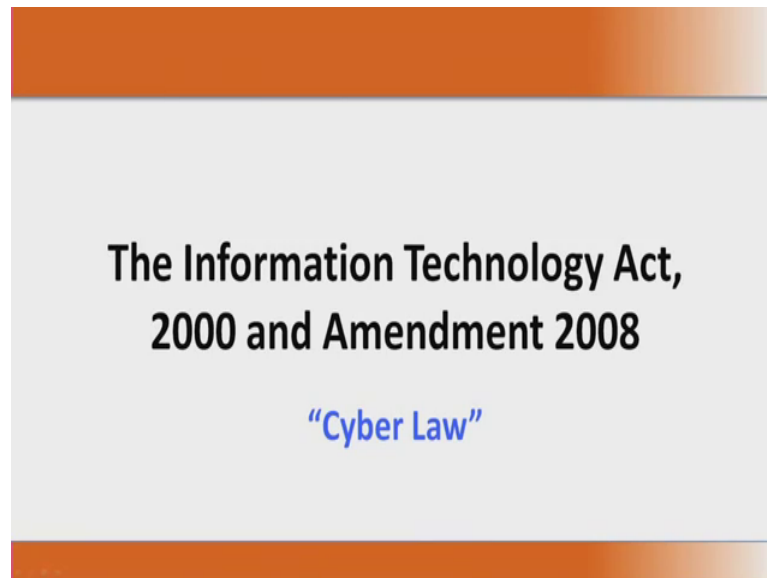


Introduction to Information Security
Prof. Dilip H. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

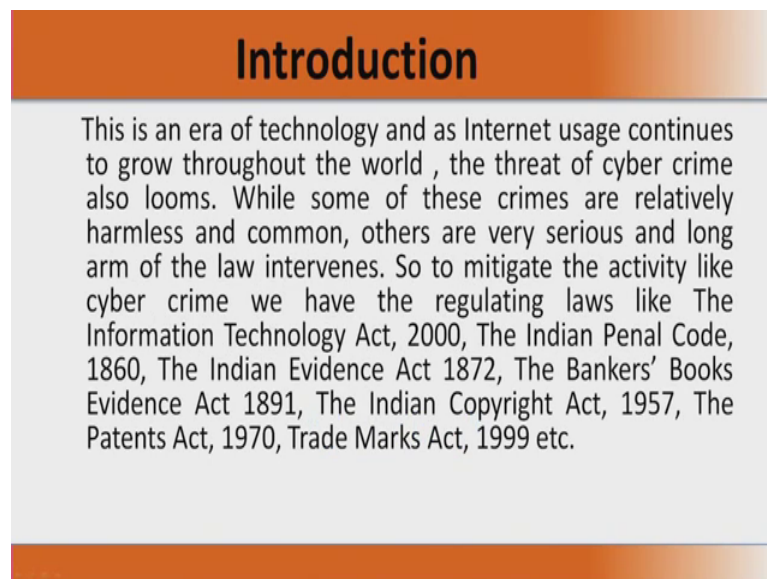
Lecture – 31

(Refer Time Slide: 00:15)



Let us take a look at our own information technology acts, which was in, which is in force in 2000, and the amendments which were done in 2008.

(Refer Time Slide: 00:21)

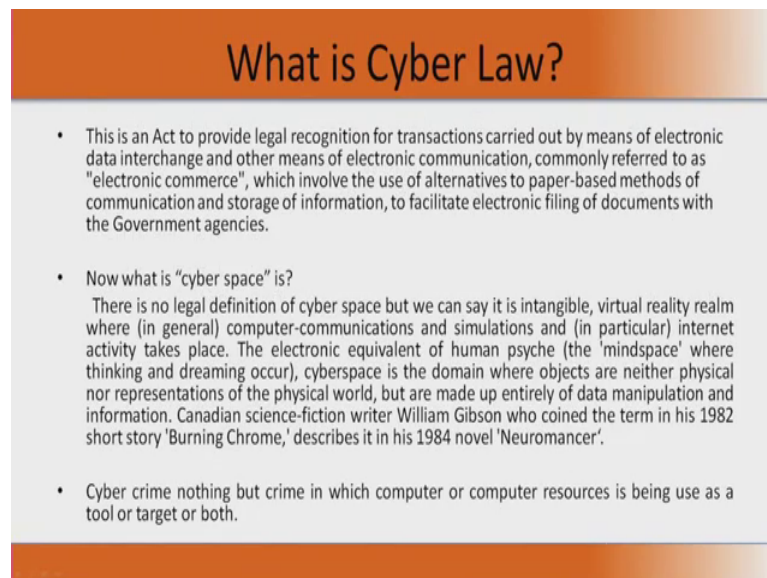


Now, to give a simple introduction, why these laws are required, this is an era of technology where the technology overtakes everything, and the internet usage continues

to grow throughout the world. So, everywhere on a mobile phone at home, in an office everywhere, there is a massive use of internet as a medium of communication, a medium for sharing information, medium for uploading downloading files, a medium for collaborating, corroborating with your loved one's.

So, the threat the advent of internet is so much that, the threat also naturally increases with the increased use of technology. Some of the crimes may be relatively small, and harmless, but there are against very serious crimes, that are committed in the cyber world. And the long arm of the law, also intervenes punishes are lays down, that this is what has to be done, and this is what should not be done. But to mitigate the activity like cyber crime, we have regulating laws like the IT act 2000, some of the earlier laws or the laws that we have in India, as of now the Indian penal code 1860, Indian's evident act 1872, banker's books evidence act 1891, copyright act 1957, patents act 1970, trademarks act 1999. So, this is, so many laws are there. Similarly, information technology act is also which was or which is in force since 2000.

(Refer Time Slide: 02:16)



What is Cyber Law?

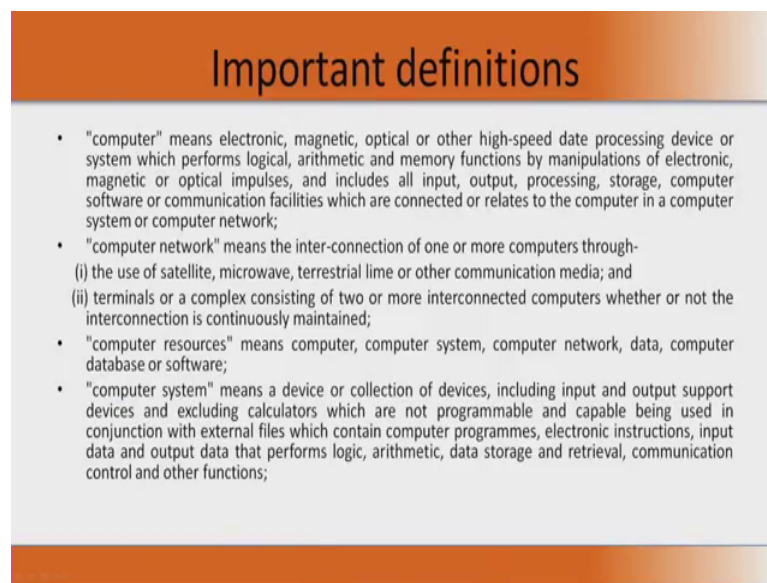
- This is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.
- Now what is "cyber space" is?
There is no legal definition of cyber space but we can say it is intangible, virtual reality realm where (in general) computer-communications and simulations and (in particular) internet activity takes place. The electronic equivalent of human psyche (the 'mindspace' where thinking and dreaming occur), cyberspace is the domain where objects are neither physical nor representations of the physical world, but are made up entirely of data manipulation and information. Canadian science-fiction writer William Gibson who coined the term in his 1982 short story 'Burning Chrome,' describes it in his 1984 novel 'Neuromancer'.
- Cyber crime nothing but crime in which computer or computer resources is being use as a tool or target or both.

What is this cyber law, this is specifically an act to provide re legal recognition for the transactions, carried out by means of electronic data, interchange EDI or other means of electronic communication. This definition, what I am reading out is actually what is there in the cyber law. So, this is an act, to provide legal recognition for the transactions carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as electronic commerce, e-commerce which involves the use of alternatives to paper based methods. So, you this is applicable to

anything, that happens legally if you are using BYOD, bring you own devices like mobiles, or your computers, the laptops, the kiosks, anything that use in an electronic form, as an alternative to paper media, this cyber law is applicable.

Even in the income tax statements, there are several regulatory things, that you can upload using a digital signature, to the regulatory authority, is a valid form which is accepted by the regulatory bodies. All those transactions all those happenings, come under the ambit of IT act 2000.

(Refer Time Slide: 03:50)



Important definitions

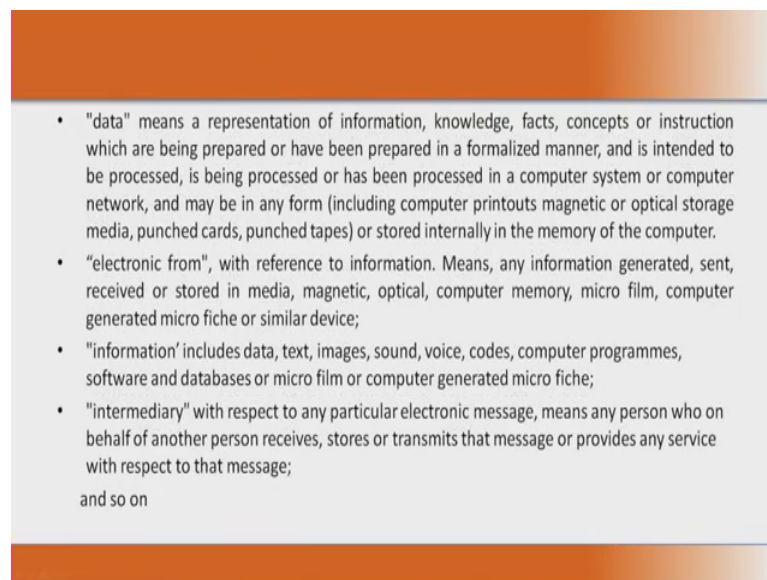
- "computer" means electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or relates to the computer in a computer system or computer network;
- "computer network" means the inter-connection of one or more computers through-
(i) the use of satellite, microwave, terrestrial line or other communication media; and
(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;
- "computer resources" means computer, computer system, computer network, data, computer database or software;
- "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

Some of the important definitions as per IT act, they defined computer as electronic magnetic optical, or other high speed data processing device. Or system, which performs logical, arithmetic, memory functions, by manipulations of electronic, magnetic, or optical impulses, and includes all input, output processing storage, Computer software, or communication facilities, which are connected or relates to the computer in a computer system or computer network.

So, computer network, it is also defined as a means of inter connection of one or more computers, through one use of satellites, microwaves, terrestrial lines, or other communication media. So, network is we will see in domain 4, what a network is, types of networks, all of these will be covered under them. Two, terminals or complex or a complex consisting of 2, or more inter connected computers, whether or not the interconnection is continually maintained.

So, it can be just connecting for all particular section, and then coming up again, this also we will see. And computer resources, also is defined here, it means computer, computer system, computer network, data, computer database or software so everything is covered under computer resources. And computer system means a device, or collection of devices including input, output support devices, and excluding calculators, which are not programmable, and capable of being used in conjunction with external files. Which contain computer programs, electronic instructions, input data and output data, that performs logic arithmetic data storage, retrieval communication control and functions. So, almost everything is covered under the definition, it will take some time to register these words, or to understand these words. So, I will allow sinking it to.

(Refer Time Slide: 06:15)



- "data" means a representation of information, knowledge, facts, concepts or instruction which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- "electronic form", with reference to information. Means, any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
- "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;
- "intermediary" with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;
and so on

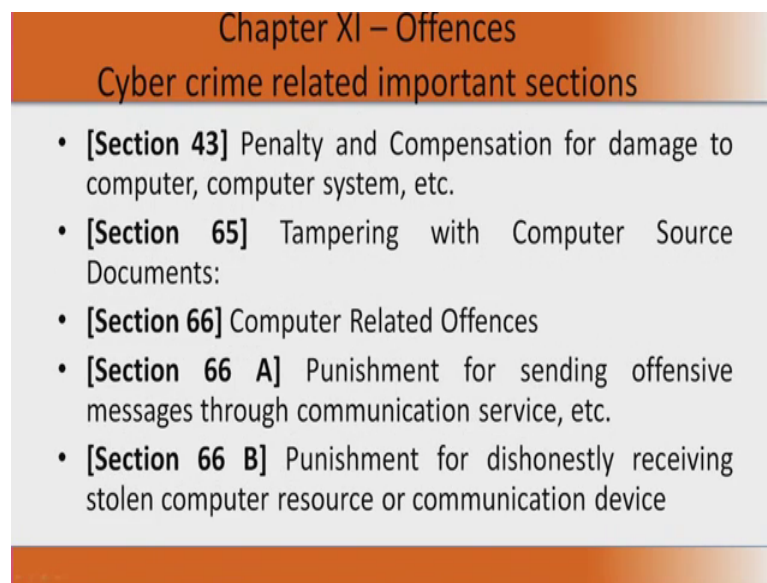
So, that you will understand it, after all couple of slides. Data is also explained here in the IT act 2000, data means representation of information, knowledge, the facts, concepts or instructions which are being prepared, or have been prepared. So, it something in progress, or in process, and something you just already done in a formalized manner with proper procedure, and is intended to be processed.

So, either it is done, or it is intended to be processed, is being processed, or has been processed in a computer system, or computer network, and may be in any form. It can be computer printouts, it can be magnetic or optical storage, magnetic is your the tape system, optically is your cd, dvds, punched cards, punched tapes, or it can be stored internally in the hard disk, or memory of the computer.

And electronics form with reference to information, means any information generated, sent, received or stored in media magnetic optical memory, micro film, computer generated micro fiche, or similar device. So, electronic form is in reference, is all these things are under electronic forms. And information includes data, text images, sound video, computer programs, software's, databases or micro film or computer generated micro fiche. All of those are covered under them.

Here the information, what they have mentioned is, it includes data also. So, raw data is also included, data in it is raw form is data, when it is processed it is information. Then intermediary with respect to any particular electronic message means, any person who on the behalf of another person, receives, stores, transmits the message or provides any service with respect to the message. So, these are some of the important terminologies is that, have been specified in IT act 2000.

(Refer Time Slide: 08:47)



Chapter XI – Offences
Cyber crime related important sections

- **[Section 43]** Penalty and Compensation for damage to computer, computer system, etc.
- **[Section 65]** Tampering with Computer Source Documents:
- **[Section 66]** Computer Related Offences
- **[Section 66 A]** Punishment for sending offensive messages through communication service, etc.
- **[Section 66 B]** Punishment for dishonestly receiving stolen computer resource or communication device

Now, will go straightly or directly, to some of the offenses which have been classified in chapter 11, of the cyber crime, IT act 2000. Will not go into details of all these sections, and penalties for now, but you can always download a copy of the cyber law, from the Deity sites, or any other site, you can Google search for IT act, and its amendments. And you will get it, if am, if you interested and learning more you can always download, and learn.

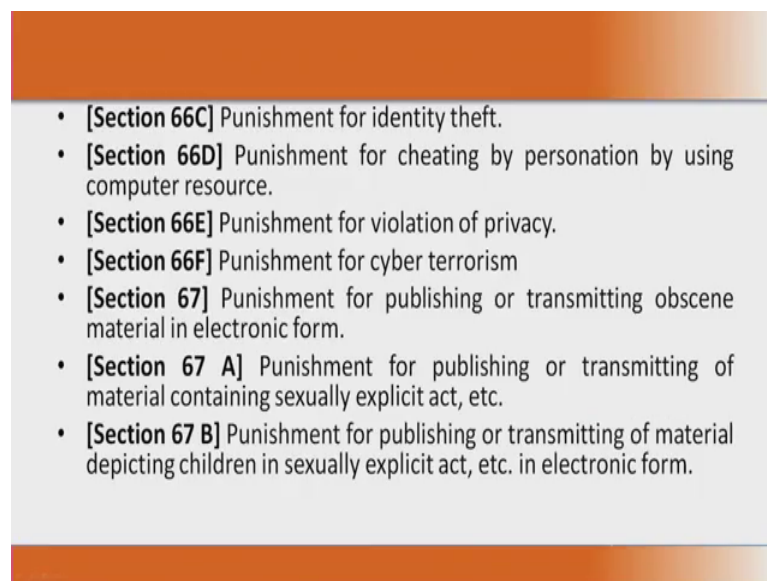
Some of the important sections are section 43, which specifies penalty and compensation for damage, to computer, computer system etc. So, when we talk about information

security itself in this program, throughout this program, we say confidentiality of information, integrity, and availability of information, there is the threat of disclosure alteration distraction. Now, 43 specifies penalty for damage, to computer or computer system.

Damage can be both physical, and logical. 65 is tampering with computer source documents, integrity is affected. 66 computer related offenses. So, all kinds of computer related, that we have going to talk about or have talked about will be covered under that. 66a is punishment for sending offensive messages, through communication service, or mobile service.

We have read a load of lots of news, about these sending lewd messages, to somebody sending obscene photographs. So, all those are covered in this. 66b specifies punishment, for dishonestly receiving stolen computer resources, or communication device. So, that is also covered.

(Refer Time Slide: 10:44)

- 
- **[Section 66C]** Punishment for identity theft.
 - **[Section 66D]** Punishment for cheating by personation by using computer resource.
 - **[Section 66E]** Punishment for violation of privacy.
 - **[Section 66F]** Punishment for cyber terrorism
 - **[Section 67]** Punishment for publishing or transmitting obscene material in electronic form.
 - **[Section 67 A]** Punishment for publishing or transmitting of material containing sexually explicit act, etc.
 - **[Section 67 B]** Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

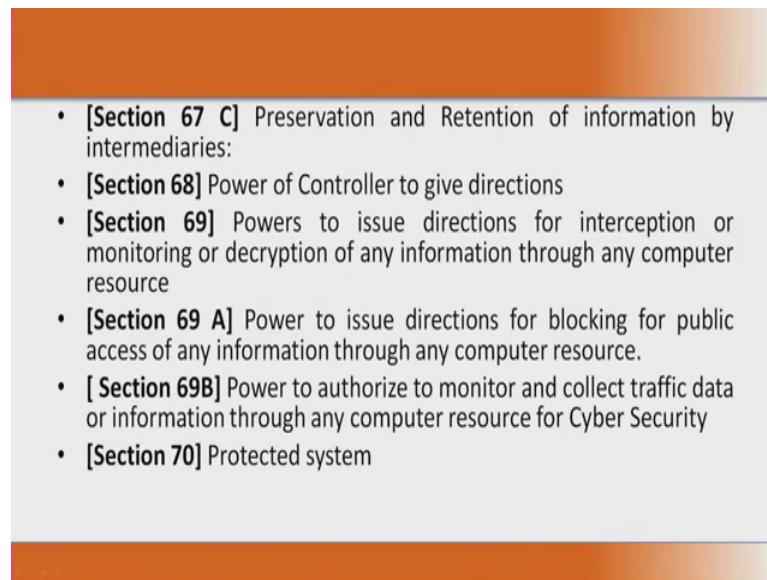
66c is punishment for identity theft, which is perhaps the most used kind of social engineering attack, which is happening right now identity theft is, where somebody masquerades you, and tries to commit a felony or a fraud using your identity. So, identity theft, it can be even simple things to learn about you from facebook.

So, which is always advisable not to put, too much information in facebook, not to put too much photos on facebook, I actually came across a person, who was telling me that, one of his relatives photo had been morphed, and used for some bad obscene purposes in

facebook. So, these things can happen. And 66d is punishment for cheating by personation, by using computer resource again logically

if you try to masquerade somebody else, that is covered here. Violation of privacy, this also we have read in the papers write a law invasion of privacy. So, there is the punishment for that. 66f is cyber terrorism, cyber bullying, online creditors know all of these or covered here. 67 is punishment for publishing, or transmitting obscene material in electronic form.

(Refer Time Slide: 13:07)

- 
- **[Section 67 C]** Preservation and Retention of information by intermediaries:
 - **[Section 68]** Power of Controller to give directions
 - **[Section 69]** Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
 - **[Section 69 A]** Power to issue directions for blocking for public access of any information through any computer resource.
 - **[Section 69B]** Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security
 - **[Section 70]** Protected system

So, we see that you say organization is a firewall, it blocks uploading, downloading of file, but why it is not only for the organizations information, storage requirements and information security requirements. Also to compliant with a law, you cannot have somebody upload or download obscene photos from the internet, or to the internet. 67a is punishment for publishing, or transmit, transmitting of material, contain containing sexually explicit act etcetera.

So, next time you watching a porn, think of 67a. 67b is punishment for publishing or transmitting material, depicting children in sexually explicit act in electronic form. 67c is preservation, and retention of information by intermediaries. 68 is power of controller to give directions. So, there are certain rules are mandated, or powers given to the controllers, to give directions to the police, to other people to intercept messages, to capture messages.

That is again specified in 69 powers to issued directions for interception, or monitoring or decryption, of any information through any computer resources. That is also there. 69a is power to issue directions, for blocking for public access of any information through computer resources. 69b is power to authorize to monitor, and collect traffic data or information through any computer resource for cyber security. And 70 deals with protected system. 70a is national, nodal in agency.

(Refer Time Slide: 14:03)

- **[Section 70 A]** National nodal agency
- **[Section 70 B]** Indian Computer Emergency Response Team to serve as national agency for incident response.
- **[Section 71]** Penalty for misrepresentation
- **[Section 72]** Breach of confidentiality and privacy
- **[Section 72 A]** Punishment for Disclosure of information in breach of lawful contract
- **[Section 73]** Penalty for publishing electronic Signature Certificate false in certain particulars.
- **[Section 74]** Publication for fraudulent purpose
- **[Section 75]** Act to apply for offence or contraventions committed outside India.

Why these specific things have been put is the Indian computer emergency response team is a very important agency under DIDY to respond to computer incident, and they work in the interest of your national security. So, 70a and 70b, so government has mandated Indian sat is the national nodal agency for all this computer related things.

So, you can also google about Indian sat. 71 is penalty for misrepresentation. 72 is breach of confidentiality, and privacy. 72a is punishment for disclosure of information. Again it is an opposite of confidentiality, 73 is penalty for publishing electronic signature certificate, false in certain particulars or false electronic signature. And particular 74 is publication for fraudulent purpose, and 75 is act to apply for offense, or contraventions committed outside India.

(Refer Time Slide: 15:26)

- **[Section 76]** Confiscation
- **[Section 77]** Compensation, penalties or confiscation not to interfere with other punishment.
- **[Section 77 A]** Compounding of Offences.
- **[Section 77 B]** Offences with three years imprisonment to be cognizable.
- **[Section 78]** Power to investigate offences

We think we discussed a few slides ago, 76 is who can confiscate, or confiscation. 77 is compensation penalties or confiscation, not to interfere with other punishment. 77a is compounding of offenses. 77b is offenses with 3 years imprisonment, to be cognizable. 78 is power to investigate offenses. So, there are several laws with respect to the computer crimes, that find place in the information technology act 2000, and it is amendment.

So, we should be proud that in India also, we are keeping up with the times, and implementing and have rules, and regulations to control, and monitor the computer activity. So, next time, you want to do something, or you do something, which is not as per this, you will have to think twice and do. The most important thing to remember is all these are done with protecting, the information related to national security.

So, it starts with a person, then it starts with an organization, it starts with it grows into a state finally it grows, into the national level. So, cyber laws you would encourage you to download it, read it, understand it, not for this sake of examination or anything else, but to know that, there are loss in the country, which help you has an individual or you has an organization, and also which helps in preventing crimes, with this we come to the end of module 2.

(Refer Time Slide: 17:14)



End of Module - 2

We look forward, to see you in module 3 and try to learn new concepts, and to see what the different kinds of threats are.

Thank you.