Course : PGDCL-05

Vardhaman Mahaveer Open University, Kota

Cyber securities and Cyber Terrorism

Course Development Committee **PGDCL-05**

Chairman

Prof. L. R. Gurjar

Director (Academic)

Vardhaman Mahaveer Open University, Kota

Convener and Members

Convener

Dr. Yogesh Sharma, Asso. Professor
Department of Law
Vardhaman Mahaveer Open University, Kota

Prof. H.B. Nanadwana
Director, SOCE
Vardhaman Mahaveer Open University, Kota

External Members:

1. Prof. Satish C. Shastri
Dean, Faculty of law, MITS, Laxmangarh
Sikar, and Ex. Dean,
University of Rajasthan, Jaipur (Raj.)

2. Prof. V.K. Sharma
Deptt.of Law
J.N.Vyas University, Jodhpur

3. Dr. M.L. Pitaliya
Ex. Dean, MDS University, Ajmer
Principal, Govt. P.G.College, Chittorgarh (Raj.)

4. Prof. (Dr.) Shefali Yadav
Professor & Dean - Law
Dr. Shakuntala Misra National
Rehabilitation University, Lucknow

5. Dr Yogendra Srivastava,
Asso. Prof. School of Law,
Jagran Lakecity University, Bhopal

Editing and Course Writing

Editor:
Dr. Yogesh Sharma
Convener, Department of Law
Vardhaman Mahaveer Open niversity, Kota

Course Writer:
Dr. Shobha Bhardwaj
Faculty of Law, Jagran Lackcity University
Bhopal

Academic and Administrative Management

Prof. Vinay Kumar Pathak
Vice-Chancellor
Vardhaman Mahaveer Open University, Kota

Prof. L.R. Gurjar
Director (Academic)
Vardhaman Mahaveer Open University, Kota

Prof. Karan Singh
Director (MP&D)
Vardhaman Mahaveer Open University, Kota

Prof. H.B. Nanadwana
Director, SOCE
Vardhaman Mahaveer Open University, Kota

Course Material Production

Prof. Karan Singh

Director (MP&D)

Vardhaman Mahaveer Open University, Kota

Production 2015 ISBN-978-81-8496-580-3

Vardhaman Mahaveer Open University, Kota
PGDCL -05 Cyber Securities and Cyber Terrorism

Unit-1

Data Security and Management

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Data Security and Management
- Understand the international efforts with reference to Data Security and Management
- Understand the technical and legal issues related to Data Security and Management

Summary:

1.1 Introduction:

Computer security is an unsolvable problem. So instead of trying to solve it, companies should think of network security as a set of risks that are inherent in doing business online. Viewing security from that perspective will lead to better decisions and superior technological design. Obviously, security gives rise to some straightforward problems, and businesses should examine whether they have solved them. The recent revelation that the payment protocols in some widely used e-commerce sites allowed customers to purchase even physical goods without paying is an example of a security problem that is quantifiable and solvable. But more often, computer security is better tackled with a risk-management approach, one that does not require exact quantification. It's a personnel problem—much like office conflict, minor theft, misrepresentation of employee credentials, and employee health. Consider that employees who take risks to get their jobs done are both assets to the organization and threats to computer security. For example, an employee who manages to tunnel around the corporate firewall to log in remotely sees the positive results of access from home. The employee's supervisor sees only increased productivity. Security risks are part of getting the job done. Networking and connectivity inherently include risk just as hiring a human being inherently carries risk.

1.2 What is Data Security?

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre. Data security is also known as information security (IS) or computer security. Examples of data security technologies include software/hardware disk encryption, backups, data masking and data erasure.

A key data security technology measure is scrambling, where digital data, software/hardware, and hard drives are scrambled and rendered unreadable to unauthorized users and hackers. Data security is also very important for health care records, so health advocates and medical practitioners in the U.S. and other countries are working toward implementing electronic medical records (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities.

Data security and privacy deliver data protection across enterprise. Together, they comprise the people, process and technology required to prevent destructive forces and unwanted actions. Data security and privacy aren't a nice-to-have. They are required by more than 50 international legal and industry mandates, as well as business leaders. With 2.5 quintillion bytes of data created every day, and with the average cost of security-related incidents in the era of big data estimated to be over USD40 million, now is the time to keep customer, business, personally identifiable information (PII) and other types of sensitive data safe against internal and external threats. Data should be protected no matter where it resides—in databases, applications or reports across production and non-production environments. Data is the raw form of information stored as columns and rows in our databases, network servers and personal computers. This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form.

However, some of this information isn't intended to leave the system. The unauthorized access of this data could lead to numerous problems for the larger corporation or even the personal home user. Having your bank account details stolen is just as damaging as the system administrator who was just robbed for the client information in their database. There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down your data from software solutions to hardware mechanisms. Computer users are certainly more conscious these days, but are your data really secure? If you're not following the essential guidelines, your sensitive information just may be at risk.

1.3 Protecting Sensitive Data:

The Information Age has brought with it the ability to share, store, and transmit data with the click of a mouse. The risky part of this equation is that storage and transmission of sensitive data across computer systems can be difficult to protect, increasing the need for vigilance. In the paper world, if a document is marked "CLASSIFIED" or "CONFIDENTIAL", we can easily protect it by placing it face-

down on our desk when someone walks by that does not have a need to know, lock it in a file cabinet when it is not being used, or when needing to share use a courier or hand-deliver to the appropriate person, and finally when it is no longer needed we can shred it. We need to take these same precautions in the computer world. Computer systems are complex. They can include operating system software, applications and programs, databases, hardware components, and networks. Each of these elements requires a different method for protecting the data. Adding to the complexity is the dynamism in terms of the way the systems and their parts interact and their requirement for frequent updates to fix bugs or protect against the latest hack attack. All of this collectively underscores the need for each of us to take responsibility to protect the sensitive data we handle. OIT is here to help, if you ever have questions about the security of a system or an electronic document you are handling. In general, Information Security professionals suggest that protecting sensitive data requires a combination of people, processes, polices, and technologies.[1]

1.4 Browser Sensitive Data:

Back in summer 2013 Google was criticized for storing user login information username and password in plaintext in the web browser without any sort of protection. For some, this was a critical security risk that could easily have been avoided, for instance by implementing a master password protecting the data. Others and Google pointed out that local access was required to access the data, and if local access was granted, the computer was compromised anyway opening other attack vectors as well. A few days ago, security research company Identity Finder, discovered another related issue in Google Chrome. According to the company's findings, Chrome stores sensitive information, entered on https websites and services, in plaintext in the browser cache. While many believe that browser's do not cache https pages and data because of the secure nature of the connection, it needs to be noted that https contents may be cached. This depends solely on a site's or server's response headers (that are transferred to the web browser). If the caching headers allow the caching of HTTPS contents, web browsers will do so.

[1] http://www.american.edu/oit/security/Protecting-Data.cfm

Chrome and sensitive data: Identity Finder discovered that Chrome was storing a range of sensitive information in its cache including bank account numbers, credit card numbers, social security numbers, phone numbers, mailing addresses, emails and more. The company confirmed that these information were entered on secure websites, and could easily be extracted from the cache with search programs that scan any type of file for plaintext data. The data is not protected in the cache, which means that anyone with access to it can extract the information. This does not necessarily mean local access, as malicious software running on a user's computer, and even social engineering, may yield the same results. Handing over the computer to a computer repair shop, sending it in to the manufacturer, or selling it on eBay or Craigslist may provide third parties with access to sensitive information stored by the browser.

How can you protect your data against this? Google wants you to use full disk encryption on your computer. While that takes care of the local access issue, it won't do a thing against malware attacks or social engineering. It is like saying that website operators may save passwords in plaintext in the database, as the battle is lost anyway if someone gains access to the server locally or remotely. In regards to Chrome, the only option that you have is to clear the cache, auto fill form data and browsing history regularly and preferably right after you have entered sensitive information in the browser. You cannot automate the process using Chrome alone, but need a third party tool or extension to clear the data when you close the browser automatically.'

Other browsers: Identity Finder only analyzed the cache of Google Chrome and if you are not using the browser, you are probably wondering if your browser stores sensitive information in plaintext as well. Firefox, almighty when it comes to customizing the browser, lets you disable SSL caching in the advanced configuration.

- Type about: config in the address bar and hit enter.
- Confirm you will be careful if this is your first visit to the page.
- Search for **browser.cache.disk_cache_ssl**
- Set the preference to false with a double-click on its name to disable SSL caching.
- Repeat the process if you want to enable it again.

Firefox will use the computer's memory to cache files, which means that the information are automatically deleted when Firefox closes, and never recorded to disk.[2]

1.5. Data Governance:

Data governance (DG) refers to the overall management of the availability, usability, integrity, and security of the data employed in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures, and a plan to execute those procedures. The initial step in the implementation of a data governance program involves defining the owners or custodians of the data assets in the enterprise. A policy must be developed that specifies who is accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness, and updating. Processes must be defined concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack. A set of standards and procedures must be developed that defines how the data is to be used by authorized personnel. Finally, a set of controls and audit procedures must be put into place that ensures ongoing compliance with government regulations.

Focus Areas for Data Governance: Focus on Data Quality: This type of program typically comes into existence because of issues around the quality, integrity, or usability of data. It may be sponsored by a Data Quality group or a business team that needs better quality data. (For example: Data Acquisition or Mergers & Acquisitions.). These types of programs almost always involve Data Quality software, which may be used by business staff, technical staff, Data Stewards, Data Governance teams, or others. These types of programs may begin with an enterprise focus, or efforts may be local to a department or a project. Sometimes, such governance groups adopt the philosophy of “act local, but think global” so the program will be ready to scale should other groups in the enterprise want to reap the benefits being realized by early adopters.

[2] http://www.ghacks.net/2013/10/12/google-chrome-saves-sensitive-data-entered-https-websites-plaintext/

What type of data do such programs generally address in early iterations of the program?

- Sets of Master Data
- Sensitive Data
- Acquired Data
- Data of interest to stakeholder groups

A charter for this type of program may hold Data Governance and Stewardship participants accountable to:

- Set direction for Data Quality
- Collect Data Quality rules from across the organization into a set that stakeholders, Data Stewards, and other Data Governance participants can access
- Reconcile gaps, overlaps, and inconsistencies in Data Quality rules
- Monitor Data Quality
- Report status for quality-focused initiatives
- Identify stakeholders, establish decision rights, clarify accountabilities

All Data Governance programs are not alike. Quite the contrary: programs can use the same framework, employ the same processes, and still appear very different.

Why is this? It's because of what the organization is trying to make decisions about or enforce rules for. An organization that is concerned with Data Privacy or Compliance is going to look at its data differently than one that is concerned about implementing a new Data Warehouse.

In this section, we look at Data Governance programs with six common focus areas. It's worth noting: A single framework can help organize efforts for all of these focus areas because of what all Data Governance programs have in common:

- They all have activities that address a three-part governance mission: to create rules, resolve conflicts, and provide ongoing services.
- They all employ most or all of the universal components of a Data Governance program.

- They all address universal governance processes and services, such as Issue Resolution and Stakeholder Care.

Data Governance programs with different focus areas will, however, differ in the type of rules and issues they'll address.

They'll differ in the emphasis they give to certain data-related decisions and actions.

And, they'll differ in the level of involvement required of types of data stakeholders.

Who is a data stakeholder?: Any individual or group that could affect or be affected by the data under discussion. Some stakeholders are obvious – business groups, IT teams, Data Architects, and DBAs. Other stakeholders may not be so obvious for a given decision or situation. Knowing which stakeholder to bring to the table – and when – is the responsibility of the Data Governance team.

Focus Areas for Data Governance: Focus on Privacy / Compliance / Security: This type of program typically comes into existence because of concerns about Data Information Security controls, or compliance. Compliance, in this context, may refer to regulatory compliance, contractual compliance, or compliance with internal requirements. This focus is often seen combined with a focus on policy enforcement. It's also seen combined with a focus on Data Quality.

The program almost always results from a senior management mandate. It may be formally sponsored by Business or IT, or it may be an outgrowth of a Governance, Risk, and Compliance (GRC) program. These programs generally begin with an enterprise scope, but often efforts are limited to specific types of data. They almost always include technologies to locate sensitive data, to protect data, and/or to manage policies or controls.

A charter for this type of program may hold Data Governance and Stewardship participants accountable to:

- Help locate sensitive data across systems
- Align governance, compliance, security, and technology frameworks and initiatives
- Help assess risk and define data-related controls to manage risk
- Help enforce regulatory, contractual, architectural compliance requirements

- Support Access Management and Security requirements
- Identify stakeholders, establish decision rights, clarify accountabilities[3]

1.6. Internet Explorer and Network Security:

General network security recommendations- The following are general security guidelines for all home and small office networks:

Keep your computer up to date: To help keep the computers on your network safer, turn on automatic updating on each computer. Windows can automatically install important and recommended up dates, or important updates only. Important updates provide significant benefits, such as improved security and reliability. Recommended updates can address non-critical problems and help enhance your computing experience. Optional updates are not downloaded or installed automatically.

Use a firewall: A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

Run antivirus software on each computer: Firewalls help keep out worms and hackers, but they're not designed to protect against viruses, so you should install and use antivirus software. Viruses can come from attachments in e-mail messages, files on CDs or DVDs, or files downloaded from the Internet. Make sure that the antivirus software is up to date and set to scan your computer regularly.
There are many antivirus programs available. Microsoft offers Security Essentials, a free antivirus program you can download from the Microsoft Security Essentials website. You can also go to the Windows Security software provider's website to find a third-party antivirus program.

Use a router to share an Internet connection: Consider using a router to share an Internet connection. These devices usually have built-in firewalls, network address translation (NAT), and other features that can help keep your network better protected against hackers.

[3] http://www.datagovernance.com/

Don't stay logged on as an administrator: When you're using programs that require Internet access, such as a web browser or an e-mail program, we recommend that you log on as a standard user account rather than an administrator account. That's because many viruses and worms can't be stored and run on your computer unless you're logged on as an administrator.

Wireless network security recommendations: If you have a wireless network, there are some additional security precautions that you should take.Use a network security key: If you have a wireless network, you should set up a network security key, which turns on encryption. With encryption, people can't connect to your network without the security key. Also, any information that's sent across your network is encrypted so that only computers that have the key to decrypt the information can read it. This can help avert attempts to access your network and files without your permission. Wi-Fi Protected Access (WPA or WPA2) is the recommended wireless network encryption method.

Change the default administrator name and password on your router or access point: If you have a router or access point, you probably used a default name and password to set up the equipment. Most manufacturers use the same default name and password for all of their equipment, which someone could use to access your router or access point without your knowledge. To avoid that risk, change the default administrator user name and password for your router. Check the information that came with your device for instructions about how to change the name and password.

Change the default SSID: Routers and access points use a wireless network name known as a service set identifier (SSID). Most manufacturers use the same SSID for all of their routers and access points. We recommend that you change the default SSID to keep your wireless network from overlapping with other wireless networks that might be using the default SSID. It makes it easier for you to identify which wireless network is yours, if there's more than one nearby, because the SSID is typically shown in the list of available networks. Check the information that came with your device for instructions about how to change the default SSID.

Position your router or access point carefully: Wireless signals can transmit a few hundred feet, so the signal from your network could be broadcast outside of your home. You can help limit the area that your wireless signal reaches by positioning your router or access point close to the center of your home rather than near an outside wall or window.[4]

1.7 Windows-Microsoft: Help to protect your PC[5]:

Account(ing) for each computer user

When you first set up Windows, you'll need to create an administrator account. An administrator account gives you the most control over the computer, what software to install, and who else can use it. You can use your administrator account to set up standard user accounts for other users.

If you're sharing your home computer with others, like your kids, husband, or wife, a separate standard user account for each user lets each person log in to a personalized experience. For example, you can set your desktop background to a picture from your Hawaii vacation, while your adolescent son might have a scrolling background of customized hot rods. Or vice versa. User accounts also determine the permissions each user has to access different files and programs or change computer settings. Each person who regularly uses your computer should have a standard account, so that they can customize their experience without impacting the other users. For more information, see User accounts: frequently asked questions.

A strong word about passwords

A password is one of the easiest ways to help protect your computer from hackers, your children, or any unauthorized user. Just as your debit card PIN is a barrier between bad guys and your bank account, a computer password is a barrier between unauthorized users and your user account. For more details, see Protect your computer with a password.

When you're choosing a password, you should make it difficult for others to guess or crack. My dad learned this the hard way when he set his password to

[4] http://windows.microsoft.com/en-in/windows/making-network-more-secure#1TC=windows-7
[5] http://windows.microsoft.com/en-IN/windows7/taking-control-of-computer-security

simply the letter "A." My sister and I deciphered that in a hurry and reconfigured his desktop for maximum hilarity (us) and maximum annoyance (Dad). Strong passwords shouldn't be too obvious—so your name, your pet's name, or your birth date aren't the best password candidates. To learn more, see Tips for creating strong passwords and passphrases.

User Account Control: Mother, may I?

The User Account Control (UAC) feature in Windows is another way to help you control significant changes to your computer. If you want to make a change that requires administrator permission—like installing new software or changing Windows settings—UAC notifies you. If you're using an administrator account, you're prompted to confirm the change. Standard users are prompted to enter an administrator password before the change can be made.

Help protect your PC from online threats

The tips above can help protect your computer from security mishaps in the home, but when you're using the Internet, you need to consider other precautions. You should establish a good security plan, keep it current, and use a little everyday common sense.

Use security software:

Think of Windows Firewall as a barrier between your computer and any marauding hackers (or unsolicited spammers) on the Internet. Windows Firewall checks information coming in to and going out of your computer. If the information appears safe, it's passed through. If the information appears to come from a shady source or contain malicious software (like a worm or virus), a firewall can help block it and also help prevent your computer from spreading malicious software to others if it's already been infected. Windows Firewall is turned on by default, but you can choose to allow specific programs—like instant messaging—through the firewall, or you can block all incoming connections to your computer if you're using a public network in an airport or coffee shop. For more information, see Understanding Windows Firewall settings.

Spyware might irritate you by displaying pop-up ads or adding unwanted toolbars and links in your web browser—or it might secretly collect information about you and your computer use and send that information back to others. To help protect your computer against spyware, you can use an antispyware program like Windows Defender. Windows Defender is also turned on by default, and it can

scan your computer for existing spyware to remove it or alert you when new spyware tries to install itself. For more information, see Using Windows Defender.

You should also install antivirus software to scan e-mails and other files for destructive programs and block them. Viruses, worms, and Trojan horses don't necessarily expose your personal information to others, but they can delete important files and slow down or even completely disable your computer. Most viruses can also replicate and distribute themselves via e-mail to all of your contacts, a quick way to make enemies out of the friends in your address book. To help prevent this from happening. You can download Microsoft Security Essentials, a free antivirus program from Microsoft, by going to the Microsoft Security Essentials website. You can also visit the Windows 7 consumer's security software provider's webpage to find a third-party antivirus program.

Monitor and update your security plan: Bad guys are diligent, so your security software is only as good as it is current. But keeping track of security updates, and making them automatically, are easier in Windows 7 with the new Action Center.

1.8 Data Security Management:

Data security management is a way to maintain the integrity of data and to make sure that the data is not accessible by unauthorized parties or susceptible to corruption of data. Data security is put in place to ensure privacy in addition or protecting this data. Data itself is a raw form of information that is stored on network servers, possible personal computers and in the form of columns and rows. This data can be anything from personal files to intellectual property and even top-secret information. Data can be considered as anything that can be understood and interpreted by humans.

Because the internet is a growing phenomenon, there was and always will be an emphasis on protecting personal or company data. Computer users as time goes on tend to be slightly more aware with their files, but are still encouraged to use some sort of data security. Data security methods can be acquired by using specific software solutions or hardware mechanisms.

Information can be encrypted or unreadable to a person with no access. When encrypting this data, mathematical sequences and algorithms are used to

scramble information. Encryption allows only an approved party to decode this unreadable text with a key. Only those that have this key can access any information. Authentication is another form of data security to be used for more daily access. A sign-on to an email account, bank account etc., only allows the user with the proper key or password. The most commonly used method of keeping data protected is with data security software. This software keeps unauthorized parties from accessing private data and offers a variety of different options. Some of these options include requiring a sign-on to email accounts, rewriting of software, and being able to control security options remotely. Data can also be protected with IP security. This means that data can be protected from a hacker while in transit.

One of the biggest reasons to keep data protected is because there are many corporations that hacker want to target and breach. Data security tends to be necessary for large businesses but the small ones usually have fewer infrastructures in place, making the information not a great loss if breached. Depending on the services and content that is to be protected, there can be preventative measures to further protect the information. For example Windows Rights Management Services (RMS) can be set to control whether or not the recipient of an email can be read and viewed, edited, copied or saved; these setting can also set an expiration date of a specific document.

By keeping data secured, it is possible to give different access to different people. For instance, sales associates can have access to their sales databases, but are unable to access another sales associate's information or business information (e.g. accounts payable, accounts receivable). Creating a single storage location (or server) for the data, and assigning individuals with different access, keeping up with data is a breeze. It makes it easier to maintain the data, and permits a quick transfer to another storage location if needed. Data security software can also serve as a source to make secure sites (that give access to data files) can only be accessed by authorized personnel.[6]

1.9 Corporate Data Quality Management[7]:

[6] http://datasecuritymanagement.com/
[7] http://www.efqm.org/corporate-data-quality-management

This part describes the Framework for Corporate Data Quality Management (CDQM). It supports organizations in the assessment and analysis of remedies for missed opportunities and unexploited potentials of CDQM. It is based on the EFQM Excellence Model - which is used by over 30,000 organizations in the world - and gives organizations the opportunity to coordinate CDQM activities by applying an approach of demonstrated value. Furthermore, the Framework can be used in several ways:

- as a tool to benchmark with other organizations,
- as a guide to identify areas for improvement and raise awareness for corporate data quality,
- as a common vocabulary and way of thinking,
- and as a framework around which CDQM capabilities can be developed.

The Framework for CDQM addresses professionals in organization which deal with the management of and those individuals benefiting from good corporate data quality. The Business Perspective on Corporate Data Quality Organizations need to respond to a number of business drivers for which high-quality corporate data are a critical prerequisite.

- Risk management and compliance
- Integrated customer management
- Business process integration, automation and standardization
- Reporting
- IT consolidation

Content:

- **Purpose of the document**
- **The business perspective on Corporate Data Quality**
- **Basic concepts**

❖ Corporate Data Quality Management

- Corporate Data and Master Data
- Quality aspects of Corporate Data
- Management of Corporate Data Quality
  - EFQM Excellence Model

- RADAR

- **The EFQM Excellence Model and the Framework for Corporate Data Quality Management**
  - **The Framework for Corporate Data Quality Management**
  - **Enablers**
    - Strategy
    - Controlling
    - Organization & People
    - Processes & Methods
    - Data Architecture
    - Applications
    - Results
    - Customer Results
    - People Results
    - Society Results
    - Business Results
- **Implementing the Framework for Corporate Data Quality Management**
  - The Self-Assessment Process
  - Choosing the right Self-Assessment technique
  - **Further help**
    - EFQM resources
    - CDQM resources
    - Consortium CC CDQ
    - Tools

1.10 Security and Privacy- Data is the Key[8]:

[8] http://www.informatica.com/Images/02160_ema_data-privacy_ar_en-US.pdf

With the increased visibility of data security breaches, organizations and regulators alike have placed high emphasis on the protection of sensitive information. Today, assuring the due care of data has become a principal focus of information security and privacy management. The challenges, however, are more complex than many realize. Many may assume that applying techniques such as encryption to data at rest or in transit are foundational to securing sensitive information.

In fact, a more realistic foundation depends on addressing the problem of data exposure. Digital information can be readily duplicated, and is often widely shared. Organizations may or may not be aware of what – or where – their most sensitive information assets are, how they are used, and what happens to this information throughout its lifecycle. They may create redundant copies of data needlessly, increasing exposure simply to facilitate objectives such as application development or training. When protective measures are warranted, modern techniques provide a more flexible range of options, including those that address one of the most significant exposure gaps of all: the protection of information when in use. One such technique is data masking. When a data resource is accessed, masking obscures its more sensitive elements such as personally identifiable information while delivering useful data. It does this, not by over-writing data in the production database, but by replacing sensitive values with realistic (but not actual) substitutes when data is delivered to the consuming user or application.

• When developers build data-centric applications, they must assure complete functionality and resolve any operational issues. This may be difficult if not impossible unless applications can interact with actual data or the production environment. Filtering out sensitive data elements manually may be impractical. It may disrupt critical application dependencies such as data formats, or leave gaps that expose sensitive items. Late-stage integration testing without access to a production database may produce misleadingly incomplete results. Development and testing has thus been one of the more visible applications of data masking.

• The technique enables more transparent use of actual information – such as a body of population data used to analyze health or accident trends, for example – without exposing the personal information of individual subjects. Masking

algorithms are often designed to be repeatable, so that the referential integrity of masked data is preserved.

• More recently, the use of masking techniques in real time (as opposed to masking a static copy of a dataset) has increased the value of masking. Such "dynamic" masking techniques enable more direct interaction with production data – and not just for development and testing. The ability to selectively deliver data, or a subset of a body of data, can significantly increase the range and flexibility of applications relying on sensitive data stores. Inline dynamic masking can accomplish this without requiring modification of the target database or the relying application. It also reduces risk exposures by eliminating the need to create copies of data sources. Together, these capabilities reduce risks as well as costs.

In order to realize the maximum benefit, however, data masking – as well as any other protective technique – may be utilized best when it integrates with a strategic approach to information management.

Knowing:

- How and when data is created and modified;
- How data is used and integrated with applications or other data sources;
- The processes required to assure data integrity; and
- How data is ultimately preserved or retired

Enables organizations to understand how and where techniques such as masking may be applied most effectively. The combination of data discovery and masking with the automation of data sub setting, for example, can optimize data protection techniques in concert with data integration and information lifecycle management technologies. This assures the delivery of only the information required without interfering with critical data dependencies, when security and risk management is integrated with enterprise information management. The relevance of information to security efforts goes beyond protecting information itself, however. Increasingly, organizations are looking to today's data-driven technologies to improve accurate and timely insight into threats and base strategies on more objective assessment – and standing at a vital crossroads of such data-driven interests are the capabilities of data integration, rationalization and analysis that make technologies such as Complex Event Management more valuable to these efforts than ever before.

1.11 Summary:

Data security and management is a very important concept of E-security. In this unit the various important concept discussed at length for better understanding and application at appropriate place. Mainly the concept of data security, protecting sensitive data, browser sensitive data, data governance, internet explorer and network security, the role of window-Microsoft: help to protect your OC, data security management, corporate data quality management and security & privacy data in the key are discussed at length to understand the unit completely.

1.12 Some Useful Books:

1. Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
2. Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
3. Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
4. Cyber Terrorism by S. Venkatesh (Authorpress)
5. Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
6. Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
7. Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
8. Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
9. Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
10. Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
11. Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
12. Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)

13. Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
14. Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
15. The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
16. Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
17. Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
18. Computers, Privacy and Data Protection: An Element of Choice (Springer)
19. All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

1.13 Check your Progress:

A. Which of the following statements are true or false:

1. Computer security is an unsolvable problem.
2. Data security also protects data from corruption.
3. Back in Summer 2013 Google was criticized for storing user login information, user name and password in plaintext in the web browser without any sort of protection.
4. All data governance programs are not alike.
5. Data security management is a way to maintain the integrity of data.

B. **Fill in the Blanks:**

1. Data security is also known as ……or computer security.
2. Data governance refers to the overall management of the …….. of the data.
3. ……can help prevent hackers or malicious software (such as worms).
4. ……is one of the easier ways to help protect your computer from hackers.

5. …….can be readily duplicated, and is often widely shared.

1.14 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Information Security
2. Availability, usability, integrity, and security
3. A Firewall
4. A Password
5. Digital Information

1.15 Terminal Questions

1) What is data security?
2) Define protection of sensitive data.
3) Discuss in detail data governance and CDQM.
4) Is security and privacy data is the key to protect computer from hackers?
5) What is internet explorer and network security?

Unit-2

E-Governance

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to E-Governance
- Understand the importance of E-Governance in Good Governance and Development
- Understand the technical and legal issues related to E-Governance

Structure:

2.1. Introduction:

The rise of e-government has been one of the most striking developments of the web. As the Internet supported digital communities evolve, and assuming that

they do indeed grow to incorporate individuals around the country (and globe) , they present the national governments with a number of challenges and opportunities. Governments in democratic states are primarily a representative mechanism whereby the selected few debate and enact the legislation for and on behalf of the nation state's citizens. There are several aspects to this that might prove of importance in the context of e-governance. Firstly, those elected representatives need access to information and communication resources. It is necessary for them to inform and listen to their constituents; it is necessary for them to communicate with one another; and at the most basis, it is necessary for them to discover and represent the wishes of those who have elected them as their representatives. While we elect individuals, we appreciate and understand that they must then balance three sometimes opposing forces: their own conscience; the philosophy of their party; and the interest of their constituency itself. At the simplest level, the implementation of e-governance can then support this information and communication requirement. E-mail between politicians and between politicians and departments can be easily established. Since many state govts. Are providing Lap tops to their MPs and MLA's, they can publish their home pages on Internet, to act as constituency interaction center. This then touches on the next aspect, that of communicating with the constituents. In addition to the standard channels and mechanisms, the politicians can receive the email messages from those wishing to express their views. There are similarly endless ways to utilize Information and communication technologies (only limited by the imagination of the implementing agency) to provide efficient and transparent solutions to citizens.

2.2. History of E-Governance in India:

Among developing countries, India has been an early adopter of e-governance. The first wave can be considered to have evolved bottom-up. Some social entrepreneurs convinced district level officials of the wonders of new ICTs, especially in providing convergent services to remote areas, and improving transparency and oversight in this regard. The Gyandoot project in Dhar district, which begun in 2000, is considered the forerunner of what was to be a rash of projects that built a front-end in many village communities which was supposed to

be serviced by a back-end mostly in the district collect orate. The idea and the effort was to create pressure from the community front-end for digitization of back-end departmental processes. The latter was largely a localized effort, mostly dependent on the initiative and energy of the concerned district collector, often with some very spirited support of the district National Informatics Centre (NIC) staff. Perhaps the most organized and successful effort in this first phase of e-governance in India, roughly between 2000-05, was Rural e-Seva in West Godavari district of Andhra Pradesh. As for community level front end development two initiatives, N-logue and Drishti stand out, each of which at one time claimed to be running thousands of community telecasters across the country that could deliver e-governance services.

There is a generally tendency to classify these early efforts as failures. Indeed, around 2005-06, N-logue closed down and Drishti moved out of e-governance services. Rural e-Seva also was never scaled up. However, what is noteworthy is that in a relatively short time, these early projects created a lasting impression of new ICTs as a possible means to bring governance close to the people, and perhaps, also make it more transparent and accountable. To that extent, they had a very significant impact, even if these initiatives themselves could not survive, due to a variety of reasons which we cannot discuss in greater detail, here. (However, if we compare this situation with the burst of the dotcom bubble in the early part of the last decade, one can see some common factors.) They created the context for the very ambitious National E-Governance Plan (NEGP), especially its flagship project, the Common Service Centers, which was inaugurated by the Government of India in 2006.

Meanwhile, many independent department level digitization and automation projects were taking shape. Digitization of records of land ownership and transactions has been one of the key areas with considerable impact, since it a very important and vexatious area for rural India. In many cases, end to end digitization was facilitated by significant changes in government rules, which provide some early instances of full-scale e-governance process re-engineering. Some other automation activities like computerization of government treasuries and financial transactions also have had considerable impact on the efficiency of governmental

functioning, and represent largely successful and sustaining e-governance efforts. From very early days, efforts were also make to computerize work flow in government offices, like e-Secretariat initiatives in a few states. However, such initiatives failed to sustain because they seemed to conflict with formal and informal ways of functioning of the Indian bureaucracy. Any progress on such basic areas of governmental activity requiring significant behavioral changes, and also having very significant implications for greater transparency and accountability, would require strong legislative push[9].

2.3. Origin of E-Governance in India (National Informatics Center):

National Informatics Centre (NIC) was established in 1976, and has since emerged as a "prime builder" of e-Government / e-Governance applications up to the grassroots level as well as a promoter of digital opportunities for sustainable development. NIC, through its ICT Network, "NICNET", has institutional linkages with all the Ministries /Departments of the Central Government, 35 State Governments/ Union Territories, and about 625 District administrations of India. NIC has been instrumental in steering e-Government/e-Governance applications in government ministries/departments at the Centre, States, Districts and Blocks, facilitating improvement in government services, wider transparency, promoting decentralized planning and management, resulting in better efficiency and accountability to the people of India.

"Informatics-led-development" programme of the government has been spearheaded by NIC to derive competitive advantage by implementing ICT applications in social & public administration. The following major activities are being undertaken:

- Setting up of ICT Infrastructure
- Implementation of National and State Level e-Governance Projects
- Products and Services
- Consultancy to the government departments

[9] http://www.itforchange.net/E-governance_in_India%3A_Existing_context_and_possible_scope_for_UNDP_programing_over_2013-18

- Research and Development
- Capacity Building

  During the last three decades, NIC has implemented many "network centric" application software for Programme implementation in various ministries and departments, using state-of-the-technology software tools. During 1980s and early part of 1990s, the policy thrust was on creating "Management Information System (MIS)" and "Decision Support System (DSS)" for development , planning and responsive administration in governments which led to the genesis of present day "e-Governance" / "e-Government". "Bridging the Digital Divide", "Social and Financial Inclusion through ICT" and "Reaching- the-Unreached" concepts were tried and made operational in the late nineties. NIC has vast expertise and experience in the design, development and operationalization of various e-Government projects in the areas of Public Administration and Governance like Agriculture & Food, Animal Husbandry, Fisheries, Forestry & Environment, Industry, Health, Education, Budget and Treasury, Fiscal Resources, Transport, Water Resources, Court Management, Rural Development, Land Records and Property registration, Culture & Tourism, Import & Exports facilitation, Social Welfare Services, Micro-level Planning, etc. With increasing awareness leading to demand and availability of ICT infrastructure with better capacities and programme framework, the governance space in the country witnessed a new round of projects and products, covering the entire spectrum of e-Governance including G2C, G2B, G2G, with emphasis on service delivery.

NIC provides Nationwide Common ICT Infrastructure to support e-Governance services to the citizen, Products and Solutions designed to address e-Governance Initiatives, Major e-Governance Projects, State/UT Informatics Support and district level services rendered.

NIC has set up state-of-the-art ICT infrastructure consisting of National and state Data Centers to manage the information systems and websites of Central Ministries/Departments, Disaster Recovery Centers, Network Operations facility to manage heterogeneous networks spread across Bhawan, States and Districts, Certifying Authority, Video-Conferencing and capacity building across the

country. National Knowledge Network (NKN) has been set up to connect institutions/organizations carrying out research and development, Higher Education and Governance with speed of the order of multi Gigabits per second. Further, State Government secretariats are connected to the Central Government by very high speed links on Optical Fiber Cable (OFC). Districts are connected to respective State capitals through leased lines.

Various initiatives like Government Procurement System(Geoponic), Office Management Software (Office), Hospital Management System (hospital), Government Financial Accounting Information System (Lekha), etc. have been taken up which are replicable in various Government organizations.

As NIC is supporting a majority of the mission mode e-Governance projects, the chapter on National e-Governance Projects lists the of details of these projects namely National Land Records Modernization Programme (NLRMP), Transport and National Registry, Treasury Computerization, VAT, MG-NREGA, India-Portal, e-Courts, Postal Life Insurance, etc. NIC also lays framework and designs systems for online monitoring of almost all central government schemes like Integrated Watershed Management (IWMP), IAY, SGSY, NSAP, BRGF, Schedule Tribes and other Traditional Forest Dwellers Act etc.

ICT support is also being provided in the States / UTs by NIC. Citizen centric services are also being rendered electronically at the district level, such as Income Certificate, Caste Certificate, and Residence Certificate etc. along with other services like Scholarship portals, permits, passes, licenses to name a few.
In executing all these activities, NIC has been given recognition in terms of awards and accolades in International as well as National levels, which are listed in the Awards Section.

Thus, NIC, a small program started by the external stimulus of an UNDP project, in the early 1970s, became fully functional in 1977 and since then has grown with tremendous momentum to become one of India's major S&T; organizations promoting informatics led development. This has helped to usher in the required transformation in government to ably meet the challenges of the new millennium.

2.4. National E-Governance Plan:

The second phase of e-governance in India can be said to have begun with inauguration of the National E-Governance Plan (NeGP) in 2006. NeGP's flagship project sought to set up about 100,000 Common Service Centers (CSCs) across India, one for every six villages. Recently, the Department of IT declared that they have achieved this target. NEGP also consists of 27 Mission Mode projects, largely for back-end computerization of different areas of governance activity. In addition, it seeks creation of a national e-governance infrastructure of State Wide Area Networks, State Data Centers, and National Service Delivery Gateways.

The infrastructural and technical support projects have mostly been working well. NEGP has been able to provide a common sense of urgency, mechanism and some funding support for large-scale adoption of e-governance by various departments of the central and state governments. Such a catalytic action, and perhaps creating a environment for competitive performance, was very much needed in the initial phase. It has been especially useful for states that are otherwise slow on the take, viz a viz e-governance, and they may also be the ones that most need governance reform. Department of IT gives technical support to e-governance initiatives of various departments at the central and state levels, including through listed consultants. They also ensure some degree of common architecture which is very important for interoperability, especially required when, at a later stage, across-the-government integration of operations and services may be sought.

One however notes that projects that focus on targeting the better-off sections, e.g. those related to passports and income tax, have produced the best results to date. On the other hand, Mission Mode Projects in areas like agriculture and panchayat computerization, that most directly concern relatively marginalized sections, have been the slowest to take off. This may requires an re-assessment of NEGP with regard to considerations of inclusion, equity and social justice.

Although there have been a few hiccups, the Unique ID project, listed as a Mission Mode Project under NEGP, is also well underway. Recently, Department of IT has come up with a 'Framework for Mobile Governance' which lays out the vision and strategy for mobile governance. It envisions setting up a Mobile Service

Delivery Gateway, Mobile App Store for governance applications, mobile authentication and payment gateway, and APIs[3] for different service providers. Department of IT has also notified a 'Policy on Open Standards for E-governance', and the work of notifications of open standards in various areas is underway. Last year, guidelines for use of social media by government agencies were issued by the Department of IT. Internal and stakeholder consultations on the opportunity and challenges for e-governance in a cloud computing environment are also underway.

NEGP has done very well in providing infrastructural and technical support for widespread adoption of e-governance in India. However, there seems to be a significant gap on the non-technical side, viz a viz governance process re-engineering[4] architectures and the broad socio-political principles that need to be addressed though and in e-governance. It is to a good extent due to the NEGP that large-scale digitization is taking place in most departments in the central and state governments. As the process of digitization and automation (the early stage of e-governance) has proceeded at a steady pace across government agencies, it has produced substantial efficiency gains and some improvements on the transparency front. If greater gains in the area of transparency, accountability and community participation have not been attained, it is largely because e-governance in India has still mostly been conceived and implemented in a techno-managerial mode and without sufficient socio-political vision.

It may come as a surprise to many that for an area that not only involves funds to the extent of thousands of cores of rupees and also is so crucial to the future of governance in India, there has never been any dedicated e-governance policy in India. One would expect to have some kind of a detailed policy document based on due consultations with all stakeholders, which provides the vision for e-governance in India, integrating governance reform priorities like decentralization, right to information, and improved community participation and monitoring. However, an examination of e-governance activities and trends in India bears testimony to the fact that e-governance in India seems to have proceeded largely on its own logic, or the absence of one. The dominant understanding seems to be that IT merely makes whatever is being done much more efficient, and therefore it may not be necessary to get into basic issues of examining an initio 'what indeed is being done', 'what was supposed to be done', and 'how things can perhaps now be done very differently'. It is to be left to those running the respective systems to

decide what they may want to do with various IT tools and opportunities. The NEGP seems merely to be there to provide technical support; this stance being often articulated by the concerned officials.

This had led to a situation whereby departments have mostly used an internal logic and considerations of internal 'interests' and objectives rather than primarily employ an external logic, of (1) the point of view of basic objectives of governance, and the specific role of their department in it, (2) need and possibility of government-wide responses to governance needs, and, mostly importantly, (3) needs and perspectives of the citizens. Mature models of e-governance worldwide proceeds from such higher level strategic considerations, before the nuts and bolts of actual departmental and offices level changes are worked out.

Such a techno-managerial approach has meant that e-governance in India has made no clear linkages with other areas of governance reform like decentralization, right to information and community monitoring, while the fact is that process re-engineering through e-governance should primarily have been serving these substantive objectives of governance reform in India. This anomaly needs to be corrected through a national e-governance policy that casts e-governance within larger socio-political objectives and then proceeds to establishing such principles that should guide systemic process re-engineering through e-governance. These principles arise out of the generic techno-social possibilities made available by the digital or information society. Such principles should be able to account for and admit rapid technology changes, and further new opportunities opened by ICTs.

Decentralization, right to information and community monitoring, as other three key areas of governance reform in India apart from e-governance, all aim at greater bottom-up participation, and accountability. They all did, however, require, and continue to require, strong central legislation and policy support. In fact, they could not have been attained without such push and support from the top, with a clearly articulated political vision and the directions. E-governance has to become more than merely applying technology to existing processes, and should be seen in its transformatory potential. For this, it must also be versioned and articulated in terms of the highest socio-political objectives of governance reform in India. These objectives then have to be translated into higher-level principles for process

architecture of e-governance, which are sufficiently generic and flexible to be applicable to a range of governance activities and systems.

However, it is true that e-governance in India was established in an environment where new ICTs were taking the world by storm, and no one could easily prejudge what could be attained by employing ICTs in governance, and how. It was therefore required to go through a period of intense experimentation. It is a tribute to the early leaders of e-governance in India that they did not shy away from this imperative of investing into what were mostly time and resource-intensive experiments. However, it may be time now to consolidate our learning and begin to take a more strategic and systemic view of governance reforms in India. A clear vision and policy for this purpose may be a prerequisite. Such a policy should also assign relevant role to government agencies and departments who shall provide technical lead and support, those that will provide governance reform vision, and generic process principles and guidelines (like the Departments of Administrative Reforms whose role in e-governance efforts should be central, but has been rather muted till date) and the departments that actually undertake e-governance activities in their respective areas of competence and work. It will also align e-governance with overall thrusts of governance reform in India – chiefly, decentralization, right to information, and community monitoring and social audits, whose objectives e-governance should primarily be serving. We need to move from procedural e-governance – which merely automates and digitizes existing processes providing efficient gains, something that is almost a natural process in all organizations worldwide, to transform e-governance that has its point of departure in specifically seeking to address the various governance challenges and reform processes in India.

A promising recent policy initiative is the Electronic Services Delivery (EDS) Bill which is with the Parliament at present. This proposed legislation makes it compulsory for all government agencies to begin delivering their services in an electronic mode. All services that can be provided electronically must be so provided. There is a provision for independent EDS Commissions at the central and state level that will monitor provision of electronic delivery of services.

This legislation is expected to put great pressure on various government agencies to quickly take on e-governance, and therefore is quite a positive move.

However, the proposed Bill just further pushes agencies towards e-governance without telling them how to do it, and with what core objectives in mind. Will the need to comply with legislative requirements, for example, make departments inclined to quickly go for cash transfers that are much easier to do over ICT based outreach infrastructure, even when run by outside agencies on a commercial basis, even when a particular service may not be most suited to a cash transfer mode? Such a welcome push for quicker e-governance uptake, as the EDS legislation is expected to provide, makes it even more important to articulate an overall e-governance policy in India, which makes a detailed socio-political examination of new possibilities in light of the specific needs and current thrusts of governance reform in India.[10]

2.5. Central Government Initiatives:

In India, the main thrust for e-Governance was provided by the launching of NICNET in 1987 – the national satellite-based computer network. This was followed by the launch of the District Information System of the National Informatics Centre (DISNIC) programme to computerize all district offices in the country for which free hardware and software was offered to the State Governments. NICNET was extended via the State capitals to all district headquarters by 1990. In the ensuing years, with ongoing computerization, Tele connectivity and internet connectivity established a large number of e-Governance initiatives, both at the Union and State levels.

The formulation of National e-Governance Plan (NEGP) by the Department of Electronics and Information Technology (DEITY) and Department of Administrative Reforms and Public Grievances (DAR&PG) in 2006 has boosted the e-Governance process.

The Central initiatives include:

- National e-Governance Plan (NEGP)
- National e-Governance Division (NEGD)
- e-Governance Infrastructure
- Mission Mode Projects

[10] http://www.itforchange.net/E-governance_in_India%3A_Existing_context_and_possible_scope_for_UNDP_programing_over_2013-18

- Citizens Services
- Business Services
- Government Services
- Projects and Initiatives
- R&D in e-Governance
- Model RFPs for e-Governance Project

2.6. State Government Initiatives:

Several State Governments have taken various innovative steps to promote e-Governance and have drawn up a roadmap for IT implementation and delivery of services to the citizens online. The applications that have been implemented are targeted towards providing Government to Citizen (G2C), Government to Business (G2B) and Government to Government (G2G) services with emphasis on use of local language.

Every State has the flexibility of identifying up to five additional State-specific Mission Mode Projects (relevant for economic development within the State). In cases where Central Assistance is required, such inclusions are considered on the advice of the concerned Line Ministries/ Departments. States have MMPs on Agriculture, Commercial Taxes, e−District, Employment Exchange, Land Records, Municipalities, Gram Panchayats, Police, Road Transport,Treasuries,etc.

Apart from MMPs the States have other e-Governance initiatives.

State/Union Territory	**Initiatives covering departmental automation, user charge collection, delivery of policy/programme information and delivery of entitlements**
Andhra Pradesh	e-Seva, CARD, VOICE, MPHS, FAST, e-Cops, AP online—One-stop-shop on the Internet, Saukaryam, Online Transaction processing
Bihar	Sales Tax Administration Management Information
Chhattisgarh	Chhattisgarh InfoTech Promotion Society, Treasury office, e-linking project

Delhi	Automatic Vehicle Tracking System, Computerization of website of RCS office, Electronic Clearance System, Management Information System for Education etc
Goa	Dharani Project
Gujarat	**Mahiti** Shakti, request for Government documents online, Form book online, G R book online, census online, tender notice.
Haryana	Nai Disha
Himachal Pradesh	Lok Mitra
Karnataka	Bhoomi, Khajane, Kaveri
Kerala	e-Srinkhala, RDNet, Fast, Reliable, Instant, Efficient Network for the Disbursement of Services (FRIENDS)
Madhya Pradesh	Gyandoot, Gram Sam park, Smart Card in Transport Department, Computerization MP State Agricultural Marketing Board (Mandi Board) etc
Maharashtra	SETU, Online Complaint Management System—Mumbai
Rajasthan	Jan Mitra, Raj SWIFT, Lokmitra, RajNIDHI
Tamil Nadu	Rasi Maiyams–Kanchipuram; Application forms related to public utility, tender notices and display
North-Eastern States	
Arunachal Pradesh,	Community Information Center. Forms available on
Manipur, Meghalaya,	the Meghalaya website under schemes related to
Mizoram & Nagaland	social welfare, food civil supplies and consumer affairs, housing transport etc.

Source: PC Quest Article

2.7. E-Governance Projects in India:

E-governance in Andhra Pradesh: This section of the website of Andhra Pradesh showcases the various E-Governance initiatives and applications being implemented in the state.

E-Governance in Ministries/Departments and State Governments The website of the Ministry of Information Technology (MIT), Govt. of India lists briefly the E-Governance Initiatives undertaken by the various Ministries/Departments and States Governments.

Gyandoot: Gyandoot is an intranet in Dhar district of Madhya Pradesh, connecting rural cybercafés catering to the everyday needs of the masses. The web site is an extension of Gyandoot intranet, for giving global access. The site has these services to offer: Commodity/ Mandi Marketing Information System; Copies of khasra, B1/khatauni and maps; On-line registration of applications; Income Certificate; Domicile Certificate (mool niwasi) ; Caste Certificate; Landholder's passbook of land rights and loans (Bhoo adhikar evam rin pustika).
Warana: The primary objective of the recently launched Wired Village project is to demonstrate the effective use of IT infrastructure in the accelerated socio-economic development of 70 villages around Warana Nagar in the Kolhapur and Sangli districts of the state of Maharashtra. The existing cooperative structure has been used in concert with high speed VSATs to allow Internet access to existing cooperative societies. The project aims to provide agricultural, medical, and education information to villagers by establishing networked facilitation booths' in the villages.
E-Governance in Noida city: Compaq India has joined hands with Electronics Research and Development Centre of India (ERDCI), Noida, to set up a competence centre that would enable e-governance in Noida city and various other states. Residents will be able to pay electricity and phone bills, file I-T returns, register marriages and deaths, among other things at information kiosks located in the city. Once the project becomes fully operational citizens can pay utilities, get grievance redressal and a variety of other essential jobs through these info kiosks.

"RajNidhi": Information kiosks : "RajNidhi" is a web enabled information kiosk system developed jointly by Rajasthan state's Department of Information Technology and Rajasthan State Agency for Computer Services (RajComp).

Earlier on March 23, 2000, Nayla became the first village of Rajasthan to have a "Raj Nidhi Information Kiosk" when the US President, Mr. Bill Clinton visited this village to observe the functioning of a Gram Panchayat.

"raj-SWIFT": Rajasthan government's Intranet: The Rajasthan States Department of Information Technology (DoIT) has developed Government own Intranet called as "raj-SWIFT". SWIFT here stands for Statewide Intranet on Fast Track. This system which has been built using Internet technology and tools would facilitate online data, text and e-mail communication between the office of the Chief Minister and all the 32 District Collectors on one-to-one basis, thus bringing the Chief Executive of the State and the district administration close enough to be just a mouse click away.

Mechanism of Single Window Clearance System: To overcome the inordinately long time required to obtain the statutory approvals/licences etc. from various government departments/agencies, the Bureau of Industrial Promotion & Office of the Commissioner (Investment & NRIs), Government of Rajasthan, has introduced a Single Window Clearance System through a Single Composite Application Form.

E-Governance in Panchayats in Kerala: The website of the department of Administrative Reforms and Public Grievances, Ministry of Personnel, Public Grievances and Pensions features an article on the e-governance initiatives adopted by the Panchayats in Kerala.

E-Governance in Himanchal Pradesh: Himanchal Pradesh to focus on IT-enabled services & e-governance, which would include medical transcription, call centers, data processing, back office operations and GIS.

Package for Effective Administration of Registration Laws Project in Kerala: THE Government of Kerala has launched a project titled PEARL (Package for Effective Administration of Registration Laws) for computerization of the Registration Department in the State.

E-Governance Centre at Haryana Secretariat: The Haryana Government has set up an e-governance centre at the Secretariat to effectively monitor information technology in the state.

National Knowledge Network: The NKN is a state-of-the-art multi-gigabit pan-India network for providing a unified high speed network backbone for all

knowledge related institutions in the country. The purpose of such a knowledge network goes to the very core of the country's quest for building quality institutions with requisite research facilities and creating a pool of highly trained professionals. The NKN will enable scientists, researchers and students from different backgrounds and diverse geographies to work closely for advancing human development in critical and emerging areas.

Features:

NKN is designed as a Smart Ultra High Bandwidth network that seamlessly interconnects the leading Scientific and Technological institutions - which are pursuing world-class research and development. NKN design is inherently proactive; it takes into account the requirements that may occur in the near term and long term.

Some of the salient features of the NKN are:

- Establishing Connectivity for Knowledge and information sharing.
- Enabling Collaborative Research in emerging areas such as Climate Modeling.
- Facilitating distance education in specialized fields such as medicine, emerging high tech areas covering info-bio-nano technology.
- Facilitating an ultra-high speed e-governance backbone for information sharing.

NKN will also act as a test bed for research in the area of network, security and delivery models for various services. As NKN is a new initiative, it will leverage existing initiatives, to ensure faster roll out with modest investment.

Services:

NKN network is designed with the aim of providing:

- Highest level of availability
- Robust & reliable connectivity
- Highest level of Scalability (specifically planned to match the unknown future demands which cannot be envisaged currently)
- Best Bandwidth Capacity: For NKN, various National Long Distance Carriers (NLDs) have provided 1Gbps / 2.5Gbps capacity links which can be self-healed. Further, the NLDs are in process of upgrading (using DWDM) to 10Gbps or more connectivity.

The main services of NKN can be broadly categorized under the following heads:

• Generic Services: Internet, Intranet, Network Management Views, e-Mail, Messaging Gateways, Caching Gateways, Domain Name System, Web Hosting, Voice over IP, Multipoint Control Unit (MCU) Services, Video Portals, SMS Gateway, Co-Location Services, Video Streaming etc.

• Community Services: Shared Storage, e-Mail List Software Application (LISTSERV), Authentication Service, EVO, Session Initiation Protocol (SIP), Collaboration Service, Content Delivery Service, International Collaborations with EU-India Grid, Global Ring Network for Advanced Applications Development (GLORIAD)etc.

• Special Services: Virtual Private Network Stitching Services

2.8. E-Governance Standards:

To ensure Interoperability among e-Governance applications, Government of India has setup an institutional mechanism for formulation of Standards through collaborative efforts of stakeholders from DIT, NIC, STQC, other Government Departments, Industry, Academia and Public. Various Working groups and Expert committees have been created for this purpose. NIC is playing a key role in coordination and steering the standards formulation process and also technical participation in preparation of Approach papers, standards formulation, drafts review process and POC.

Policy on Open Standards, Metadata and Data standard for Person Identification & Land Region Codification, Biometric Data Standards for Fingerprint and Face Images, Interoperability Guidelines for Digital Signature Certificates, Guidelines for usage of Digital Signature, Indian Languages Encoding and Font standards, Quality Assurance Framework, Conformity Assessment Requirements document, Information Security Framework and Guidelines have been already published on the portal (http://egovstandards.gov.in). Standards for e-Forms design, Interoperability Framework for e-Governance in India, Technical standards in Interoperability areas are in the advanced stage of preparation.

Notified Standards:-

Biometrics Standards:

Face Image Data Standards Ver1.0

Fingerprint Image Data Standard Ver1.0

Iris Image Data Standard Ver1.0

Conformity Assessment Requirement (CARE)

Conformity Assessment Requirements for e-Governance Applications Ver.1.0

Presentation on Overview of CARE Document Ver.1.0

Digital Preservation Standard:

E-Governance Standards for Preservation Information Documentation of e-Records Ver1.0 (Metadata & Schema)

E-Governance Standards for Preservation Information Documentation of e-Records Ver1.0 (XSD)

Localization & Language Technology Standard:

Character Encoding: Standard Ver1.0

Fonts: Standard Ver.1.0

Metadata and Data Standards:

MDDS Demographic Ver. 1.1

Quality Assurance Framework:

Presentation Overview of QAF Document Ver.1.0

QualityAssuranceFramework Ver.1.0

Technical Standards for IFEG:

Technical Standards for IFEG Ver1.0

Guidelines:

Digital Signature:

Digital Signature Certificate Interoperability Ver2.0

Usage of Digital Signature in e-Governance Ver1.0

Digital Preservation:

Best Practices and Guidelines for Production of Perceivable e-Records Ver1.0

Indian Government Websites:

GOI Web Guidelines

Information Security:

ESAFE-GD210-ImplementationGuidelines ver1.0

ESAFE-GD220-AssessmentGuidelines ver1.0
ESAFE An overview
ESAFE Framework Approach Paper Ver1.0
ESAFE GD100 IS Guidelines for Security Categorization of Information System Ver1.0
ESAFE GD200 Catalog Of Security Controls Ver1.0
ESAFE GD201 Baseline Security Controls Low Impact Information System Ver1.0
ESAFE GD202 Baseline Security Controls Medium Impact Information System Ver1.0
ESAFE GD203 Baseline Security Controls High Impact Information System Ver1.0
ESAFE GD300 Guidelines for Information Security Risk Assessment and mgmt Ver1.0
Localization of e-Governance Applications in Indian Languages:
Best Practices for Localization of e-Governance Applications in Indian Languages Ver5.7
E-Procurement Guidelines:
Compliance to Quality Requirements of e-Procurement Systems
Mobile Governance:
Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices
Best Practices for Localization of Mobile Web Applications in Indian Languages

2.9. Web-Services:

NIC is extending comprehensive World Wide Web services(http://webservices.nic.in) to Central and State Governments, Ministries & Departments in the areas of consultancy, web design and development, web hosting, value added web services for promotion of websites, enhancement of websites & training. Hosting infrastructure is being provided to a large number of e-governance projects like CGHS, Panchayats Portal, Government accounting, Exam Results Portal, Online Counseling to Admission to various professional courses across the country.

NIC's wide range of hosting services starts right from Shared Hosting and Dedicated Servers to Co-located Servers and Managed Hosting. Hosting solutions are available on a variety of platforms such as Linux, Windows and Solaris etc. NIC also supports state-of-the-art web technologies and a variety of databases on the servers. The hosting infrastructure includes a large number of powerful performances tuned and secure servers. Load balancing and clustering solutions are used to effectively manage the heavy traffic on the websites during peak-hours and to ensure a high degree of availability. A site brought to NIC for hosting can be up on the server in less than an hour's time. Developing a successful presence on the web takes a combination of quality content, dynamic programming, powerful graphics and very importantly, a carefully planned promotion strategy. NIC helps in fine-tuning the site in such a way that it gets a high ranking in various search engines. Sites are also promoted through NIC's own portals such as "India Image" and "GOI-Directory" which attracts a large number of visitor's everyday from all across the globe.

- URL:
  http://webservices.nic.in
- *Contact Details*

Data Centre and Web services Division National Informatics Centre A-Block, CGO Complex Lodhi Road, New Delhi-110003, Email:-nic-web support [at]lsmgr[dot]nic[dot]in.Phone:011-2430536

2.10 Summary:

E-governance is a very important feature of government. In the present unit the concept of history of e-governance in India, origin of e-governance in India through National Informatics Center, National E-Governance plan, Central Government initiatives, State Government initiatives, various important e-governance projects in India, National Knowledge Network, e-governance network and e-services are discussed at length for understanding with the help of various related examples and initiatives of the government to strengthen this sector in the interest of citizens.

2.10. Some Useful Book:

20. Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
21. Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
22. Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
23. Cyber Terrorism by S. Venkatesh (Authorpress)
24. Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
25. Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
26. Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
27. Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
28. Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
29. Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
30. Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
31. Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
32. Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
33. Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
34. The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
35. Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
36. Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
37. Computers, Privacy and Data Protection: An Element of Choice (Springer)
38. All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

2.11. Check your Progress:

A. Which of the following statements are true or false?

1. The rise of e-governance has been one of the most striking developments of the web.
2. Digitization of records of land ownership and transactions has been one of the key areas with considerable impact.
3. NIC provides nationwide common ICT infrastructure to support e-governance services to the citizen.
4. The National Knowledge Network is a state of art multi gigabit pan India network for providing a unified high speed network.
5. A site brought to NIC for hosting can be up on the server in less than an hour's time.

B. Fill in the Blanks:

1. Among developing countries, …… has been early adapter of e-governance.
2. National Informatics Center (NIC) was established in……
3. A promising recent policy initiative in the ……..Bill which is with the Parliament at present.
4. DISNIC means…….
5. NIC is extending comprehensive ……to Central and State Governments.

2.12. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. India
2. 1976

3. Electronic Service Delivery (EDS)
4. District Information System of the National Informatics Center
5. World Wide Web Services

2.13. Terminal Questions:

a. What is the history of e-governance in India?

b. What is National E-governance Plan?

c. Discuss in detail Central and State Governments initiative with reference to e-governance.

d. Write a note on National Knowledge Network.

e. Write a note on E-Governance Standards and E-Services.

Unit-3

Net Neutrality

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Net Neutrality
- Understand the international dimensions of Net Neutrality
- Understand the technical and legal issues related to Net Neutrality

Structure:

3.1. Introduction:

Net neutrality (also network neutrality, Internet neutrality or net equality) is the principle that Internet service providers and governments should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, or mode of communication. The term was coined by Columbia University media

law professor Tim Wu in 2003 as an extension of the longstanding concept of a common carrier.

There has been extensive debate about whether net neutrality should be required by law, particularly in the United States. Debate over the issue of net neutrality predates the coining of the term. Advocates of net neutrality such as Lawrence Lessig have raised concerns about the ability of broadband providers to use their last mile infrastructure to block Internet applications and content (e.g. websites, services, and protocols), and even to block out competitors.

Neutrality proponents claim that telecom companies seek to impose a tiered service model in order to control the pipeline and thereby remove competition, create artificial scarcity, and oblige subscribers to buy their otherwise uncompetitive services. Many believe net neutrality to be primarily important as a preservation of current freedoms. Prominent supporters of net neutrality include Vinton Cerf, co-inventor of the Internet Protocol, and Tim Berners-Lee, creator of the Web.

Examples of net neutrality violations include when the internet service provider, Comcast, intentionally slowed peer-to-peer communications. In 2007, one other company was using deep packet inspection to discriminate against peer-to-peer, file transfer protocol, and online games, instituting a cell-phone style billing system of overages, free-to-telecom value added services, and bundling. Critics of net neutrality argue that data discrimination is desirable for reasons like guaranteeing quality of service. Bob Kahn, co-inventor of the Internet Protocol, called the term net neutrality a slogan and opposes establishing it, but he admits that he is against the fragmentation of the net whenever this becomes excluding to other participants.

3.2. Net Neutrality: Meaning and Scope:

Net neutrality is an idea derived from how telephone lines have worked since the beginning of the 20th century. In case of a telephone line, you can dial any number and connect to it. It does not matter if you are calling from operator A to operator B. It doesn't matter if you are calling a restaurant or a drug dealer. The operators neither block the access to a number nor deliberately delay connection to a particular number, unless forced by the law. Most of the countries have rules that

ask telecom operators to provide an unfiltered and unrestricted phone service. When the internet started to take off in 1980s and 1990s, there were no specific rules that asked that internet service providers (ISPs) should follow the same principle. But, mostly because telecom operators were also ISPs, they adhered to the same principle. This principle is known as net neutrality. An ISP does not control the traffic that passes its servers. When a web user connects to a website or web service, he or she gets the same speed. Data rate for YouTube videos and Face book photos is theoretically same. Users can access any legal website or web service without any interference from an ISP.[11]

Network Neutrality (or "net" neutrality) is the concept of online non-discrimination. It is the principle that consumers/citizens should be free to get access to - or to provide - the Internet content and services they wish, and that consumer access should not be regulated based on the nature or source of that content or service. Information providers - which may be websites, online services, etc., and who may be affiliated with traditional commercial enterprises but who also may be individual citizens, libraries, schools, or nonprofit entities - should have essentially the same quality of access to distribute their offerings. "Pipe" owners (carriers) should not be allowed to charge some information providers more money for the same pipes, or establish exclusive deals that relegate everyone else (including small noncommercial or startup entities) to an Internet "slow lane." This principle should hold true even when a broadband provider is providing Internet carriage to a competitor. Net neutrality was a founding principle of the Internet. It is a principle incorporates both the “common carrier” laws that have long governed the phone lines used for both voice telephony and dial up access. Now, many consumers receive broadband service over other technologies (cable, DSL) that are not subject to the same common-carriage requirements. While these technologies are unquestionably superior to dial-up, the lack of enforceable net neutrality principles concerns us. Cable and DSL companies are planning to engage in “bit discrimination” by providing faster connections to websites and services that pay a premium, or by preferring their own business partners when delivering content. As the Internet moves forward, is it really wise to leave net neutrality behind?

[11] http://timesofindia.indiatimes.com/

3.3. Arguments for Net Neutrality:

Proponents of net neutrality are divided, however, on the question of whether or not the Internet is a public good and whether or not access to the Internet should be a fundamental right. One of the central arguments in favour of making Internet access a fundamental right is that it provides a crucial platform to other rights such as freedom of speech, freedom of the press and freedom of assembly. This is particularly relevant given the ubiquity of the Internet in all aspects of modern life and across platforms. The Internet has been compared to the electric grid to emphasize its importance to innovation and progress in the 21st century, with the suggestion that if the electric grid had not been neutral, many would have been priced out of science and invention.

Any attempt to bring the Internet under tighter government regulation can be presented as governmental overreach, particularly if the legislation was written for older technology. The question of how to classify broadband - as an information service, a telecommunications service, a cable service, or a public utility - has plagued the net neutrality debate. The idea of government control of the Internet is particularly sensitive given recent controversies surrounding intelligence-gathering. The matter is further complicated because the Internet itself has no owner, but the various hardware and software components of the Internet do are owned by different parties with certain intellectual property rights. Free enterprise is another principle to contend with. Internet service providers (ISPs) have paid to develop and maintain the infrastructure that provides the Internet, and bandwidth is costly. ISPs argue that they should be able to recoup those costs by charging those who use more. Some data types - a prominent example being video streaming services - consume much more bandwidth than others, and as such ISPs have to cover those costs; their options are to charge consumers more or to charge content providers for transmitting the data.

One problem with this argument, particularly in developing countries, is that many ISPs also have other business interests, and the potential for conflict and censorship arises. If an ISP also provides international calling services, then it makes sense for the ISP to discourage the use of Skype; if they provide video broadcast services, why promote online streaming? Especially in developing countries, where content is increasingly provided online rather than through

'traditional' media, there is a risk of content being controlled by the gatekeepers of the Internet. A lot of Internet usage in developing and emerging markets takes place on phones. This has led carriers to team up with content providers to create limited-access internet plans, so-called 'walled gardens'. Google Free Zone and Face book Zero are two such examples, whereby customers of participating networks can use limited Google or Face book services for free. These plans may be offered as a way to entice customers to use more data, and by doing so move to a more expensive plan. It is a costly gamble for the network provider, as Face book at least is not covering the cost of the free data, meaning the network provider must do so. However, network providers need these content services, because they are increasingly what attract customers rather than traditional voice and text plans. India currently has no law on net neutrality, and the Telecom Regulatory Authority of India, while supporting non-discrimination in principle, does not currently enforce it. While in general Indian ISPs adhere to the net neutrality principle, there have been instances of certain types of traffic being slowed down by Indian ISPs, without the knowledge of customers. The TRAI had noted the importance of net neutrality and the risks of ISPs controlling content in a 2006 consultation paper. Vodafone India, Airtel, Aircel and other providers have indicated a desire for revenue-sharing agreements with content providers like YouTube and Face book, a view also shared by the Cellular Operators Association of India (COAI).

The Supreme Court of India held in LIC v Manubhai D Shah that Article 19(1)(a) - the right to freedom of speech and expression - requires an inclusive public environment, following the argument that constitutionally guaranteed free speech is of little use if it is limited by private parties. If influential parties can squeeze smaller competitors into slower Internet lanes, they gain the ability to silence debate and control views undemocratically. Analysts have suggested that protecting freedom of speech is one of the best arguments for net neutrality in India. With India seeking to connect the next billion, and becoming a key player in the global Internet debate, it is important to have clearly formed domestic policies. The combination of regulatory interest, corporate opposition and constitutional rights suggest that the time is right for a nuanced debate on net

neutrality in India, with eventual regulation balancing the needs of providers and consumers who are both increasingly reliant on the Internet.[12]

The American Library Association is a strong advocate for intellectual freedom, which is the "right of all peoples to seek and receive information from all points of view without restriction." Intellectual freedom is critical to our democracy, because we rely on people's ability to inform them. The Internet connects people of diverse geographical, political, or ideological origins, greatly enhancing everyone's ability to share and to inform both themselves and others. Libraries' longstanding commitment to freedom of expression in the realm of content is well-known; in the context of the net neutrality debate, however, we believe it is equally important to stress that the freedom of libraries and librarians to provide innovative new kinds of information services will be central to the growth and development of our democratic culture. A world in which librarians and other noncommercial enterprises are of necessity limited to the Internet's "slow lanes" while high-definition movies can obtain preferential treatment seems to us to be overlooking a central priority for a democratic society – the necessity of enabling educators, librarians, and, in fact, all citizens to inform themselves and each other just as much as the major commercial and media interests can inform them. The ability of the Internet to spread and share ideas is only getting better. With modern technology, individuals and small groups can produce rich audio and video resources that used to be the exclusive domain of large companies. We must work to ensure that these resources are not relegated to second-class delivery on the Internet – or else the intellectual freedoms fostered by the Internet will be constrained. One application that libraries are especially invested in is distance learning. Classes offered using audio and video streamed over the Internet have huge potential to bring expert teachers into the homes of students around the globe.[13]

3.4. **Arguments against Net Neutrality:**

[12] http://orfonline.org/cms/sites/orfonline/modules/analysis/AnalysisDetail.html?cmaid=70589&mmacmaid=70590

[13] http://www.ala.org/advocacy/telecom/netneutrality

Net neutrality has its proponents and opponents, and I do not have space here to address that dispute. In its broadest and absolutist form, net neutrality is highly controversial (including arguments that existing status quo is not neutral in any genuine sense). I take as given, however, that some form of net neutrality is both an important and a desirable goal. In particular, intentional manipulation of information that is available to internet users – especially for political purposes.

An example of net neutrality in practice is the American Federal Communications Commission's Open Internet Order of 2010, which was the subject of litigation in the recently concluded Verizon v. FCC. The Open Internet order imposed obligations of transparency, no blocking, and no unreasonable discrimination, upon internet service providers. The second and third requirements were vacated by a United States Court of Appeals. The rationale for the Court's decision was that ISPs could not be equated, in law, to "common carriers". A common carrier is an entity that offers to transport persons and/or goods in exchange for a fee (for example, shipping companies, or bus companies). A common carrier is licensed to be one, and often, one of the conditions for license is an obligation not to discriminate. That is, the common carrier cannot refuse to carry an individual who is willing and able to pay the requisite fees, in the absence of a compelling reason (for example, if the individual wishes the carrier to transport contraband). Proponents of net neutrality have long called for treating ISPs as common carriers, a proposition – as observed above – was rejected by the Court.

3.5. **Data Discrimination:**

While the basic principle of data discrimination is censorship, those in favor of this practice claim that there are benefits. The ISPs are a business, and as such, "…correctly state that external, non-market driven constraints on their ability to price discriminate can adversely impact their incentive to invest in broadband infrastructure and their ability to recoup that investment." There are times when it could make sense, in the eyes of the ISPs, to give preference to one type of content over another. For example, loading a plain text and image website is not nearly as strenuous as loading sites such as Hulu and YouTube. Frieden states that, "Some Internet Service Providers (ISPs) seek to diversify the Internet by prioritizing bit

streams and by offering different quality of service guarantees. To some observers, this strategy constitutes harmful discrimination that violates a tradition of network neutrality in the switching, routing and transmission of Internet traffic." While the QoS argument is that network neutrality rules make allowances for network owners to practice some types of discrimination to protect the functioning of the network.

Those that oppose data discrimination say that it hurts the growth of the Internet, as well as the economy that is rooted into the depths of the Internet model. "Instead of promoting competition, such picking of winners and losers will stifle the investment needed to perpetuate the Internet's phenomenal growth, hurting the economy. "If, for example, telecommunication network operators blocked data packets of Voice-over-IP services that might substitute their own telephone services, this would not only discriminate against specifi c firms, but also reduce competition and economic welfare. Technically, this would not be a problem. Although data packets are homogeneous with respect to switching and transmission treatment, type, source, and destination can be revealed and data packets be handled differently if a network operator prefers to do so. Another problem is that the type of data that is given preferential treatment is up to the discretion of the ISP. This allows them to move data as they see fit, whether it be through a political, moral, any other such kind of "lens". This goes against the first amendment, the freedom of speech because by stopping certain kinds of information from reaching the end user, they are censoring content. It is not the place of the ISP to censor content from the people.

The real threat to an open Internet is at the local network (the ends), where network owners can block information coming in from the inter-network, but it also is at the local network where the most harm can occur. Because of this, network neutrality rules allow some discrimination by the local network to protect itself, though it may not be based on content or type of application. For example, network owners want to protect their networks from being damaged. So, some discrimination is allowed to "prevent physical harm to the local Broadband Network caused by any network attachment or network usage." This means that local network operators may not control which types of applications users choose to employ, what type of devices users use to access the network, or which type of

legal content users choose to convey or consume. The only allowable restrictions are on applications that cause harm to the local network.

Proponents of network neutrality concede that network security is crucial enough to warrant making exception to a network neutrality rule. Allowing network providers to deviate from neutrality only to the extent necessary to protect network trustworthiness is rooted in judicial and regulatory decisions and administrative rules that helped establish the principle of nondiscrimination as the core of network neutrality. Sen. Al Franken has spoken out on FCC rulings "calling net neutrality the 'free speech issue of our time,'" Franken (D-MN) expressed his displeasure with the FCC's recent net neutrality rules. 'These rules are not strong enough,' he said, pointing out that paid prioritization was not banned and that wireless networks are allowed to discriminate at will. The rules mark the 'first time the FCC has ever allowed discrimination on the Internet' and they 'will create essentially two Internets.'

3.6. Quality of Service and Net Neutrality:

Whether a communication network delivers the applications you expect as a subscriber, at the promised speed and with all features as advertised, depend upon quality of service, or QoS. The concept is part of the International Telecommunication Regulations (ITRs), which state that administrations shall "cooperate in the establishment, operation and maintenance of the international network to provide a satisfactory quality of service," and that they shall "provide and maintain, to the greatest extent practicable, a minimum quality of service." In line with the treaty, ITU has published handbooks and nearly 200 technical standards (called "Recommendations") on QoS, which are currently in force. They cover such parameters as:

- speed (data throughput) of access networks
- congestion in backbone networks
- delays in transmission (latency)
- variations in delay (jitter), and
- loss of information during transmission.

However, a major challenge for determining QoS has arisen since the ITRs were agreed in 1988. There has been a fundamental shift away from traditional networks based on dedicated service channels, or separate networks for each service. Nowadays, the trend is for a single infrastructure based on the Internet protocol (IP) to deliver all services, whether voice, video or data- and increasingly to just a single device. Traditionally, responsibility for QoS in international communications is divided among the terminating national networks. But in modern packet-based networks, quality parameters are mostly undefined and the responsibility for QoS is no longer clear. Basically, in an IP environment, services are applications executed in the equipment of the user, and the networks themselves cannot fully control the end-to-end quality of what is delivered. The problem is becoming more urgent with the dramatic increase in mobile communications, which may include hybrid connections with wired networks and terminals. Added to this, networks are becoming increasingly congested because of the boom in data (especially video) traffic. New approaches are needed for the new structure of today's communication systems. To continue providing adequate QoS, network operators and service providers can build more infrastructure — but this requires huge investments to deal with the enormous growth expected in traffic. The parallel solution is traffic management: making systems more efficient, while also setting restrictions on the amount of data that can be sent, and who gets priority as a sender or receiver. How traffic on IP networks could — or whether it should — be restricted in this way is sometimes included in discussions of "net neutrality."

3.7. Pricing Models:

The 'evils of price discrimination' are almost always voiced by individuals fervently advocating for the necessity of universal and uncapped internet access tariffs – often to the extent that metered internet access should be legislated out of existence, so that the digital world can flourish unbounded and 'free', just as its instigators intended. If one digs a little deeper, one would probably find that the vast majority of these ardent advocates currently purchase their (uncapped) fixed internet connection in a 'triple play bundle' alongside their cable or IPTV subscription and some form of voice telephony service.

Do these advocates realize the double standard they exhibit when calling for the prohibition of one form of price discrimination while at the same time benefiting from price discrimination that underpins the entire business case of their digital experiences? Because 'flat rate' internet access and triple play bundles are simply other forms of price discrimination. If price discrimination is illegal then surely these too must be banned?

Take flat-rate pricing plans. Suppose A and B both purchase a flat-rate internet connection for $30 per month. In one month, A uses 100 Gb and B 1Gb. A's usage is more costly than B's, simply because it causes more congestion on the network. B pays $30 per Gb for traffic moved, but A pays only 30c per Gb. This is clearly price discrimination, as each pays a different price for the same service.

It is strictly regressive – the less resource consumed to serve demand, the higher the price paid. The low-volume users subsidize the high volume ones, who generate more traffic and contribute to higher levels of congestion that further disadvantage low volume consumers when all must pay a higher price for flat-rate connections to finance more capacious pipes that must be installed to cope with the increased traffic volumes. This is hardly an equitable outcome – rather, it is a modern day 'tragedy of the commons'. The solution is, unsurprisingly, metered Internet connections (also known as usage-based pricing) – Just like road tolls and other usage-based charges are used to ameliorate congestion and fund new routes. Now turning to bundling. Suppose that a retailer offers stand-alone fixed line voice and internet connections at $30 each. Suppose B values his 1 Gb internet usage sufficiently to pay up to $35 per month for it, but values a fixed line voice connection at only $15. On the other hand, C values voice at $35 and potential internet usage of 1 Gb per month at $20. Under separate pricing, B would buy only internet at $30 (leaving a surplus of $5) as his valuation of voice ($15) is less than the price ($30). Likewise, C will buy only voice (surplus $5) but not internet. Suppose now that the retailer offers a bundle of voice and internet at $49, in addition to the stand-alone offers. If B buys the bundle, his benefit is $35 + $15 = $50, less the price of $49, leaving a surplus of $1. This is less surplus in total than buying the internet connection alone ($5), so he does not buy the bundle – he purchases only internet. He still pays $30 per Gb of internet access. On the other hand, if C buys the bundle, his benefit is $35 + $20 = $55 less price paid $49, leaving a surplus of $6. This exceeds the surplus from buying the voice connection

alone ($5), so be buys the bundle. The marginal (extra) price paid for internet over the price paid for voice alone) is $19. So he pays $19 per Gb of internet access. Once again, this is price discrimination – the price paid by C for exactly the same service as received by B is lower. Ergo, bundling enables price discrimination to take place.

Indeed, bundling plans have enabled many lower-valuing individuals to purchase internet (and voice and cable tv) connections that would never have been purchased under stand-alone pricing. Consider D, who values 1 Gb of internet at $25 and voice at $25. Under stand-alone pricing, neither would be purchased, but under bundling, both are (surplus $1). Network operators have always used price discrimination of this form to increase the total number of connections sold, in order to capitalize on the scale economies that follow from the fact that networks have very high fixed (and sunk) costs, but low variable costs. Price discrimination is absolutely standard in all other forms of transportation – such as senior citizens paying discounted prices on off-peak bus travel, or large discounts for multi-trip tickets relative to the single ticket price – for precisely the same reasons as it is used in communications networks. Often, it can make the difference between being able to make a commercial return on a network/bus route or not, and can bring forward the time at which a network is made available, relative to non-discriminatory (and stand-alone) pricing.

So is price discrimination really an 'evil' that must be eliminated if the 'net' is to be truly 'open'? If it was, then the internet would be a much smaller, more exclusive and less valuable resource than the one that has emerged as a consequence of a raft of highly discriminatory pricing strategies. The good news is that the FCC's Net Neutrality announcement suggests that "good" (i.e. welfare-enhancing) discrimination will still be possible. So maybe there is a legitimate case for taxing content distributors for the congestion costs that their traffic causes non-consumers in a world of un-metered internet access pricing. Indeed, it may just be the final frontier for internet 'fairness' for all – in the same manner as taxing polluters for the costs they cause to the economy or levying tolls to discourage costly road congestion.[14]

3.8. Net Neutrality under Threat:

[14] http://www.techpolicydaily.com/communications/net-neytrality-debate-price-discrimination/

Certain Internet traffic management ("ITM") techniques currently allow ISPs to block, downgrade or prioritize specific data flows. Research has shown that ITM is frequently deployed in order to block or downgrade specific Internet traffic relating to online services which compete with other services offered by the ISPs. Such practices compromise end-users' capacity to freely receive and impart information online using applications, services and devices of their choice, and jeopardize the open and neutral character of Internet architecture. Furthermore, some large European ISPs have made clear through the media and other avenues, such as shareholders' meetings and industry associations, that they intend to depart from neutral Internet access provision, in order to discriminate and priorities specific data-flows and monetize the value that specific online applications, services and content (conceived by Internet users) present to their subscribers. This illustrates that existing European approaches based purely on economic and competition-law principles have thus far failed to fully enforce the network neutrality principle, even though European telecommunications markets have generally been considered relatively competitive. Indeed, just as the right to vote alone is not enough to ensure freedom in a constitutional democracy, the possibility to switch providers – which may be seen as the right to 'vote (an ISP) with your feet' – is not enough to adequately ensure the enjoyment of users' freedoms on the Internet. Therefore, it seems necessary to query what kind of policy and legal approach would be best suited to enforce the network neutrality principle and safeguard the public-service value of the Internet.

3.9. **Net Neutrality: US Position:** (Reuters[15]) –

U.S. President Barack Obama said Internet service providers should be regulated more like public utilities to make sure they grant equal access to all content providers, touching off intense protests from cable and telecoms companies and Republican lawmakers. Obama's detailed statement on the issue of "net neutrality," a platform in his 2008 presidential campaign, was a rare intervention by the White House into the policy setting of an independent agency. Shares of major Internet service providers Comcast Corp (CMCSA.O) and Time Warner Cable Inc (TWC.N) fell sharply after Obama said ISPs should be

[15] http://www.reuters.com/article/2014/11/10/us-usa-internet-neutrality-idUSKCN0IU1I620141110

reclassified to face stricter regulations and banned from striking paid "fast lane" deals with content companies. The president also said the Federal Communications Commission's new rules should apply equally to mobile and wired ISPs, with recognition of special challenges that come with managing networks.

"Simply put: No service should be stuck in a 'slow lane' because it does not pay a fee," Obama, currently in Asia, said in a statement released by the White House. "That kind of gate keeping would undermine the level playing field essential to the Internet's growth." Nearly 4 million comments flooded the FCC this year after Chairman Tom Wheeler proposed new Internet traffic rules in May that would prohibit the ISPs from blocking any content but allowed content companies to strike "commercially reasonable" deals to ensure their websites and applications load smoothly and swiftly. Although Wheeler had pledged to police any such paid-prioritization deals that would harm consumers, public interest groups worried that his proposed rules would create "fast lanes" for the companies that pay up and relegate others to "slow lanes." ISPs say they have not and will not strike paid prioritization deals but have balked at the prospect of being regulated more like public utilities. "Reclassification ..., which for the first time would apply 1930s-era utility regulation to the Internet, would be a radical reversal of course," Verizon Communications Inc (VZ.N) said in a statement. Verizon in January won a federal court case challenging the FCC's previous set of net neutrality rules, which allowed "commercially reasonable" discrimination of traffic but indicated the FCC would disapprove of pay-for-priority deals.

The court supported the commission's authority to regulate broadband access but said the agency was applying stricter rules to ISPs that did not jibe with the way the FCC classified them, which is as an information service. Consumer advocates have for years pressed the FCC to reclassify broadband as a telecommunications service as a way to have more oversight authority, but ISPs have pledged they would fight the matter in court. Verizon on Monday said a "gratuitous" move to reclassify would probably not stand up in court, while AT&T said it would expect to participate in a legal challenge.

'OBAMACARE FOR THE INTERNET': Wheeler, Obama's friend and former major fundraiser, on Monday reiterated that he, too, opposed Internet fast lanes or harmful prioritization deals but said that approaches including

reclassification of ISPs to regulate them more strictly raised substantive legal questions.

"We must take the time to get the job done correctly, once and for all, in order to successfully protect consumers and innovators online," Wheeler said. Obama and other White House officials acknowledged that the FCC, as an independent agency, would ultimately shape the regulations. But Republicans lawmakers quickly seized on Obama's encroachment, days after their party won control of both houses of Congress in a midterm election largely viewed as a repudiation of the president's policies.

Net neutrality is Obamacare for the Internet," said Senator Ted Cruz of Texas. "It puts the government in charge of determining Internet pricing, terms of service, and what types of products and services can be delivered." Though lobbyists say legislative efforts to overturn new rules would face a White House veto, cable and wireless companies were expected to turn to Republican allies in Congress for stricter oversight of the FCC. "The president's call ... would turn the Internet into a government-regulated utility and stifle our nation's dynamic and robust Internet sector with rules written nearly 80 years ago for plain old telephone service," said Senator John Thune, a Republican expected to lead the Senate Commerce Committee. Wheeler had originally pushed to reinstate net neutrality rules before the end of the year, but experts on Monday said the latest developments probably pushed the process into 2015. Time Warner Cable shares fell as much as 7.2 percent, and closed down almost 5 percent, while Comcast dropped as much as 6.1 percent and closed own 4 percent. Comcast, whose bid to buy Time Warner Cable is under regulatory review, was by far the most actively traded stock on U.S. markets.

3.10. Net Neutrality and TRAI (Telephone Regulatory Authority of India):

Following Airtel's violation of Net Neutrality principles, Rahul Khullar, the TRAI Chairman, while acknowledging that Airtel has violated Net Neutrality, made some worrying statements to the Financial Express, and left me wondering about the point of making a case before an already-prejudiced adjudicator, and

whether the consultation will end up being a farce to justify a decision already taken by the TRAI.

To the Financial Express, Khullar said:

'"If the telecom players fall under a set of rules, then should not the OTT players be also brought under some kind of rules? Otherwise there would be a non-level playing field," he said.'

Pointing out the ways OTT players could be brought under regulation, Khullar said that there could be licensing norms for them also wherein they have to pay licence fees to the government on a revenue-share basis. The other option, which is simpler, is that a termination charge is put on calls originating from Viber or Skype kind of services.'

While Khullar explains the case for bringing OTT applications (which, according to telecom operators, includes Social Networking, Instant Messaging (IM), Applications (Apps),VoIP, Cloud Services, Internet Television, IPTV, Machine to Machine communications), arguing about a level playing field, where is he explaining the consumer point of view, or the Internet industry point of view? If he has to present a case (he shouldn't), shouldn't he present cases from all three sides, to the audience, as a neutral, unbiased adjudicator? Instead, while he says Airtel's actions violate net neutrality, he clarifies that it isn't illegal for Airtel to do so, and mentions the need for a level playing field. Where is the consumer interest perspective? Frankly, the only level playing field needed is so that Airtel, which runs Wynk, doesn't use its role as an access service provider to make competitors like Saavn and Gaana more expensive. Remember that Airtel also runs Airtel Talk, a VoIP service. Will VoIP on Skype be made more expensive than on Airtel Talk?

While Khullar explains the case for bringing OTT applications (which, according to telecom operators, includes Social Networking, Instant Messaging (IM), Applications (Apps),VoIP, Cloud Services, Internet Television, IPTV, Machine to Machine communications), arguing about a level playing field, where is he explaining the consumer point of view, or the Internet industry point of view? If he has to present a case (he shouldn't), shouldn't he present cases from all three sides, to the audience, as a neutral, unbiased adjudicator? Instead, while he says Airtel's actions violate net neutrality, he clarifies that it isn't illegal

for Airtel to do so, and mentions the need for a level playing field. Where is the consumer interest perspective?

Frankly, the only level playing field needed is so that Airtel, which runs Wynk, doesn't use its role as an access service provider to make competitors like Saavn and Gaana more expensive. Remember that Airtel also runs Airtel Talk, a VoIP service. Will VoIP on Skype be made more expensive than on Airtel Talk?

Neutrality is critical: The TRAI needs to approach Net Neutrality without a prejudiced mind. Three core principles of neutrality:

1. All sites must be equally accessible: ISPs and telecom operators shouldn't block certain sites or apps just because they don't pay them. No gateways should be created, in order to give preferential discovery to one site over another.
2. All sites must be accessible at the same speed (at an ISP/telco level): This means no speeding up of certain sites because of business deals. More importantly, it means no slowing down some sites.
3. The cost of access must be the same for all sites (per Kb/Mb or as per data plan): This means no "Zero Rating". In countries like India, Net Neutrality is more about cost of access than speed of access: all lanes are slow.

It's important for the growth of the Internet in India, and both consumers and the Internet industry (Digital India, anyone?) that neutrality be absolute, and the principle of the 'calling party pays' remain true for the Internet as well[16].

3.11. Summary:

Net neutrality is a very important phenomenon of the E-security. In this unit the meaning and scope of net neutrality, arguments for net-neutrality, arguments against net neutrality, data discrimination, quality of service and net-neutrality, pricing models, net-neutrality under threat, the US position on Net-Neutrality, and Net Neutrality and TRAI are discussed at length to understand the concept and feature of the Net-Neutrality. This is a universal concept and applicable to all countries.

[16] http://www.medianama.com/

3.12. Some Useful Books:

1. Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
2. Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
3. Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
4. Cyber Terrorism by S. Venkatesh (Authorpress)
5. Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
6. Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
7. Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
8. Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
9. Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
10. Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
11. Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
12. Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
13. Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
14. Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
15. The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
16. Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
17. Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)

18. Computers, Privacy and Data Protection: An Element of Choice (Springer)
19. All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

3.13. Check your Progress:

A. Which of the following statements are true and false:

A. Net neutrality is also known as Network Neutrality, Internet Neutrality or Net Quality.
B. India currently has no law on Net Neutrality.
C. The American Library Association is a strong advocate for intellectual freedom.
D. TRAI needs to approach Net-Neutrality without a prejudicial mind.
E. One core principle of neutrality is "all sites must be equally accessible".

B. Fill in the Blanks:

i. Net neutrality term was coined by Columbia University Media Law Professor ……
ii. Users can access any legal website or web service without any interference from an ……..
iii. Network Neutrality or net neutrality is the concept of ……
iv. The basic principle of data discrimination is ……
v. …….techniques currently allow ISPs to block, downgrade or prioritize specific data flows.

3.14. Answer to Check your Progress:

A.

1. True
2. True
3. True

4. True
5. True

B.

1. Tim Wu in 2003
2. ISP
3. Online non-discrimination
4. Censorship
5. Certain Internet Traffic Management (ITM)

3.15. Terminal Questions:

a. What is the meaning and scope of Net- Neutrality?
b. What are the arguments in favour of Net-Neutrality?
c. What are the arguments against Net-Neutrality?
d. Define data discrimination.
e. What is pricing models?

Unit-4

Legal Recognition of Digital Signature

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Legal Recognition of Digital Signature
- Understand the remedies which are available against illegal use of Digital Signature
- Understand the technical and legal issues related to Legal Recognition of Digital Signature

Structure:

4.1 Introduction:

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures enable the recipient of the information to verify the authenticity of the information's origin, and also verify that the information is intact. Thus, digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more. A digital signature serves the same purpose as a handwritten signature. However, a handwritten signature is easy to counterfeit. A digital signature is superior to a handwritten signature in that it is nearly impossible to counterfeit, plus it attests to the contents of the information as well as the identity of the signer.

The vision of National eGovernance Plan (NeGP) of Government of India is to "make all Government services accessible to the common man in his locality, through Common Service Delivery Outlets and ensure efficiency, transparency and reliability of such services at affordable costs to realise the basic needs of the common man". The key objective of this vision is to provide e-services - G2B and G2C - in a ubiquitous manner. With the implementation of the National eGovernance Plan (NeGP), more and more Departments/Line Ministries in India are automating their operations and business processes and making their Service delivery online. As a result, electronic documentation is slowly permeating every aspect of the business workflow in the Government Departments. However when a signature authorization is required on a document, a hard copy is printed to get a physical routing of signatures. The reintroduction of paper into the workflow increases the Government costs, requires additional time, and prohibits the Government Departments/Line Ministries from realizing the true benefits of a fully electronic workflow. Digital Signatures provide a viable solution for creating legally enforceable electronic records, closing the gap in going fully paperless by completely eliminating the need to print documents for signing. Digital signatures enable the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones. The purpose of a digital signature is the same as that of a handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptography). Like the pen and paper method, a digital signature attaches the identity of the signer to the document and

records a binding commitment to the document. However, unlike a handwritten signature, it is considered impossible to forge a digital signature the way a written signature might be. In addition, the digital signature assures that any changes made to the data that has been signed cannot go undetected.

4.2 Legal Position of Digital Signature :

As per section 2(1) (f) of the Information Technology Act, 2000 the definition of the ‘digital signature is "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.”

Section 5 of the Information Technology Act, 2000: Legal recognition of digital signatures: Where any lay provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation: For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, means affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Section 3 of the Information Technology Act, 2000: Authentication of electronic records:

A. Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.
B. The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation: For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same

hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

A. To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
B. That two electronic records can produce the same hash result using algorithm.

4. Any person by the use of a public key of the subscriber can verify the electronic record.
5. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

4.3 Legal Recognition of Electronic Record (Section 4):

Section 4 of the Information Technology Act, 2000: Legal recognition of electronic **records:**

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

(a) Rendered or made available in an electronic form; and
(b) Accessible so as to be usable for a subsequent reference.

Section 6 of the Information Act, 2000: Use of electronic records and digital signatures in Government and its agencies:

(1) Where any law provides for-

i. the filing of any form, application or any other document with any office authority, body for agency owned or controlled by the appropriate Government in a particular manner;
ii. The issue or grant of any license, permit. Sanction or approval by whatever name called in a particular manner;
iii. the receipt or payment of money in a particular manner, the, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case be, is effected by

means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-

a) the manner and format in which such electronic records shall be filed, created or issued;

b) The manner or method of payment of any fee or charges for filing, creation or issue any electronic record clause (a).

4.4 Secure Electronic Record (Section 14):

11. Attribution of electronic records.-

An electronic record shall be attributed to the originator,-

a) if it was sent by the originator himself;
b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
c) by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledge of receipt.-

(1) Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by-

a) any communication by the addressee, automated or otherwise; or
b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have been never sent by the originator.

Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgement has

not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which he acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as tough it has never been sent.

13. Time and place of dispatch and receipt of electronic record. –

(1) Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resources outside the control of the originator.;

Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:- the addressee has designated a computer resource for the purpose of receiving electronic record,- receipt occurs at the time when the electronic record enters the designated computer resources; or

if the electronic record is spent to a computer resources of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be received at the place where the addressee has his place of business.

The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

For the purpose of this section.- if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;

if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
"usual place of residence ", in relation to a body corporate, means the place where it is registered.

14. Secure electronic record.-

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

4.5 Secure Digital Signature (Section 15):

15. Secure digital signature.-

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was –

(a) Unique to the subscriber affixing it;

(b) Capable of identifying such subscriber;

(c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which related in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

4.6 Digital Signature Certificate:

35. Certifying authority to issue Digital Signature Certificate.–

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that-

the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

the applicant holds a private key, which is capable of creating a digital signature;

the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance Digital Signature Certificate. –

A Certifying Authority while issuing a Digital Signature Certificate shall certify that- it has complied with the provisions of this Act and the rules and regulations made thereunder;

it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

the subscriber's public key and private key constitute a functioning key pair;

the information contained in the Digital Signature Certificate is accurate; and

it has no knowledge of any6 material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations in clauses (a) to (d).

37. Suspension of Digital Signature Certificate. –

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate.- on receipt of a request to that effect from-

The subscriber listed in the Digital signature Certificate; or

Any person duly authorized to act on behalf of that subscriber;

If it is of opinion that the Digital Signature Certificate should be suspended in public interest.

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.'

39. Revocation of Digital Signature Certificate. –

(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it-

Where the subscriber or any other person authorized by him makes a request to that effect; or upon the death of the subscriber; or upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that-a material fact represent in the Digital Signature Certificate is false or had been concealed;

A requirement for issuance of the Digital Signature Certificate was not satisfied;

The Certifying Authority's private key of security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

The subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.
A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation. –

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
Where one or more repositories are specified the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

4.7 Regulation of Certifying Authorities:

17. Appointment of Controller and other officers. –

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may, also by the same or subsequent notification, appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
(3) The Deputy Controllers and Assistant Controllers shall perform functions assigned to them by the Controller under the general superintendence and control of the Controller.
(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controller shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Officer of the officer of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller. –

The Controller may perform all or any of the following function, namely:-

a) exercising supervision over the activities of Certifying Authorities;
b) certifying public keys of the Certifying Authorities;
c) laying down the standards to be maintained by Certifying Authorities;
d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
e) specifying the conditions subject to which the Certifying Authority shall conduct their business;
f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
g) specifying the form and content of a Digital Signature Certificate and the key;
h) specifying the form the manner in which accounts shall be maintained by the Certifying Authorities;
i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;
k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
m) laying down the duties of the Certifying Authorities;
n) Maintaining a data-base containing the disclosure record of ever Certifying Authority containing such particulars as may be specified by regulations which shall be accessible to public.

21. License tissue Digital Signature Certificates. –

1. Subject to the provisions of sub-section (2), any person may make an application to the Controller for a license to issue Digital Signature Certificates.
2. No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.
3. A license granted under this section shall-
   a) be valid for such period as may be prescribed by the Central Government;
   b) not be transferable or heritable;
   c) Be subject to such terms and conditions as may be specified by the regulations.

4.8 Classes of Digital Signature:

In addition to four classes of certificates given below, the Certifying Authority may issue more classes of Public Key Certificates, but these must be explicitly defined including the purpose for which each class is used and the verification methods underlying the issuance of the certificate. The suggested four classes are the following:-

Class 0 Certificate: This certificate shall be issued only for demonstration/ test purposes.

Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-

commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

4.9 Digital Signature v Hand written Signature:

A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. A Digital Signature is a combination of 0 & 1s created using crypto algorithms. An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Further, paper contracts often have the ink signature block on the last page, allowing previous pages to be replaced after the contract has been signed. Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail. As can be seen in the underlying figure, a Digital Signature is a string of bits appended to a document. The size of a digital signature depends on the Hash function like SHA 1 / SHA2 etc used to create the message digest and the signing key. It is usually a few bytes.

Difference between Electronic Signatures and Digital signatures: An electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

Overview of how Digital Signatures work: The Digital Signatures require a key pair (asymmetric key pairs, mathematically related large numbers) called the Public and Private Keys. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like crypto smart card or crypto token. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key. In order to digitally sign an electronic document, the

sender uses his/her Private Key. In order to verify the digital signature, the recipient uses the sender's Public Key.

Let us understand how the Digital Signatures work based on an example. Assume you are going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you had sent and that it is really from you.

a) You copy-and-paste the contract into an e-mail note. Get electronic form of a document (eg : - word or pdf file)
b) Using special software, you obtain a message hash (fixed size bit string) of the contract.
c) You then use your private key to encrypt the hash.
d) The encrypted hash becomes your digital signature of the contract and is appended to the contract.

At the other end, your lawyer receives the message.

a) To make sure the contract is intact and from you, your lawyer generates a hash of the received contract.
b) Your lawyer then uses your public key to decrypt the Digital Signature received with the contract.
c) If the hash generated from the Digital Signature matches the one generated in Step 1, the integrity of the received contract is verified.

4.10 Power to make rules by Central Government in respect of Digital Signature:

Section 10 of the Information Technology Act 2000: Power to make rules by Central Government in respect of digital signature: The Central Government may, for the purposes of this Act, by rules, prescribe-

1) the type of digital signature;
2) the manner and format in which the digital signature shall be affixed;
3) the manner or procedure which facilitates identification of the person affixing the digital signature;
4) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

5) any other matter which is necessary to give legal effect to digital signatures.

4.11 Summary:

The concept of the digital signature is now accepted worldwide and protected through various legal provisions at national and international level. In this unit the concept of legal position of digital signature, legal recognition of electronic records, secure electronic records, secure digital signature, digital signature certificate, regulation of certification authorities, classes of digital signature, the difference between digital signature and hand written signature and the power to make rules by Central Government in respect of digital signature are discussed at length to understand the relevant concept incorporated under the various legislations dealing digital signature.

4.12 Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)

- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

4.13 Check your Progress:

A Which of the following statements are true or false:

a) A major benefit of the public cryptography is that it provides a method for employing digital signature.

b) A digital signature serves the same purpose as a hand written signature.

c) Section 37 of the Information Technology Act, 2000 is related to suspension of digital signature certificate.

d) Section 17 of the IT Act, 2000 is related to appointment of Controller and other Officers.
e) There are 6 classes of digital signature.

B Fill in the Blanks:

1) Instead of using pen and paper, a digital signature uses……..
2) The definition of 'digital signature' is incorporated under……of the IT Act, 2000.
3) ……of the IT Act, 2000 is related to legal recognition of the electronic records.
4) ……of the IT Act, 2000 is related to Secure Digital Signature.
5) …….of the IT Act, 2000 is related to Certifying Authority to issue digital signature certificate.

4.14 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. False

B.

1. Digital Key (Public Key Cryptography)
2. Section 2(1)(f)
3. Section 4
4. Section 15
5. Section 35

4.15 Terminal Questions

1) Discuss legal position of digital signature.
2) What is electronic record and secure electronic record?
3) What is digital signature certificate?

4) Differentiate between digital signature and hand written signature.
5) What is the power to make rules by Central Government in respect of digital signature?

Unit-5

Web Content Accessibility Guidelines (WCAG)

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Web Content Accessibility Guidelines
- Understand the international approaches of Web Content Accessibility Guidelines
- Understand the technical and legal issues related to Web Content Accessibility Guidelines

Structure:

5.1. Introduction:

Web Content Accessibility Guidelines (WCAG) is developed through the W3C process in cooperation with individuals and organizations around the world, with a goal of proving a single shared standard for web content accessibility that meets the needs of individuals, organizations, and governments internationally.

The WCAG documents explain how to make web content more accessible to people with disabilities. Web "content" generally refers to the information in a web page or web application, including:

- natural information such as text, images, and sounds
- code or markup that defines structure, presentation, etc.
- Web accessibility is about creating websites that are accessible to people of all ages and types of disabilities.
- An Accessible Web means that people with disabilities can perceive, understand, navigate, and interact with the Web, and that they can contribute to the Web.
- Accessibility also benefits older people and general usability of websites.
- Web Accessibility Reduces Disability Discrimination
- Increases people with a disability's access to Information

Accessibility also considers the way people are currently using the internet, and the functions of people's lives that are currently online, and continue to move online. Creating an Equitable Web is important because it allows people to remain connected to the community at large.

5.2. **Who WCAG for?:** WCAG is primarily intended for:

- Web content developers (page authors, site designers, etc.)
- Web authoring tool developers
- Web accessibility evaluation tool developers
- Others who want or need a standard for web accessibility

Related resources are intended to meet the needs of many different people, including policy makers, managers, researchers, and others.

WCAG is a technical standard, not an introduction to accessibility.

Four areas of accessibility[17]

- Perceivable
- Operable
- Understandable
- Robust

Sitting under these four areas are 12 guidelines. The guidelines provide information including pass and fail examples in the areas of design, content and technology.

Perceivable

- Text Alternatives: Provide Text Alternatives for any non-text content.
- Time-based Media: Provide Alternatives for time based media.
- Adaptable: Create content that can be presented in different ways without losing information or structure.
- Distinguishable: Make it easier for users to see and hear content including separating foreground from background.

Operable

- Keyboard Accessible: Make all functions available from a keyboard.
- Enough Time: Provide users enough time to read and use content.
- Seizures: Do not design content in a way that is known to cause seizures.
- Navigable: Provide ways to help users navigate, find content and determine where they are.

Understandable

- Readable: Make text content readable and understandable.
- Predictable: Make Web pages appear and operate in predictable ways.
- Input Assistance: Help users avoid and correct mistakes.

Robust

- Compatible: Maximise compatibility with current and future user agents, including assistive technologies.

[17] http://www.energetica.com.au/blog/492-a-brief-introduction-to-the-elements-of-accessibility

Web Accessibility is something that we here at Energetica are particularly passionate about, simply put, Energetica are Accessibility Experts. There is a lot of information that must be considered when developing accessible content, and we're only just beginning to scratch the surface. If your organisation is thinking of developing accessible content, why not get in touch with us.

Further Information: Web Accessibility at a Glance

Don't be fooled by the 'at a glance' part though. The elements that make up web accessibility success or failure are complex, and sometimes subjective. I know I said earlier that there isn't a "checklist" approach that can easily be applied to accessibility – there isn't but lists are nice and easy to read so I have included a link to a resource that includes a checklist below.

5.3. What is WCAG 2.0?

WCAG 2.0 is a stable, reference able technical standard. It has 12 guidelines that are organized under 4 principles: perceivable, operable, understandable, and robust. For each guideline, there are testable success criteria, which are at three levels: A, AA, and AAA.

The WCAG 2.0 supporting technical materials include:

- How to Meet WCAG 2.0: A customizable quick reference to Web Content Accessibility Guidelines 2.0 requirements (success criteria) and techniques is essentially the WCAG 2.0 checklist. Most people use this quick references as the main resource for working with WCAG.
- Techniques for WCAG 2.0 gives you specific details on how to develop accessible Web content, such as HTML code examples. The techniques are "informative", that is, you do not have to use them. The basis for determining conformance to WCAG 2.0 is the success criteria from the WCAG 2.0 standard, not the techniques. Read more in Techniques in the FAQ.
- Understanding WCAG 2.0 has additional guidance on learning and implementing WCAG 2.0 for people who want to understand the guidelines and success criteria more thoroughly.
- WCAG 2.0 is approved as an ISO standard: ISO/IEC 40500:2012. ISO/IEC 40500 is exactly the same as the original WCAG 2.0, which is introduced

above along with supporting resources. The content of ISO/IEC 40500 is freely available from www.w3.org/TR/WCAG20; it is available for purchase from the ISO catalogue. Benefits of WCAG 2.0 as an ISO standard are summarized in ISO in the FAQ. More information on W3C and the ISO process is in the W3C PAS FAQ.

Understanding the Four Principles of Accessibility:

Layers of Guidance:

The Guidelines: Under each principle there is a list of guidelines that address the principle. There are a total of 12 guidelines. A convenient list of just the guidelines can be found in the WCAG 2.0 tables of contents. One of the key objectives of the guidelines is to ensure that content is directly accessible to as many people as possible, and capable of being re-presented in different forms to match different peoples' sensory, physical and cognitive abilities.

Success Criteria: Under each guideline, there are Success Criteria that describe specifically what must be achieved in order to conform to this standard. They are similar to the "checkpoints" in WCAG 1.0. Each Success Criterion is written as a statement that will be either true or false when specific Web content is tested against it. The Success Criteria are written to be technology neutral.

All WCAG 2.0 Success Criteria are written as testable criteria for objectively determining if content satisfies the Success Criteria. While some of the testing can be automated using software evaluation programs, others require human testers for part or the entire test.

Although content may satisfy the Success Criteria, the content may not always be usable by people with a wide variety of disabilities. Professional reviews utilizing recognized qualitative heuristics are important in achieving accessibility for some audiences. In addition, usability testing is recommended. Usability testing aims to determine how well people can use the content for its intended purpose. The content should be tested by those who understand how people with different types of disabilities use the Web. It is recommended that users with disabilities be included in test groups when performing human testing.

Each Success Criterion for a guideline has a link to the section of the How to Meet document that provides:

- sufficient techniques for meeting the Success Criterion,
- optional advisory techniques, and
- Descriptions of the intent of the Success Criteria, including benefits, and examples.

5.4. Essential Component of the Web Accessibility[18] :

It is essential that several different components of Web development and interaction work together in order for the Web to be accessible to people with disabilities. These components include:

- content - the information in a Web page or Web application, including:
  - natural information such as text, images, and sounds
  - code or markup that defines structure, presentation, etc.
- Web browsers, media players, and other "user agents"
  - assistive technology, in some cases - screen readers, alternative keyboards, switches, scanning software, etc.
  - users' knowledge, experiences, and in some cases, adaptive strategies using the Web
  - developers - designers, coders, authors, etc., including developers with disabilities and users who contribute content
  - authoring tools - software that creates Web sites
  - evaluation tools - Web accessibility evaluation tools, HTML validators, CSS validators, etc.
  - Web **developers** usually use **authoring tools** and evaluation tools to create Web **content**.
  - **People** ("**users**") use Web **browsers, media players, assistive technologies,** or other "**user agents**" to get and interact with the **content**.

There are significant interdependencies between the components; that is, the components must work together in order for the Web to be accessible. For example, for alternative text on images:

- Technical specifications address alternative text (for example, HTML defines the alternative text attribute (alt) of the image element (img))

[18] http://www.w3.org/WAI/intro/components.php

- WAI guidelines - WCAG, ATAG, and UAAG, described below - define how to implement alternative text for accessibility in the different components
- Developers provide the appropriate alternative text wording
- Authoring tools enable, facilitate, and promote providing alternative text in a Web page
- Evaluation tools are used to help check that alternative text exists
- User agents provide human and machine interface to the alternative text
- Assistive technologies provide human interface to the alternative text in various modalities
- Users know how to get the alternative text from their user agent and/or assistive technology as needed

When accessibility features are effectively implemented in one component, the other components are more likely to implement them.

- When Web browsers, media players, assistive technologies, and other user agents support an accessibility feature, users are more likely to demand it and developers are more likely to implement it in their content.
- When developers want to implement an accessibility feature in their content, they are more likely to demand that their authoring toolmake it easy to implement.
- When authoring tools make a feature easy to implement, developers are more likely to implement it in their content.
- When an accessibility feature is implemented in most content, developers and users are more likely to demand that user agents support it.

If an accessibility feature is not implemented in one component, there is little motivation for the other components to implement it when it does not result in an accessible user experience. For example, developers are unlikely to implement an accessibility feature that authoring tools do not support and that most browsers or assistive technologies do not implement consistently.

If one component has poor accessibility support, sometimes other components can compensate through "work-arounds" that require much more effort and are not good for accessibility overall. For example,

- ❖ developers can do more work to compensate for some lack of accessibility support in authoring tools; for example, coding markup directly instead of through a tool
- ❖ users can do more work to compensate for some lack of accessibility support in browsers, media players, and assistive technology and lack of accessibility of content; for example, using different browsers or assistive technologies to overcome different accessibility issues

However, in most cases the works-arounds are not implemented and the result is still poor accessibility. Additionally, sometimes poor accessibility support in one component cannot be reasonably overcome by other components and the result is inaccessibility, making it impossible for some people with disabilities to use a particular Web site, page, or feature.

Guidelines for different Components: The World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI) develops Web accessibility guidelines for the different components:

- Authoring Tool Accessibility Guidelines (ATAG) addresses authoring tools
- Web Content Accessibility Guidelines (WCAG) addresses Web content, and is used by developers, authoring tools, and accessibility evaluation tools
- User Agent Accessibility Guidelines (UAAG) addresses Web browsers and media players, including some aspects of assistive technologies

WAI guidelines are based on the fundamental technical specifications of the Web, and are developed in coordination with:

- W3C technical specifications (HTML, XML, CSS, SVG, SMIL, etc.)

5.5. User Agent Accessibility Guidelines (UAAG) Overview:

The User Agent Accessibility Guidelines (UAAG) documents explain how to make user agents accessible to people with disabilities, particularly to increase accessibility to Web content. User agents include Web browsers, media players, and assistive technologies, which are software that some people with disabilities use in interacting with computers.

UAAG is part of a series of accessibility guidelines, including the Web Content Accessibility Guidelines (WCAG WG) and the Authoring Tool Accessibility Guidelines (ATAG). Essential Components of Web Accessibility explains the relationship between the different guidelines.

UAAG is primarily for developers of Web browsers, media players, assistive technologies, and other user agents.

UAAG and supporting resources are also intended to meet the needs of many different audiences, including policy makers, managers, and others. For example:

- People who want to choose user agents that are more accessible can use UAAG to evaluate user agents
- People who want to encourage their existing user agent developer to improve accessibility in future versions can refer the user agent vendor to UAAG

UAAG 1.0 contains a comprehensive set of checkpoints that cover:

- Access to all content, including content tied to events triggered by the mouse or keyboard
- User control over how content is rendered
- User control over the user interface, with documentation of accessibility features
- Standard programming interfaces, to enable interaction with assistive technologies

Technical document format: UAAG 1.0, the techniques documents, and the checklist follow the W3C format for technical specifications which includes several sections at the beginning: links to different versions, editors, copyright, abstract, and status with the link to errata and the email address for comments. Most WAI specifications have a link at the top to the Table of Contents User Agent Accessibility Guidelines 1.0 was approved in December 2002 and is the stable and reference able version. UAAG 2.0 is being developed to help make future generations of Web browsers more accessible, to provide alternative information based on the users technology and platform, and to align with WCAG 2.0 and ATAG 2.0. WAI anticipates UAAG 2.0 may be completed in 2013. Because of the nature of the **W3C development process,** WAI cannot be certain when the final version of UAAG 2.0 will be available. UAAG 1.0 will remain the latest approved version until version 2.0 is complete.

Currently UAAG 2.0 **is a mature draft and we expect that the main content will not change significantly. We recommend that you use the UAAG 2.0 draft in most cases, understanding that it might change.** UAAG technical documents are developed by the User Agent Accessibility Guidelines Working Group (UAWG), which is part of the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). For more information about the working group.

5.6. Who develops WCAG?:

The WCAG technical documents are developed by the Web Content Accessibility Guidelines Working Group (WCAG WG), which is part of the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). WAI updates Techniques for WCAG 2.0 and Understanding WCAG 2.0 periodically. We welcome comments and submission of new techniques. Opportunities for contributing to WCAG and other WAI work are introduced in Participating in WAI.

16 September 2014 - the Working Group has published updated versions of Understanding WCAG 2.0 and WCAG 2.0 Techniques. The WCAG Working Group will meet face to face on 26 and 27 October 2014 in Santa Clara, California.

Publications: WCAG 2.0 was published as a W3C Recommendation 11 December 2008. This document is accompanied by other support materials (updated 16 September 2014) produced by the WCAG Working Group:

- Web Content Accessibility Guidelines 2.0
- How to Meet WCAG 2.0
- Understanding WCAG 2.0
- Techniques for WCAG 2.0
- Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT)

Web Content Accessibility Guidelines 2.0 is the normative document; the rest are supporting documents.

Current Work:

WCAG 2.0

Guidelines:

- Current **internal editors'** Working Draft of WCAG 2.0
- Current **formal public** version of WCAG 2.0 - 11 December 2008
- How to meet WCAG 2.0
- Errata in Web Content Accessibility Guidelines 2.0
- Archive of public comments
- Wiki used to track changes discussed in teleconferences
- WCAG Questionnaires are used to solicit group feedback in preparation for discussion
- Requirements for WCAG 2.0
- Open issues are maintained in the WCAG 2.0 Bugzilla database; being migrated to Comments Tracker

Understanding WCAG 2.0:

- Current **internal editors'** Working Draft of Understanding WCAG 2.0
- Current **formal public** version of Understanding WCAG 2.0 -16 September 2014

Techniques for WCAG 2.0:

- Current **internal** Working Draft of Techniques for WCAG 2.0
- Current **public** version of Techniques for WCAG 2.0 - 16 September 2014
- Requirements for WCAG 2.0 Checklists and Techniques
- Techniques submission form
- Recently submitted techniques

Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT)

- Current editors' draft of WCAG2ICT
- Current public version of WCAG2ICT - 5 September 2013

Testing WCAG 2.0

The Test Samples Development Task Force previously developed some preliminary tests. The WCAG 2.0 Evaluation Methodology Task Force (Eval TF) is working on ways to use tests.

Translations of WCAG 2.0

Translations of WCAG 2.0 have been undertaken to increase awareness and facilitate feedback on the drafts. The WCAG 2.0 translations page lists translations that are available at this time.

WCAG 1.0

- Errata in Web Content Accessibility Guidelines 1.0
- Tables of WCAG 1.0 Errata - does not represent consensus or a commitment to publish a revised WCAG 1.0.
- Publications:

- **Web Content Accessibility Guidelines (WCAG) 2.0** W3C Recommendation, 11 December 2008
- How to Meet WCAG 2.0
- Understanding WCAG 2.0
- Techniques for WCAG 2.0
- Applying WCAG 2.0 to Non-Web Information and Communications Technologies (WCAG2ICT)

- Web Content Accessibility Guidelines (WCAG) 1.0 W3C Recommendation, 5 May 1999.
    - Translations of WCAG 1.0
    - Errata in Web Content Accessibility Guidelines 1.0
- Techniques for WCAG 1.0 suite of W3C Notes, 20 September 2000
    - Techniques for Web Content Accessibility Guidelines 1.0.
    - Core Techniques for Web Content Accessibility Guidelines 1.0.
    - HTML Techniques for Web Content Accessibility Guidelines 1.0.
    - CSS Techniques for Web Content Accessibility Guidelines 1.0.
    - History of changes to the techniques.

Related documents not published by the WCAG WG

- Getting Started: Making a Web Site Accessible Includes links to Scenarios, Quick Tips, WCAG Curriculum, FAQ
- Overview of WCAG 2.0 Documents

5.7. WCAG 2.0 coverage of Mobile Accessibility:

"Mobile accessibility" generally refers to making websites and applications more accessible to people with disabilities when they are using mobile phones. WAI's work in this area includes people using a broad range of devices to interact with the web: phones, tablets, TVs, and more.

This page summarizes existing and developing resources related to mobile web accessibility. **There are not separate guidelines for mobile accessibility — mobile is covered in existing W3C accessibility guidelines** (particularly WCAG and UAAG, which are introduced below).

WAI's accessibility guidelines address mobile accessibility:

- WCAG (Web Content Accessibility Guidelines) covers web pages and web applications, including content used on mobile devices. To learn how WCAG addresses similar issues as Mobile Web Best Practices and Mobile Web Application Best Practices, see Shared Web Experiences.
- UAAG (User Agent Accessibility Guidelines) covers web browsers and other 'user agents', including mobile browsers. For examples of how web browsers that follow UAAG benefit people with

disabilities using the Web on mobile devices, see Mobile Accessibility Examples from UAAG.

- ATAG (Authoring Tool Accessibility Guidelines) covers software used to create web pages and applications, including for mobile.
- WAI is working to enhance technologies for mobile accessibility, including:
- IndieUI (Independent User Interface) is a way for user actions to be communicated to web applications, including mobile applications. This will make it easier for applications to work with a wide range of devices, including assistive technologies.
- WAI-ARIA (Accessible Rich Internet Applications) defines a way to make web content more accessible, especially dynamic content and advanced user interface controls. It applies to web applications and to accessing websites with mobile devices.
- W3C addresses mobile accessibility. WAI ensures that the core W3C technologies support accessibility, including those that are essential for the mobile web. All W3C work is reviewed for accessibility by WAI's Protocols and Formats Working Group (PFWG). W3C work on mobile includes:
- Mobile Web Application Best Practices, Mobile Web Best Practices, mobileOK Checker
- Standards for Web Applications on Mobile summarizes technologies developed in W3C that increase the capabilities of web applications, and how they apply specifically to the mobile context.

- Most of this page addresses people with disabilities using mobile devices. We also have related resources that address situations such as: a web development project wants to make their websites and web applications work better for all mobile users (including those without disabilities) and also work better for users with disabilities using "traditional" computers.
- Web Content Accessibility and Mobile Web: Making a Web Site Accessible Both for People with Disabilities and for Mobile Devices introduces the significant overlap between making a website

accessible for a mobile device and for people with disabilities. Provides a brief overview that is useful for the business case.

- Shared Web Experiences: Barriers Common to Mobile Device Users and People with Disabilities provides examples of barriers that people with disabilities and people using mobile devices experience when interacting with web content. It is organized by the principles perceivable, operable, understandable, and robust, and includes links to the relevant sections of MWBP (Mobile Web Best Practices) and WCAG (Web Content Accessibility Guidelines).
- Relationship between Mobile Web Best Practices (MWBP) and Web Content Accessibility Guidelines (WCAG) provides guidance for people who are familiar with MWBP and want to know how it relates to WCAG, or are familiar with WCAG and want to know how it relates to MWBP.
- WAI's current work related to mobile accessibility includes:
- IndieUI (Independent User Interface) - See the IndieUI Overview for an introduction and links to the in-progress specification and the Use Cases and Requirements.
- WAI-ARIA (Accessible Rich Internet Applications) - See the WAI-ARIA Overview for an introduction and links to the draft documents.
- HTML5 through the HTML Accessibility Task Force.
- WCAG techniques and other guidance for designers and developers through the Mobile Accessibility Task Force.
- UAAG (User Agent Accessibility Guidelines) material: Mobile Accessibility Examples from UAAG, and How UAAG Applies in the Mobile Context (a rough draft of Applying UAAG to Mobile Phones is available).
- A Mobile Accessibility Research Report based on the Mobile Accessibility Symposium in June 2012.
- Accessibility Support Database that will provide information on accessibility support in web technologies, including mobile devices and mobile platforms.

- Reviewing Standards for Web Applications on Mobile through the Protocols and Formats Working Group (PFWG).

5.8. Understanding Techniques for WCAG Success Criteria:

WCAG 2.0 guidelines and success criteria are designed to be broadly applicable to current and future web technologies, including dynamic applications, mobile, digital television, etc. They are stable and do not change.

Specific guidance for authors and evaluators on meeting the WCAG success criteria is provided in techniques, which include code examples, resources, and tests. W3C's Techniques for WCAG 2.0 document is updated periodically, about twice per year, to cover more current best practices and changes in technologies and tools.

The three types of guidance in Techniques for WCAG 2.0 are explained below:

- Sufficient techniques
- Advisory techniques
- Failures

Also explained below:

- General and technology-specific techniques - which can be sufficient or advisory
- Other techniques - beyond what is in W3C's published document
- Technique tests
- User agent and assistive technology support
- Using the techniques - with important considerations

Techniques are informative—that means they are not required. The basis for determining conformance to WCAG 2.0 is the success criteria from the WCAG 2.0 standard—not the techniques.

Sufficient techniques are reliable ways to meet the success criteria.

- From an author's perspective: If you use the sufficient techniques for a given criterion correctly and it is accessibility-supported for your users, you can be confident that you met the success criterion.
- From an evaluator's perspective: If web content implements the sufficient techniques for a given criterion correctly and it is accessibility-supported for the content's users, it conforms to that success criterion.

Advisory techniques are suggested ways to improve accessibility. They are often very helpful to some users, and may be the only way that some users can access some types of content.

Advisory techniques are not designated as sufficient techniques for various reasons such as:

- they may not be sufficient to meet the full requirements of the success criteria;
- they may be based on technology that is not yet stable;
- they may not be accessibility supported in many cases (for example, assistive technologies do not work with them yet);
- they may not be testable;
- in some circumstances they may not be applicable or practical, and may even decrease accessibility for some users while increasing it for others;
- they may not address the success criterion itself, and instead provide related accessibility benefits.

Authors are encouraged to apply all of the techniques where appropriate to best address the widest range of users' needs.

Failures are things that cause accessibility barriers and fail specific success criteria. The documented *failures* are useful for:

- Authors to know what to avoid,
- Evaluators to use for checking if content does not meet WCAG success criteria.

Content that has a *failure* does not meet WCAG success criteria, unless an alternate version is provided without the failure.

General techniques describe basic practices that apply to all technologies. *Technology-specific techniques* apply to a specific technology.

Some success criteria do not have technology-specific techniques and are covered only with general techniques. Therefore, both the general techniques and the relevant technology-specific techniques should be considered.

Publication of techniques for a specific technology does not imply that the technology can be used in all situations to create content that meets WCAG 2.0 success criteria and conformance requirements. Developers need to be aware of the limitations of specific technologies and provide content in a way that is accessible to people with disabilities.

In addition to the techniques in W3C's Techniques for WCAG 2.0 document, *there are other ways to meet WCAG success criteria*. W3C's techniques are not comprehensive and may not cover newer technologies and situations.

Web content does not have to use W3C's published techniques in order to conform to WCAG 2.0. (See also Techniques are Informative *above.)*

Content authors can develop different techniques. For example, an author could develop a technique for HTML5, WAI-ARIA, or other new technology. Other organizations may develop sets of techniques to meet WCAG 2.0 success criteria.

Any techniques can be sufficient if:

- they satisfy the success criterion, and
- all of the WCAG 2.0 conformance requirements are met.
- Submitting Techniques

The WCAG Working Group encourages people to submit new techniques so that they can be considered for inclusion in updates of the Techniques for WCAG 2.0document. Please submit techniques for consideration using the Techniques Submission Form.

5.9. How WCAG 2.0 is different from WCAG 1.0:

Generally, WCAG 2.0 applies broadly to more advanced technologies; is easier to use and understand; and is more precisely testable with automated testing and human evaluation. The fundamental issues of web accessibility are the same, though there are some differences in the approach and requirements between WCAG 1.0 and WCAG 2.0. Web Content Accessibility Guidelines 1.0 was

published in May 1999. WCAG 2.0 was published on 11 December 2008. W3C WAI recommends using WCAG 2.0, instead of WCAG 1.0. Most websites that conform to WCAG 1.0 should not require significant changes in order to conform to WCAG 2.0, and some will not need any changes at all. For those familiar with WCAg 1.0, it will take a little time to learn the new approach of how the WCAG 2.0 documents provide guidance.

5.10. Authoring Tool Accessibility Guidelines (ATAG):

Authoring Tool Accessibility Guidelines (ATAG) Overview: Authoring tools are software and services that "authors" (web developers, designers, writers, etc.) use to produce web content (static web pages, dynamic web applications, etc.). Examples of authoring tools are listed below under "Who ATAG is for".

The Authoring Tool Accessibility Guidelines (ATAG) documents explain how to:

- make the authoring tools themselves accessible, so that people with disabilities can create web content, and
- help authors create more accessible web content — specifically: enable, support, and promote the production of content that conforms to Web Content Accessibility Guidelines (WCAG).

ATAG is part of a series of accessibility guidelines, including the Web Content Accessibility Guidelines (WCAG) and the User Agent Accessibility Guidelines (UAAG). Essential Components of Web Accessibility explains the relationship between the different guidelines.

ATAG is primarily for developers of authoring tools, including the following types of authoring tools:

- web page authoring tools, for example, what-you-see-is-what-you-get (WYSIWYG) HTML editors
- software for generating websites, for example, content management systems (CMS), courseware tools, content aggregators
- software that converts to web content technologies, for example, word processors and other office document applications with "Save as HTML"
- multimedia authoring tools

- websites that let users add content, such as blogs, wikis, photo sharing sites, online forums, and social networking sites
- other types of tools listed in the glossary definition of authoring tools
- ATAG and supporting resources are also intended to meet the needs of many different audiences, including policy makers, managers, and others. For example:
- People who want to choose authoring tools that are accessible and that produce accessible content can use ATAG to evaluate authoring tools.
- People who want to encourage their existing authoring tool developer to improve accessibility in future versions can refer the authoring tool vendor to ATAG.

ATAG 2.0 is currently a W3C "Candidate Recommendation". (These stages are explained in How WAI Develops Accessibility Guidelines through the W3C Process.) To move ATAG 2.0 to the next step toward a final W3C Recommendation, WAI is asking for submission of technical feedback from authoring tool developers. You can help in two ways:

1. Implement one or more ATAG Success Criterion If you create or customize authoring tools (see Who is ATAG For), submit an example of your authoring tool to show how the tool meets ATAG2.0. While conformance to all of the applicable success criteria will be required when ATAG becomes a final W3C Recommendation, it is not necessary to claim conformance to all of the ATAG 2.0 success criteria for this stage. You may choose which ones to submit for testing during this Candidate Recommendation stage in order to verify the implementation of specific success criterias.
2. Test for ATAG 2.0 conformance: We need volunteers with accessibility testing experience to use the WAI test process to validate that the submitted examples actually do meet ATAG.

ATAG technical documents are developed by the Authoring Tool Accessibility Guidelines Working Group (AUWG), which is part of the World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). For more information about the working group, see the AUWG page.

5.11. Summary:

This unit is related to web content and its accessibility guidelines globally. In this regard there is no change in domestic and international norms in general. This concept is also very complex in nature and required full attention with technical expertise on the topic. In this unit the concept of who WCAG for, what is WCAG 2.0, component of web accessibility, user agent accessibility guidelines, who develops WCAG, WCAG2.0 coverage of mobile accessibility, understanding various techniques of WCAG and success criteria, how WCAG2.0 is different from WCAG1.0 and authority tool accessibility guidelines are discussed at length for better understanding and application.

5.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)

- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI **Publication)**
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

5.13. Check your Progress:

A. Which of the following statements are true or false:

a) The WCAg documents explain how to make web content more accessible to people with disabilities.

b) Four areas of accessibility perceivable, operable, understandable and robust.

c) WCAG2.0 is an approved ISO standard.

d) The UAAG documents explain how to make user agents accessible to people with disabilities, particularly to increase accessibility to web content.

e) WCAG covers web pages and application, including content used on mobile devices.

B. Fill in the Blanks:

i. WCAG is a ……, not an introduction to accessibility.

ii. WCAG2.0 is a ……, referenceable technical standards.

iii. WCAG means ……..

iv. ATAG means……

v. ATAG tools are ……..

5.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Technical standards
2. Stable
3. Web Content Accessibility Guidelines
4. Authority Tools Accessibility Guidelines
5. Software and Services

5.15. Terminal Questions:

1. What is WCAG2.0?
2. Who develops WCAG?
3. What is User Agent Accessibility Guidelines?
4. What are essential component of Web Accessibility?
5. How WCAG2.0 is different from WCAG1.0?

Unit-6

Cyber Warfare on Privacy and Identity Theft

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Cyber Warfare on Privacy and Identity Theft
- Understand the remedies which are available against Cyber Warfare on Privacy and Identity Theft
- Understand the technical and legal issues related to Cyber Warfare on Privacy and Identity Theft

Structure:

6.1. Introduction:

The term identity theft was coined in 1964; however, it is not literally possible to steal an identity — less ambiguous terms are identity fraud or impersonation — terms which tend less toward emplacement of onus upon the impersonated person and which tend more toward emplacement properly of the onus upon the victim and the perpetrator of fraud. "Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained," and identity theft is not always detectable by the individual victims, according to a report done for the FTC. Identity fraud is often but not necessarily the consequence of identity theft. Someone can steal or misappropriate personal information without then committing identity theft using the information about every person, such as when a major data breach occurs. A US Government Accountability Office study determined that "most breaches have not resulted in detected incidents of identity theft". The report also warned that "the full extent is unknown". A later unpublished study by Carnegie Mellon University noted that "Most often, the causes of identity theft is not known," but reported that someone else concluded that "the probability of becoming a victim to identity theft as a result of a data breach is ... around only 2%". More recently, an association of consumer data companies noted that one of the largest data breaches ever, accounting for over four million records, resulted in only about 1,800 instances of identity theft, according to the company whose systems were breached.

Identity theft is one of the growing concerns in cyber crime in India today. According to Norton Cybercrime Report 2011, globally 431 million adults experienced cybercrime in 2011 and more than 1 million plus adults became victims every day. As per the report, India is fast emerging as a soft target for organized cybercrime with four in five online adults have been victims of identity theft in 2011. Identity theft can have serious financial implications. "Credit and Debit cards can be applied for in the name of another individual. Fraudulent bank loans could be taken out in the name of the victim. Even a multiple range of debts can be incurred in victim's name," says Ian Craig, Managing Director, CPP India.

6.2. Identity Theft: The Growing Crime:

Identity theft is widely considered to be the fastest growing crime in the world. The rapid growth of identity theft is due to multiple ways in which the ways we live our lives and process information have been changed. All of these changes make it easier for others to access our personally identifying information and ultimately take hole of our identities. The internet has made transmission of our personally identifying information quick and easy, and sometimes less secure. We can access band and credit card accounts online, pay bills online, and shop and make credit card transactions online. All of these processes make things quicker and more convenient, but they also pose risks to our personal information. Individuals can create spyware that is installed on our computers when we install freeware or other programs off the internet. This spyware can collect information about what sites we are going to, what passwords we are using, and what information we are transmitting, and then send it to someone else. This person can then use our personal information himself or sell it to someone else. Certain types of spyware called "Trojan horses" can even allow their inventors remote access to our computers and hard drives. When we make online credit card transactions, online retailers store our contact and credit card information in databases we assume to be secure. Marketing agencies collect information on out spending habits as well as contact information and personal information. This is stored in databases we assume to be securing as well. However, malicious employees of these types of companies may have access to our information. They may be bribed to give out our information or they may even take this information for their own use or sell it to others. Postal mail poses a threat as well. Credit card companies overflow customers and potential customers with pre-approved credit cards and courtesy checks meant to be used in place of the customer's credit card. If this mail is not opened and destroyed (preferably using a shredder) properly, identity thieves can rummage through your trash and take your credit for their own use. In the United States, social security numbers are also being used as a means of personal identification more commonly than in the past. And the more these valuable identifiers are used, the easier it is for someone to get a hold of yours and use it for himself.[19]

[19] http://www.spamlaws.com/id-theft-history.html

Identity theft or identity fraud (true name fraud) is the taking of the victim's identity to obtain credit, credit cards from banks and retailers, steal money from the victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy or obtain a job using the victim's name. The Impersonator steals thousands of rupees in the victim's name without the victim even knowing about it for months or even years. Recently criminals have been using the victim's identity to commit crimes ranging from traffic violations to grave crimes. Lots of places have knowledge about ones identity. – For example: personal doctor, accountant, lawyer, dentist, school, place of work, health insurance and many others have ones identity information. If some criminally minded person is working at the office (or just visiting) decides to use this information to assume a person's identity, he would not know it.

It is easy to impersonate another if the information's about the victim are ready. In some case all that is needed is the date of birth and other identifying information such as address and phone numbers and whatever else they can find out about him. With this information, and a false driver's license with their own picture, they can begin the crime. They often provide an address of their own, claiming to have moved. Negligent credit grantors in their rush to issue credit do not verify information or addresses. So once the imposter opens the first account, they use this new account along with the other identifiers to add to their credibility. This facilitates the proliferation of the fraud. Now the thief is well on his/her way to getting rich and ruining another person's credit and good name. You will need a report to clean up the credit mess. As soon as a person is made aware of the fraud he must immediately note the fraud in accounts, put a fraud alert on his credit profile, and contact l the police in the country where the fraud occurs. One may not be able to stop the fraud immediately. It is very complex. But this will get him started. Identity Theft occurs when someone wrongfully uses another person's identification to obtain credit, loans, services, even rentals and mortgages in his name. This type of crime is common in bank business field. The sureties/guarantors are usually impersonated for the purpose of the loan. The

salary certificate of the employees is also personated for loan. Identity Theft is a frightening and overwhelming experience if it does happen to anybody.[20]

Identity theft- Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased. If you're a victim of identity theft, it can lead to fraud that can have a direct impact on your personal finances and could also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved.

Identity fraud: Identity fraud can be described as the use of that stolen identity in criminal activity to obtain goods or services by deception. Fraudsters can use your identity details to:

- Open bank accounts.
- Obtain credit cards, loans and state benefits.
- Order goods in your name.
- Take over your existing accounts.
- Take out mobile phone contracts.
- Obtain genuine documents such as passports and driving licences in your name.
- Stealing an individual's identity details does not, on its own, constitute identity fraud. But using that identity for any of the above activities does.

Sources such as the non-profit Identity Theft Resource Center sub-divide identity theft into five categories:

- Criminal identity theft (posing as another person when apprehended for a crime)
- Financial identity theft (using another's identity to obtain credit, goods and services)
- Identity cloning (using another's information to assume his or her identity in daily life)

[20] http://www.lawyersclubindia.com/articles/IDENTITY-THEFT-IN-CYBER-SPACE-232.asp#.VKPPzdKUfVs

- Medical identity theft (using another's identity to obtain medical care or drugs)
- Child identity theft.

Identity theft may be used to facilitate or fund other crimes including illegal immigration, terrorism, phishing and espionage. There are cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

6.3. Invasion of Privacy:

These are the contours of the privacy right. Naturally, it is not absolute, and the Court has taken pains to specify that on numerous occasions. What, then, justifies an infringement? The Court has consistently called for a "*compelling State interest*", one that rises beyond the simple "*public interest*" encoded in the 19 restrictions. Side-by-side with compelling State interest, the Court has also required – although it has never expressly spelt it out – the restrictive law to be *narrowly tailored*. In other words, the government must show that its infringing law not only achieves the compelling State interest, but does so in a way that restricts privacy in the narrowest possible manner. If there are other conceivable ways of achieving the same goal that do not infringe upon privacy to the extent the impugned law does, the law will be struck down. We see this in the police surveillance cases, where in *Gobind*, for instance, the Court read into Regulation 855 an additional requirement of gravity, to ensure that it was narrowly tailored; and we see it even more clearly in the phone-tapping cases, where the Court's rules require not only specification of persons, numbers and addresses, but also require the State to resort to surveillance only if other methods are not reasonably open, and in so doing, to infringe privacy minimally. Targeting, indeed, is critical: all the surveillance cases that we have explored have not only involved specific, targeted surveillance (indeed, S. 5(2) of the Telegraph Act only envisages targeted surveillance), but the very fact that the surveillance is targeted and aimed at individuals against whom there are more than reasonable grounds of suspicion, has been a *major – almost dispositive – ground* on which the Court has found the surveillance to be constitutional. Targeting, therefore, seems to be an integral aspect of narrow tailoring.

The very legitimate concern that creating a private sphere only serves to justify relations of non-State domination and oppression within that sphere – both symbolically, and actually (see, for instance, the infamous marital rape exception in Indian criminal law). It presumes – instead of arguing for – the basic philosophical idea of the ultimate unit of society being indivisibly, atomized individual selves living in hermetically sealed "zones" of privacy, an assumption that has come under repeated attack in more than fifty years of social theory. I hope to explore these arguments another day, but the purpose of this series has been primarily doctrinal, not philosophical: to look at surveillance in the framework of established constitutional doctrine without questioning – at least for now – the normative foundations of the doctrine itself.

6.4. Identity Theft under Indian Law:

Under The IT Act, 2000 as amended by Information Technology (Amendment) Act, 2008, Section 66-C is applicable and Section 419 of Indian Penal Code, 1860 is applicable. The victim of identity theft can file a complaint in the nearest police station where the above crime has been committed or where he comes to know about the crime. If crime is proved accused shall be punishable with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. As per Section 77-B of IT Act, 2000 the above offence shall be cognizable and bailable while if Section 419 of IPC is applied along with other Section s the said offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Section 66C of the Information Technology Act, 2000 (Amended in 2008) is Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 419 in The Indian Penal Code, 1860: Punishment for cheating by personation.—whoever cheats by personation shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

Section 420 IPC, 1860: When the fraudster deceive people into disclosing valuable personal data in the nature of identifiable information which is used later to swindle money from victim account.

Section 468 IPC, 1860: When the fraudster commits forgery of website which is in the nature of electronic record to lure the victims to pass their identifiable information in order to cheat them.

Section 471 IPC, 1860: When fraudster fraudulently or dishonestly uses as genuine, the aforesaid fake website in the nature of electronic record.

Section 66 IT Act, 2000: When the fraudster by the stolen identifying information say login id & password, deletes or alter the information or data in the account of the victim in the server which is a computer resource.

Section 67 IT Act, 2000: When the fraudster uses the stolen information like profile, personal details & contact details of the victim to create & post obscene profile in the name of the victim on the social networking site.

6.5. Stages of Identity Theft:

There are three stages of identity theft. Any identity theft case may include one or all of these stages:

Acquisition of the identity: It involves the acquisition of the identity through theft, hacking, redirecting or intercepting mail or by purchasing identifying information on the internet.

Use of the identity: After the acquisition of the identity, the fraudster may use the identity to commit another crime resulting in financial gain to him like misuse of the credit card information to make online purchase, opening new accounts, sell the identities to others who commit fraud. Sometime the stolen information may be used to harass the victim, like posting of pornography or obscene material by fraudster posing himself as the victim.

Discovery of the theft: Many cases of misuse of credit cards are discovered quickly, however in some cases the victim of an identity theft may not even know how or when their identity was stolen and theft may take 6 months to several years to come to the notice of the victim. Study reveals that the longer it takes to discover the theft, the greater the loss incurred by the victim.

What Are The Common Ways To Commit Identity Theft Crime?

The various ways prevalent to commit the identity theft crime which makes use of internet or the virtual world and other which does not, known as traditional methods. Some of the ways to commit the identity theft crime which is not exhaustive are as follows:

Theft: There may be a theft of your wallet or bag containing bank credit cards, passport other identifying documents containing your vital personal information.

Hacking, unauthorized access to systems, and database theft : The fraudsters frequently compromise systems, diverting information directly or indirectly with the help of gadgets on the network. Hackers gain access to a huge base of confidential data, decrypt it and misuse the same elsewhere for financial gain or commit fraud.

Phishing: Phishing is the most prevalent method to steal the personal identifying information. The fraudster sends a fraudulent email with a link to a fake website that is exact replica of the original bank sites which are so designed to fool the users so that they reveal their personal information.

Vishing: It is the act of calling a victim on the phone by the fraudster posing as the bank representative in an attempt to scam victim users into disclosing personal information.

Pharming: It is a technique used by fraudster to by setting up a phony web server and intercepting user names and PIN numbers.

Nigerian 419 Scam: This is the most prevalent method still conning many persons around the globe wherein the fraudster sends the email to target persons in guise of some rich family member of a dead African Millionaire who is in distress due to political turbulence in his country. The fraudster seeks your help to get the large sum of money in your account with a commission of huge money to you for your services of offering your account to receive the money. This scam is called as Nigerian 419 fraud (for the relevant section of the Nigerian Criminal Code). There is another category of Nigerian fraud of similar nature where the victim receives unsolicited email declaring that he has won the lottery after his email being selected from thousands of other emails. These scams qualify as identity crimes because they involve collecting personal and bank information from unsuspecting Internet users who are gullible enough to respond to these solicitations.

Theft by past & present employees: Perpetrators can also obtain personal information by bribing employees who have access to personal records, data bases or confidential information.

Skimming: Skimming can occur when a criminal attaches a small skimmer gadget to an ATM which records the magnetic stripe details of the ATM card and the camera films the personal identification number filed by the user.

Shoulder Surfing: The fraudster can also obtain your personal data without breaking into your homes. In public places, some people loiter around ATM & Telephone Booths who watch your enter your secret PIN Number or simply looking over your shoulder on a public telephone or just by eavesdropping if you are giving your credit card information over the phone.

Dumpster Diving: It is a method perpetrators use by going through a victim's garbage, dustbins or trash bins. They obtain copies of cheques, credit card statements, bank statements, receipts, and carbons and search for anything bearing your name, address, telephone number, and credit card number[21].

6.6. Case Study: Stuxnet, June, 2009:

The Stuxnet virus that ravaged Iran's Natanz nuclear facility "was far more dangerous than the cyber weapon that is now lodged in the public's imagination," cyber security expert Ralph Langer tells Foreign Policy. Stuxnet, a joint U.S.-Israel project, is known for reportedly destroying roughly a fifth of Iran's nuclear centrifuges by causing them to spin out of control. But the exploit had a previous element that was more complicated and "changed global military strategy in the 21st century," according to Langer. The lesser-known initial attack was designed to secretly draw "the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control" the centrifuges used to enrich uranium, Peter Sanger of The New York Times reported last June. Langer adds that the worm also subtly increased the pressure on spinning centrifuges while showing the control room that everything appeared normal by replaying the plant's protection system values while the attack occurred. The goal of the worm was not aimed at destroying centrifuges, but "reducing lifetime of Iran's centrifuges and making the Iranians' fancy control systems appear beyond their understanding," Langer writes.

[21] http://www.neerajaarora.com/identity-theft-or-identity-fraud/

He notes that the coding was "so far-out, it leads one to wonder whether its creators might have been on drugs." (The worm was reportedly testedat Israel's Dimona nuclear facility.) . Only after years of undetected infiltration did the U.S. and Israel unleash the second variation to attack the centrifuges themselves and self-replicate to all sorts of computers.

The second Stuxnet is considered the first cyber act of force, but the new details reveal that the impact of the first virus will be much greater. That's because one of the most innovative aspects of the initial virus was how it was delivered into Natanz through a worker's thumb drive, thereby taking advantage of the weakest link: humans. From Foreign Policy: The sober reality is that at a global scale, pretty much every single industrial or military facility that uses industrial control systems at some scale is dependent on its network of contractors, many of which are very good at narrowly defined engineering tasks, but lousy at cyber security. Or as one of the architects of the Stuxnet plan told Sanger: "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand." Given that the next attackers may not be nation-states, they may be much more likely to go after civilian critical infrastructure. Langer notes that most modern plants operate with a standardized industrial control system, so "if you get control of one industrial control system, you can infiltrate dozens or even hundreds of the same breed more."[22]

6.7. Case Study-I:

Charu Singh (name changed), an aspiring airhostess, was aghast when her boyfriend broke up with her. What triggered the split was — someone hacked into her Facebook account and sent nasty messages about her. She filed a case at the Gurgaon Cyber Crime Cell and a subsequent probe proved that her roommate was the culprit. According to police, this is not just a one-off case. There has been an alarming spurt in cases of identity theft — stealing someone's personal details in order to access resources or obtain credit or other benefits in that person's name or misuse the victim's details for nefarious purposes — in Gurgaon.

[22] http://www.businessinsider.in/The-Stuxnet-Attack-On-Irans-Nuclear-Plant-Was-Far-More-Dangerous-Than-Previously-Thought/articleshow/26113763.cms

Till August this year, 70 identity theft cases have been registered with the city Cyber Crime Cell against 40 reported last year. In most of the cases, conmen access accounts of individuals on various social networking sites such as Facebook, Twitter and Orkut and retrieves their photos and other information and uses the same for making fake driving licences, applying for telephone connections, opening bank accounts and making PAN cards and credit cards. In today's digital age, your personal information such as name, date of birth, address, phone number, email ID are easily accessible online and offline.

Such easily available information can be misused by conmen. With these bits information, a fraudster can procure a phone connection or a credit card pretending to be you. One does not get to know until one gets a statement from the service provider. But by then the damage would have been done. Police admitted that in many cases victims do not come forward to file a case. In some cases, victims take back their complaints once they come to know that people close to them had committed the crime. Inspector Suresh Singh, Cyber Crime Cell in-charge, said, "Victims often withdraw their complaints as most of the accused are known ones. Many students do not realise when they use webcams to interact with their friends who often record the videos." Recently, a student had complained about her fake Facebook account complete with her personal details. Later, it was discovered the accused was her former boyfriend. In August, Ekta Nath, (name changed) an engineering student, filed a case after her intimate video with her ex-boyfriend was launched on a porn site. Police later arrested her ex-boyfriend for the crime.[23]

6.8. Case Study-II:

Online fraudulent share & commodity transactions: Now a day the shares are sold and purchased online. There has been spurt in the cases in which the complainant report that there online share/commodity account has been compromised and fraudulent transactions has been executed by unknown fraudster which resulted in huge loss to him. In the online transaction, the client is allotted an online account with client id & password through which he executes the sale & purchase transactions through the server based in the broker office. The fraudster who are

[23] http://www.hindustantimes.com/india-news/gurgaon/identity-theft-cases-on-the-rise/article1-931638.aspx

generally software experts or the executives (core dealers) at the broker office try to acquire the client id & password from the broker office itself, hit & trial methods or social engineering. After acquiring the client Id & password, the fraudster makes unauthorized access to the client account and also accesses their own account in which the profits are to be transferred from the victim client account. The fraudster executes the transactions into the client accounts at unrealistic prices and match these transactions into their own account simultaneously. In this way, he shifts the profit to his own account and losses to the account of the unsuspecting clients.

Bank Phishing scams: Phishing is the Internet's biggest identity theft scam and is widely prevalent in India. In some recent cases of phishing (offence which involves identity theft) reported in India, the MO was same i.e. a fake target Bank Web site was created and the bank customers received an e-mail message asking them to renew certain services claiming that failure to do so would result in the suspension or deletion of their accounts. The e-mail provided a link to a phishing site, in an illegal attempt to collect personal and account information

Nigerian 419 Scam or Advance Fee Fraud: There has been number of cases reported where the perpetrators of the fraud send mail to the victim e-mail id, requesting the help of the victim for retrieving blocked funds and offer a healthy percentage of these funds as commission. The victim believing the fraudster in lure of receiving huge funds pass on his credit card information, bank account details to fraudster.

Defamation or posting of porn or obscene material on social networking sites: There has been also spurt of cases in which the victim have reported that their profile and personal information has been stolen and a fake & vulgar profile in his or her name containing pornography & obscene material along with the victims contact details like phone numbers & address has been posted on the social networking site like ORKUT.[24]

6.9. Case Study-III:

Majority of the banks in India have migrated to online and mobile banking. Most of the transactions are conducted via payment cards, debit and credit cards, and

[24] http://www.neerajaarora.com/identity-theft-or-identity-fraud/

electronic channels such as ATMs. Consequently, both private and public banks, as well as financial institutions in India are becoming increasingly vulnerable to sophisticated cyber attacks. According to the RBI, 8322 cases of cyber frauds were reported in 2012 amounting to 527 million INR. Although the number of cases reported has decreased from 15018 cases reported in 2010, the amount involved in such cases has increased from 405 to 527 million INR in 2012 implying that the average value per cyber fraud case has increased significantly. One of the most common forms of cyber attacks relating to banks is phishing, a financial scam in which fraudsters use social engineering techniques and spyware or malware codes to steal confidential financial and personal information of customers such as bank account numbers, credit card numbers, internet banking passwords, etc. These details can also be used for siphoning money off customers' bank accounts, a loss that has to be ultimately borne by the banks themselves. Typical phishing attacks involve sending emails messages to customers containing logos or images impersonating to be financial institutions. These emails usually contain a web link which is a malicious web page that looks exactly like the financial institution's webpage. Majority of these attacks are done for financial gain.

One in four phishing attacks used the .IN domain and involved targeting the bank balances of customers. Although these attacks originated from all over the world, Hyderabad hosted the second highest number of phishing attacks in the country. Interestingly, emerging cities such as Chandigarh, Bhubaneswar, Surat, Cochin, Jaipur, Vishakhapatnam and Indore are also experiencing phishing attacks.[25]

Credit cards have always been one of the biggest targets for cyber criminals; the most common form of credit card frauds involves skimming. With the rapid increase in the use of plastic money, India is witnessing a tide of skimming frauds. Skimming is a hi-tech forgery that involves copying of customer and card information stored on the magnetic strip of a credit card, including the CVV number, by using an electronic device known as the 'skimmer'. When the credit card is swiped through such a device, it reads and captures the information stored on the credit card. This information is used by the fraudster to create a cloned card which can then be used to make unauthorised and fraudulent transactions. Skimming frauds are extremely difficult to detect as the credit card is not actually

[25] http://www.pwc.in/en_IN/in/assets/pdfs/publications/2013/invading-privacy-cyber-crimes-on-the-rise.pdf

stolen or reported. The customer to whom the card belongs becomes aware of the fraud only when a transaction is made using the cloned cards. The number of credit card frauds is increasing despite the various proactive measures taken by Indian banks to set up internal control systems to mitigate frauds relating to skimming or cloning of credit cards. As per the RBI statistics, in the quarter ended December 2012, there were 1590 cases of credit card reported involving an 94.86 million INR as compared to 1327 cases reported in the quarter ended September 2012 involving 49.29 million INR.

The two most common types of skimming attacks occur at the following locations:

- ATMs
- PoS (point of sale), either by employees who use handheld skimming devices or fraudsters who swap PoS devices with devices that have been manipulated to capture unauthorised card information. e.g., swiping credit cards at restaurants or petrol pumps.

Example-I: In May 2012, the RBI warned against fraud emails from mail id: alert@rbi.org. The mails were sent by unscrupulous entities offering a new online security platform and asking customers to share information. According to the mail, the new online security platform offered to prevent online identity theft in internet banking. The email further asked the recipient to download attachment and update their information. The RBI cautioned the public not to open such emails or try to download the attachment on their computer. (Source: The Economic Times)

Example-II: In April 2012, an Indore-based gang of fraudsters involved in phishing the accounts of customers across the country of two leading banks in India were busted. The gang had opened fictitious accounts in their names in at least two dozen different banks in the city. These accounts were utilized to siphon off the money from the account holders of these banks through phishing. The money was later withdrawn from the fictitious account through ATM or cheques. The accused have been booked under section 419, 420 IPC and 66 IT Act.(Source: The Times of India)

Example-III: In January 2013, two residents of Chandigarh received credit card bills for shopping done in Mumbai and Hyderabad. The money was deducted from their accounts before they could even approach the bank. People are losing money by making payments at petrol pumps in Chandigarh city. Nearly 55 cases of

skimming have been reported from petrol pumps in Chandigarh over the last six months. In these cases, miscreants cloned the cards and shopped at faraway places such as Mumbai and Hyderabad. The scam is worth lakhs. (Source: The Times of India)

Example-IV: In April, 2012, a gang of fraudsters were arrested in Hyderabad for skimming and cloning credit and debit cards using a complex modus operandi of hacking international IP addresses, internet hawala, and spying and electronic data theft. The racket came to light in May 2011 when people who visited two malls complained that huge amounts were withdrawn from their accounts. The gang succeeded in skimming off 4 to 5 crore INR from unsuspecting credit and debit card holders across the country — from Hyderabad to Delhi, Kolkata to Bangalore. They used 15 point of sale (electronic draft capture) skimming machines, one ATM data skimming machine, ATM dome cameras, electronic magnetic writers, card printers and ATM pin pad skimmer machines and even placed spy cameras at ATMs which picked up the PINs of users. (Source: The Indian Express)

6.10. Tips to prevent Identity Theft:

- To guard against identity theft, never give out your Social Security number. Treat it as confidential information.
- Commit all passwords to memory. Never write them down or carry them with you.
- When using an ATM machine, make sure no one is hovering over you and can see you enter your password.
- When participating in an online auction, try to pay the seller directly with a credit card so you can dispute the charges if the merchandise does not arrive or was misrepresented. If possible, avoid paying by check or money order.
- Adopt an attitude of healthy skepticism toward websites that offer prizes or giveaways. Chances are, all that's been "won" is the opportunity to buy something you didn't want in the first place.
- Choose a commercial online service that offers parental control features.

- Tell your children never to give out their address telephone number password school name or any other personal information.
- Make sure your children know to never agree to meet face-to-face with someone they've met online without discussing it with you. Only if you decide that it's okay to meet their "cyber-friend" should they arrange to meet this person, and then the meeting should be in a familiar public place in the presence of a trusted adult.
- Tell your children never to respond to messages that have bad words, are scary, or just seem weird.
- Tell your children never to enter an area that charges for services without asking you first.
- Tell children never send a picture of themselves to anyone without your permission.
- Make sure that access to the Internet at your children's school is monitored by adults.
- In other words the following tips to avoid being a victim of fraud:

1) Be vigilant: This is perhaps the most important piece of advice to give to individuals concerned about identity theft. Be aware of unsolicited phone calls or emails, particularly those asking for details such as passwords and account details.
   If you receive communications claiming to be from a bank or other financial institution, always check they are legitimate. If not, you should report any suspicious activity to the company or to the police.
   2. Never share confidential information: Confidential data should be exactly that, confidential. Keep information, such as pin numbers, bank account details and passwords, to yourself. Make sure that you have different pin numbers and passwords for different accounts and services. By doing so, you will ensure that if one of these is compromised, then the impact will be limited to one account.
   3. Check your bank statements: This is something that many of us neglect to do, but checking the dreaded bank statement could help you to stop identity theft before it becomes serious. Check carefully for any suspect

transactions and, if you are unsure about any of these, consult your bank.

4. Shred personal information: Never throw away personal and financial information without shredding it first. Many fraudsters engage in a process known as 'bin raiding' in order to acquire personal details, which can be used to steal your identity. You can avoid compromising your details by shredding documents before you throw them away.

2) Keep important documents safe: Keep important documents, such as your passport and driving licence, safe and secure when you don't need them. Don't carry credit cards and cheque books around with you unless absolutely necessary.[26]

Summary:

Cyber warfare on privacy and identity theft is very debatable issue worldwide. In this unit the various important case studies are incorporated for better understanding and practical application. In this unit the concept of identity theft as the growing crime worldwide, invasion of privacy, Indian theft under India Law, stages of identity theft and other concept are discussed in a proper academic fashion to explain in a easy and simple language. The case study of Stuxnet is discussed at length in particular to understand foreign position on this very complex issue.

6.11. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)

[26] https://www.red24.com/press/idtheftassistance.php

- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)

- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

6.12. Check your Progress:

A. Which of the following statements are true or false:

a) The term identity theft was coined in 1964.

b) Identity theft is one of the growing concerns in cyber crime in India today.

c) There are three stages of identity theft.

d) Skimming can occur when a criminal attacks a small skimmer gadget to an ATM.

e) The Stuxnet is a virus that ravaged Iran's Natanz Nuclear Facility.

B. Fill in the Blanks:

i. Identity theft or identity fraud is the taking of the victim's identity to ……., steal money from the victim's ……..etc.

ii. Identity theft happens when fraudsters access enough information about someone's identity to commit……

iii. ……..of the Information technology Act, 2000 is related to Identity Theft.

iv. …….of the Indian Penal Code, 1860 is related to Identity Theft punishment.

v. …….of the IPC is related to when the fraudster fraudulently or dishonestly uses as genuine, the fake website in the nature of electronic record.

6.13. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True

5. True

B.

1. Obtain Credit, Existing Account
2. Identity Fraud
3. Section 66-C
4. Section 419
5. Section 471

6.14. Terminal Questions:

1. What are the common ways to commit identity theft crime?
2. What is identity theft?
3. Discuss in detail the identity theft under the Indian law.
4. Discuss the case study of Stuxnet.
5. Discuss in detail the two case studies related to identity theft.

Unit-7

International Law Governing Censorship

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to International Law Governing Censorship
- Understand the various norms and rules related to Censorship Worldwide
- Understand the technical and legal issues related to Censorship

Structure:

7.1. Introduction:

Internet censorship in India is selectively practiced by both federal and state governments. While there is no sustained government policy or strategy to block access to Internet content on a large scale, measures for removing content that is obscene or otherwise objectionable, or that endangers public order or national security have become more common in recent years. However, websites blocked either by the government or Internet service providers can often be accessed through proxy servers. The Internet provides important and unimportant information to millions of people all around the globe. But if we search for the same information in China and in the Czech Republic, data found may differ, because of censorship. Internet censorship is the control of information on the Internet. In the past, information was also censored. There was and there is censorship of press, radio, books, music, films and many others. Books were burned during Pinochet regime in Chile in 1973, because they included unsuitable information for regime. In some countries, there is censored almost everything, in others just a little, for instance just a racist stuff. On the Internet censorship some government may control publishing of articles that are not suitable for them, or suppress web pages they do not like. A country may increase the Internet censorship due to events like Arab Spring. Internet censorship is very specific, because it has many distinctions from other media it is a decentralized medium. It is interactive, so readers can write comments, for instance. There are almost no state borders on the Internet and we can read information from very distant countries. Who should have the right to censor the Internet? What should be censored? In the addition, the legal relationship between censors, website owners, users and internet connection providers is very complicated.

7.2. Internet Censorship:

The recently published Freedom on the Net 2012: A Global Assessment of Internet and Digital Media report by Freedom House, an independent watchdog organisation, highlighted the increasing trend of censoring the web across the world. Out of the 47 countries it surveyed, it discovered that as many as 19 countries have since 2011 adopted policies to censor the web, which effectively hampers online speech. While it found Estonia with the greatest degree of Internet freedom, countries like Iran, Cuba and China were found to be on the other

extreme. Governments of many countries are playing the Orwellian script by introducing draconian laws to censor the web. Let's take a look at Internet censorship followed in some countries that drew lot of attention in the past year.

Since the past couple of years, the instances of Internet censorship in India has increased manifold. In 2011, India adopted the new 'IT Rules 2011' that supplemented the IT Act 2000. These rules made it mandatory for Internet intermediaries to remove objectionable content within 36 hours of receiving complaint. But the terms included were vague and open to interpretations. These rules received sharp criticism, but they have prevailed. In 2011, government also drew flak as it asked major sites like Google, Facebook and Yahoo to 'pre-screen' content and remove any objectionable, defamatory content from going live. It was alleged that the government urged the Internet companies to use human beings and not machines to do the needful. Later in 2012, these companies were dragged to court of law over the same. The Internet companies on their part stood their ground and refused to comply with these terms. However, the **Google Transparency Report** points out to the increased request from government to take down objectionable content and even seek information pertaining to users account. We witnessed numerous instances of attempts to censor Internet right from arrest of cartoonist Aseem Trivedi and blocking of this site to blocking of sites by ISP over concerns of privacy, suspension of Twitter accounts allegedly for fanning rumours during the recent Assam violence and even arrests over posts on social networking sites. While India falls under 'partially free' category, when it comes to Internet freedom, the increasing attempts of surveillance and censorship have raised concerns amongst the Internet watchdog agencies around the world.

7.3. Censorship Through Blocking:

United States of America – a country that has witnessed widespread protest against bills that seeked to curb Internet freedom – remains largely free from Internet censorship as is seen and practiced in countries around the world. We have witnessed the highly publicized battle against controversial bills like Stop Online Piracy Act (SOPA), Anti-Counterfeiting Trade Agreement (ACTA), Cyber Intelligence Sharing and Protection Act (CISPA), PROTECT IP Act (PIPA). These laws, if they had come into effect, would have had an impact not only in the US,

but also many other countries of the world. Anti-SOPA movement in particular garnered support from popular sites like Google, Wikipedia, Reddit, Mozilla etc. as they blacked-out their sites for 24 hours. Vigilant netizens and pro-Internet activists ensured that these bills didn't become a reality.

What may play a role is the presence of Silicon Valley and the fact that US happens to be the home of all the major tech companies of the world. Economic concerns ensure that these tech giants have a say in the proceedings. However, there have been increased monitoring of social networking sites in the recent years. For instance, micro blogging site Twitter was issued requests to access personal data of users, particularly those associated with organisations like WikiLeaks and even the Occupy Wall Street movement. Another incident that created quite a furore and received flak was The New York Police Department's initiative to monitor online activities of Muslim student groups, which according to reports was underway since 2006.

Egypt: The role of Internet in aiding revolution came forth during the civil unrest in Egypt, as the country took to streets in a bid to end the 30-year long tyrannical regime of its President Hosni Mubarak. What came to the aid of the common man waging the war against the authorities was the anonymity provided by the Internet, as it was being thoroughly used as a tool to spread information about the on-ground activities, rally supporters and most importantly, bringing to the world the voices against the atrocities of the regime. Of course, the government was quick on its toes and did attempt to block the Internet, but was largely unsuccessful in doing so. Internet played such a crucial role in the revolution that the Egypt revolution was popularly dubbed as Facebook Revolution. A Google employee Wael Ghonim, who founded a Facebook page condemning the death of an Egyptian youth at the hands of the police, became the face of the revolution. He was arrested by the authorities as he urged people to join the revolution via social networking. His arrest and subsequent release garnered media attention around the world. It garnered more support for the revolution and built pressure on the Egyptian authorities. Post the revolution, the current military administration is taking no chances. It maintains control over the Internet and social media in particular. It has in place monitoring tools to keep a check on the online activities of its netizens. Several cases of online activists and bloggers facing the wrath of the authorities have come forth in the past year. Another effect of the Egypt revolution is that it

has led to increased censorship on the Internet by governments of many of the Middle Eastern countries like Saudi Arabia.

Pakistan: India's neighbor Pakistan is also reeling under increased instances of Internet censorship. Incidents of blocking sites are on the rise. While most of the clampdown has been against pornographic content on the web, increasingly, it has also been done to block sites that pose no apparent threat and seem politically motivated. For instance, it blocked the website of a popular magazine 'Rolling Stone' stating that it contained pictures of scantily-clad females. But the real reason could be an article published in the magazine that highlighted the rise in military spend. Facebook was also temporarily blocked over the whole 'Draw Mohammed Day' contest controversy. What made news more recently was the subsequent unblocking and re-blocking of YouTube. The site was banned for over hundred days owing to the anti-Islam movie 'Innocence of Muslims', which incited much ire across the world. Recently, when it was unblocked, many media channels pointed out that the video that caused such furore, owing to which the site was blocked in the first place, was still accessible on the site. This resulted in authorities blocking the site again. According to reports, Pakistani authorities also plan to have in place a national automated URL filtering and blocking system.[27]

7.4. Selective Censorship & Filtering:

Censorship of internet content can take many forms and ranges from governments blocking the dissemination of political opinion to blacklisting pornographic and pirate websites. The Opened Initiative is collaboration between three groups – the Citizen Lab at the University of Toronto's Munk school of global affairs, Harvard University's Berkman centre for internet & society and the SecDev Group in Ottawa – that investigates internet filtering around the world.

ONI principal investigator and Citizen Lab director Ronald Deibert says:

Originally and probably still to a large extent, pornography is both the most widely targeted content and also the one that's justified the most by countries. Most countries, if they're going to engage in internet censorship, start by talking about a broad category of inappropriate content. But what we've found over the last decade

[27] http://tech.firstpost.com/news-analysis/internet-censorship-a-growing-concern-64179.html

is the spectrum of content that's targeted for filtering has grown to include political content and security-related content, especially in authoritarian regimes. The scope and scale of content targeted for filtering has grown.

For each country, the ONI looks at the following four categories of filtering and gives each a rank ranging from "No evidence of filtering" to "Pervasive filtering":

Political – content opposing the current government or its policies; can also relate to human rights, freedom of expression, minority rights or religious movements

• **Social** – content that might be perceived as offensive by the general population such as sexuality, gambling, illegal drugs, etc

• **Conflict/security** – Content related to armed conflicts, border disputes, militant groups and separatist movements

• **Internet tools** – Tools enabling users to communicate with others, circumvent filtering or that otherwise provide a service. Each country is then classified in terms of consistency – how consistently these topics are filtered across internet service providers – and transparency – how visible the process is by which sites are blocked and whether users are able to view what's on the blacklist.

According to the ONI data, Iran was the worst ranked, with "pervasive" filtering in the political, social and internet tools categories and "substantial" for conflict/security filtering. Tested in 2011, Iran's filtering was rated as being "highly" consistent and had "medium" transparency. Even the country's president isn't immune to the blacklist – it was reported in February this year that censors had blocked access to several news sites supporting Ahmadinejad ahead of the parliamentary elections in March. Worse yet, Iran has proposed a national internet, which would both increase the government's grip over individual connections but also restrict foreign users from accessing Iranian websites. Additionally, individuals are also required to provide personal details to even use a cyber cafe.

After Iran were China, which had "pervasive" political and conflict/security filtering, along with "substantial" internet tools and social filtering. In addition to highly consistent filtering, China also had a lower transparency score than Iran. On April 12, Chinese users were cut off from all foreign websites, possibly due to a reconfiguration of the so-called "great firewall."

Meanwhile, authorities have shut down 42 websites since March this year. "The market for filtering technologies has grown worldwide; what started out as a

market primarily oriented to corporate environments in the west has now become a major growing business for government," said Deibert.

Our research identified many corporations – mostly Silicon Valley corporations – that have provided products and services to regimes that have violated human rights. The market for these types of technologies that are used to implement control is growing more sophisticated

However, Deibert feels governments are moving away from widespread blacklists of websites to filter and towards what the ONI calls "next-generation filtering," which includes targeted surveillance and "just in time" filtering, or temporarily filtering content only when it's valuable – for instance, during an election. "We're seeing a trend away from traditional internet censorship and towards next-generation controls," he said. "The future is not in the great firewall but in the way countries like Iran have come to filter content."[28]

7.5. Censorship & WTO:

China and other governments that engage in internet censorship that restricts access to information from other countries are violating their WTO commitments, Google has argued in a new position paper. Warning that the "transformative economic benefits of the Internet are under threat" from government-imposed limits informational flow, the company urged the international community to "take action to ensure the free flow of information online."

Google: GATS covers internet restrictions

WTO Appellate Body decisions, such as one on China's regulations pertaining to the import of various media products, "demonstrate that information restrictions are subject to GATS disciplines," the paper argued.

Under GATS provisions for non-discrimination, Google said, foreign firms should be treated no less favourably than domestic ones, and foreign service suppliers should have "reasonable and non-discriminatory access to public telecommunications networks, including to move information within and across borders." The exceptions spelled out in the GATS require governments to clearly justify any derogation, and apply them in a non-discriminatory manner.

[28] http://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list

"It is now up to other [WTO] members to ensure that exceptions do not become the rule," the paper said, urging governments to protect "members' right to pursue legitimate policy goals while preventing the broad application of exceptions that would undermine the value of the GATS."

Google has famously clashed with Beijing over its internet censorship policies. It pulled out of China earlier this year, following a period during which it censored search results in China in an attempt to work with Beijing. In the paper, Google says that in October 2007, Chinese officials, angry over the US Congress's decision to present an award to the Dalai Lama, rigged the so-called 'great firewall' so that users seeking to access US-based search engines were instead sent to Baidu, a Chinese-owned search engine.

China is hardly the only country guilty seeking to censor the internet. The paper says that "more than 40 governments have instituted broad-scale restrictions of information flow on the internet," describing intermittent blockages of YouTube and blogging and social networking sites in countries ranging from.

Calls for a "21st century internet trade agenda": Outlining what it called a "21st century Internet trade agenda," Google called on governments in the US, the EU and elsewhere to take "concrete steps to ensure that rules in the next generation of trade agreements reflect [the] new challenges of Internet trade."

As an example of what this might mean, Google praised the yet-to-be finalized Korea-US free trade agreement (FTA) text for including a provision committing both countries to "endeavour to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders," because of information flows' importance to facilitating trade. Looking ahead, Google said, governments must first "close gaps in the existing WTO framework in order to ensure that all GATS disciplines apply to all Internet trade." It called for new bilateral and multilateral trade negotiations to cover and include "new rules that reflect today's information economy." The "free flow of information should be on the table" in the Doha Round services negotiations, the paper argued. It said that existing proposals on computer and telecommunications services by the US, Canada, Japan, and the EU "would begin to rationalize and increase certainty to the scheduling of internet services." Ultimately, "a new round of commitments will be needed to ensure that all GATS disciplines apply to all of the economic activities on the internet."

The paper noted that the EU had "opportunities to advance the Internet trade agenda" in its ongoing free trade agreement talks, such as those with India and Canada. The Trans-Pacific Partnership trade agreement talks afforded the US a similar opportunity with a number of countries from around the Pacific Rim. WTO accession procedures were also pointed to as an example of where pressure could be put on Russia and some Middle Eastern countries to relax the onerous restrictions they place on internet use.

Tear down this firewall?: Google is not the first group to call for using WTO rules to attack internet censorship policies. The California First Amendment Coalition, a freedom of expression advocacy group, has petitioned the US trade representative's office to initiate WTO dispute proceedings with China over its internet restrictions. The 'great firewall', it argues, is a market access barrier that makes it almost impossible for foreign internet companies like the online auction site eBay to do business in China, to the benefit of their Chinese competitors. As of January of this year, the USTR's office said it had not taken any decisions about how to address the petition. At time of publication on Wednesday, it was too early in Washington to reach US officials to comment. ICTSD reporting; "Google Sees Rules Violations in Limits on Internet Access," NEW YORK TIMES, 17 November 2010.[29]

7.6. Online Gambling bears upon Censorship:

With the development of the Internet, online gambling industry has grown very rapidly. This fast expansion has elicited anti-Internet gaming legislation from state and federal governments, along with self-regulation in the credit card industry. Major reasons for inhibiting online gambling include the increase in problem gambling, children's access to gambling sites, fraud over the Internet, and moral decay (Manter 2003; Smith 2002). The video game-like nature of virtual casinos often makes it hard for gamblers to resist the temptation to gamble on the net (Kish 1999). In an online environment, problematic gambling can be exacerbated because online gamblers remain anonymous and may lose track of how much money is being won or lost due, in part, to the intangibility of digital money

[29] http://www.ictsd.org/bridges-news/bridges/news/government-internet-censorship-violates-wto-rules-says-google

(Manter 2003). Underage gambling may occur since children and teenagers have easy access to gambling sites without leaving their home (Kish 1999). Since offshore gambling operations are beyond the reach of U.S. regulatory laws, online gamblers continue to suffer from the misconduct of fraudulent offshore site operators. For example, online gamblers' losses are deducted immediately from their online accounts, while their winnings are often not credited (Keller 1999). Proponents of Internet gambling regulation believe that regulations would protect consumers from threat of fraud, addiction, bankruptcy, and moral decay, as well as from the dangers of untaxed online betting (Mainelli 2000).

In response to these major concerns, the Senate passed the Internet Gambling Prohibition Act of 1999 to ban all online gaming (Birnbaum 2000). Additionally, the Internet Gambling Enforcement Act was passed by the House of Representatives in 2002 to prevent the use of credit cards, checks, and electronic fund transfers to pay for interactive betting (Smith 2002). For online gambling activities, consumers usually register at a site and deposit money to open accounts by using credit cards or make payments through digital cash services such as PayPal and NETeller (McAleavy 2002). In response to legislative efforts, major credit card companies announced that they would forbid the use of their credit cards in monetary transactions between gamblers and online gambling businesses. eBay, which purchased PayPal, also stated that it would prohibit the service from processing online gambling transactions (McAleavy 2002). Simply put, online gambling is illegal under existing federal law in the United States.

The debate concerning the regulation of Internet content and the protection of minors is not limited to gambling websites. Commercial sites promoting violent computer games have raised many concerns from parents, educators, and legislators (Simons 1999; Tribe 1999). A survey released by the Entertainment Software Association (2004) showed that Americans identified video, PC, and Internet-based games as their favorite forms of entertainment, compared to watching TV or going to movies. With the increasing popularity of these games, critics are concerned that children or teenagers have unlimited access to Internet game sites which feature interactive violence. They have blamed violent computer or video games for desensitizing gamers to bloodshed, or for inducing violent behaviors. In response to these concerns, as well as the public's outrage over school violence, the FTC and the Justice Department urged an investigation into the

entertainment industry's marketing practices aimed at children and teenagers and a study of the link between aggressive behavior and consumption of violent entertainment (Broder 1999; Wallace 1999).

The negative consequences of computer gaming in several areas: physical activity, education, and psychological health. For example, research has shown that an excessive amount of computer gaming could lead to a lack of physical exercise and addiction (Griffiths 1997). Researchers are concerned that excessive computer gaming by school children could cause them to neglect their homework and have less interest in their education, even though these concerns remain largely unsubstantiated (Creasey and Myers 1986; Griffiths 1997). Researchers have also reported evidence to suggest that violent computer games among children and adolescents could increase the priming and elaboration of aggressive thought networks (Anderson and Dill 2000; Berkowitz 1984, 1990), weaken inhibitions against aggressive behavior, and increase acceptance of the use of violence to resolve conflict (Berkowitz and Green 1967; Dill and Dill 1998).

These concerns about the potentially negative effects of gambling and gaming websites lie at the core of the censorship debate. Prior studies contend that support for the government regulation of media content results from the perceived harm of messages (Rucinski and Salmon 1990). Efforts to restrict media content are seldom based on pinpointing research evidence showing the negative impact of these messages. Instead, they are grounded primarily on perceptions of the harmful effects of messages on others -- the "gullible" public (Gunther 1995; McLeod, Eveland, and Nathanson 1997; Rojas, Shah, and Faber 1996). This argument is explained by the third-person effect in the field of mass communication theory (Davison 1983). The third-person effect has been recently referred to as "the influence of presumed influence"(Gunther and Storey 2003, p.199), which incorporated the idea that people perceive some influence of a communication on others and, as a result, change their own attitudes or behaviors. The third-person effect claims that people perceive the impact of presumably harmful messages to be greater on others than on themselves, and thus they are willing to censor these messages (Davison 1983).[30]

[30] http://jiad.org/article55.html

7.7. Censorship & Trade Law:

Internet is a global market place. The rapid development of the Internet, and especially of Internet-based commerce, has largely taken place outside the standard trade-regulatory frameworks that cover most other forms of cross-border commerce. As the size of the Internet markets has grown, and as their contribution to the overall economy has become more pronounced, more attention has been given to regulatory concerns, such as trade-restrictive measures, damaging the climate of trade and investment in the fields of e-commerce, information-based services and online transmissions. Recently, Many attempts to enforce such measures have been highlighted in media: In 2009, the Iranian elections were dubbed the 'Twitter' revolution after the online service which the authorities attempted to block; China originally planned to introduce a filtering software called the Green Dam Youth Escort on every PC sold in the country, and has also blocked popular search engines and video-streaming sites on several occasions. The Chinese government has announced a ban on the distribution of news by foreign news agencies in China, except the state-owned agency, Xinhua, forbidding Reuters, AP, Bloomberg, AFP, Kyodo, to sell content to Chinese media. The problem arises from the simple fact that Internet does not respect national boundaries and online services provided at one point on the globe can, in principle, be accessed at any other point. Governments, who prefer that particular pieces of information of services should remain inaccessible from the population, are unable to act outside its jurisdiction using traditional means of enforcement: Anyone, with little or no means, to have an instant global reach without traditional market-entry barriers like physical investments, distributors, real estate, and infrastructure – and more importantly all the regulatory instruments (such as permits, licences and supervision) that are based upon them.[31]

7.8. Internet Censorship-US Position:

The USA Government has enacted two Federal laws intended to censor offensive online content. Neither of these laws are in force as at March 2002. The first law

31 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/droi/dv/droi_20100602_35po_/droi_20100602_35po_en.pdf

(the CDA) was struck down by the USA Supreme Court on First Amendment grounds. The second law (the COPA), which is more narrowly focused and covers only communications that are made for commercial purposes on the World Wide Web, is the subject of a Court injunction (also on First Amendment grounds) preventing its enforcement pending a decision of the Supreme Court. The Court decision is expected to be handed down in the latter part of 2002.

Since 1996, four U.S. states, New York, New Mexico, Michigan and Virginia have passed Internet censorship legislation restricting/banning online distribution of material deemed "harmful to minors". These laws have been struck down on Constitutional grounds.

Information about the two Federal laws is provided below.

The Communications Decency Act (CDA): The CDA was enacted in February 1996. In the same month, a US Court issued a restraining order preventing its enforcement. In June 1996, a panel of federal judges in Philadelphia ruled the CDA unconstitutional. In June 1997, the US Supreme Court struck down the CDAon grounds that it violated the First Amendment.

The following brief information about the CDA is extracted from the USA Court of Appeals for the Third Circuit's decision (Feb 2000) on the COPA:

"The CDA prohibited Internet users from using the Internet to communicate material that, under contemporary community standards, would be deemed patently offensive to minors under the age of eighteen. In so restricting Internet users, the CDA provided two affirmative defenses to prosecution; (1) the use of a credit card or other age verification system, and (2) any good faith effort to restrict access by minors. In holding that the CDA violated the First Amendment, the Supreme Court explained that without defining key terms the statute was unconstitutionally vague. Moreover, the Court noted that the breadth of the CDA was "wholly unprecedented" in that, for example, it was "not limited to commercial speech or commercial entities . . . [but rather] [i]ts open-ended prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers.

Further, the Court explained that, as applied to the Internet, a community standards criterion would effectively mean that because all Internet communication is made available to a worldwide audience, the content of the conveyed message will be judged by the standards of the community most likely to be offended by the

content. Finally, with respect to the affirmative defenses authorized by the CDA, the Court concluded that such defenses would not be economically feasible for most noncommercial Web publishers, and that even with respect to commercial publishers, the technology had yet to be proven effective in shielding minors from harmful material. As a result, the Court held that the CDA was not tailored so narrowly as to achieve the government's compelling interest in protecting minors, and that it lacked the precision that the First Amendment requires when a statute regulates the content of speech."

Child Online Protection Act (COPA): COPA is the sequel to the CDA and aimed to avoid the constitutional defects of the CDA. COPA covers communications that are made for commercial purposes on the World Wide Web. It requires commercial Web publishers to ensure that minors do not access "material harmful to minors" on their Web site.

COPA was enacted on 21 October 1998. On 20 November 1998, the US District Court for the Eastern District of Pennsylvania issued a temporary restraining order against enforcement of the law and subsequently, on 1 February 1999, issued an injunction preventing the government from enforcing the law. On 22 June 2000, the US Court of Appeals for the Third Circuit upheld the lower court's injunction. The Court stated in its conclusion that "Due to current technological limitations, COPA -- Congress' laudatory attempt to achieve its compelling objective of protecting minors from harmful material on the World Wide Web -- is more likely than not to be found unconstitutional as overbroad on the merits."

The decision was appealed to the US Supreme Court and that Court's decision is expected to be handed down in the latter part of 2002.

An overview of COPA's provisions is included in the Court of Appeals February 2000 decision:

'COPA ... attempts to "address[ ] the specific concerns raised by the Supreme Court" in invalidating the CDA. COPA prohibits an individual or entity from:

"knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, mak[ing] any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors."

As part of its attempt to cure the constitutional defects found in the CDA, Congress sought to define most of COPA's key terms. COPA attempts, for example, to

restrict its scope to material on the Web rather than on the Internet as a whole;4 to target only those Web communications made for "commercial purposes";5 and to limit its scope to only that material deemed "harmful to minors."

Under COPA, whether material published on the Web is "harmful to minors" is governed by a three-part test, each of which must be found before liability can attach:

a. the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
b. depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
c. taken as a whole, lacks serious, literary, artistic, political, or scientific value for minors.

COPA also provides Web publishers subject to the statute with affirmative defenses. If a Web publisher" has restricted access by minors to material that is harmful to minors" through the use of a "credit card, debit account, adult access code, or adult personal identification number . . . a digital certificate that verifies age . . . or by any other reasonable measures that are feasible under available technology," then no liability will attach to the Web publisher even if a minor should nevertheless gain access to restricted material under COPA.'

Offline Classification: In the USA, films, videos and computer games are not legislatively required to be classified prior to exhibition, sale or hire. Voluntary non-government established and administered rating systems are widely used.[32]

7.9. Motivation for Censorship:

As censorship as a phenomenon is as old as civilization itself, it is hardly surprising that the motivations and targets of online censorship are not markedly different from those that affect other media. The political motivation, to curb critical ideas, opposition groups and regime criticism, is common. Internet traffic is rigorously monitored and critical sites based overseas blocked in many countries,

[32] https://www.efa.org.au/Issues/Censor/cens3.html

including, among others, China, Iran, Maldives, Myanmar, North Korea, Syria, Tunisia, Turkey, Uzbekistan, Vietnam to mention a few. In Cuba, accessing the Internet is per se an illegal act, without the proper official permits. Subject for political censorship could also be ethnic or armed conflicts. In China for example, information relating to Falun Gong, Taiwan, Tiananmen Square or the Tibetan independence movement are blocked. Information about North Korea is routinely censored in South Korea. Law enforcement agencies in Russia and other CIS countries have been given powers to fully monitor all Internet activities following the experiences in Ukraine and Georgia, where the opposition successfully utilized modern communications to start popular revolts. Political figureheads are sensitive subjects too – popular services such as the streaming video service YouTube and blogging services have been shut down in Turkey for defaming Kemal Atatürk, the founding father of the republic. Similarly, criticism of the King, lèse majesté, is forbidden in Thailand online as well as offline (and is often used to prosecute the opposition). French and German laws against glorification of Nazism and holocaust denial are upheld online against sites hosted overseas, whereas enjoying sometimes constitutional protection in other countries.

Second motivation for censorship is for moral reasons, based on what societies perceive as immoral or illegal. Examples of such are numerous, and usually concern pornography, gambling or criminal activities. Blocking of foreign sites on these grounds is common in many Muslim countries, where adult content, gambling, substance abuse and discussion of many matters relating to faith are forbidden (which in Iran extends to discussion of women's rights). Moral censorship on more secular grounds also exists: in the United States, online gambling is illegal though the sites are not blocked. Sites involved in illegal file-sharing and downloading of copyrighted materials are blocked in some countries, including China and Denmark, but remain accessible in most others. Most countries (including those who do not practice censorship per se) block sites offering child pornography.

A third motive, albeit more rare, is for commercial purposes. The most prominent example is Mexico, where the former state-owned operator, Telmex, blocked Internet-based carriers such as Skype and Vonage, providing an inexpensive voice-over IP (VoIP) services. Mexico was already found by the WTO to discriminate against phone operators in the US by overcharging US operators for dispatching

their calls into Mexico, so-called interconnectivity fees. There were also similar cases over VoIP, such as Deutsche Telekom in Germany and several companies of France and the UK. China practiced similar restrictions by only granting licenses to two domestic operators to run VoIP services. Commercial censorship might also be applied by a non-state actor: In China, Sanlu (a major local dairy producer) is said to have paid Baidu, the leading search engine in China, $250,000 to block search results related to melamine contamination of Sanlu's milk products.[33]

7.10. Case Study[34]:

Call for pre-censorship of content on Social Media: December 2011 saw India's Union Communications and Information Technology minister Kapil Sibal calling for social media biggies including Google, Facebook, Twitter amongst others to pre-censor content uploaded by their users. This invited widespread criticism from Indian netizens and media alike. He later clarified that he did not mean pre-censorship of content but meant that companies ought to have standards that prevent such content from being on their space. He also insisted that these companies need to follow the law of the land, which meant that the social media companies ought to follow the restrictions to freedom of speech as deemed by the constitution. Content that violate the following issues are considered as restrictions and violations on freedom of speech.

- Security of the State
- Friendly relations with foreign States
- Public order
- Decency and morality
- Contempt of court
- Defamation
- Incitement to an offence
- Sovereignty and integrity of India.

[33] http://www.ecipe.org/app/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf

[34] http://internetdemocracy.in/2012/03/the-internet-censorship-saga-in-india/

The media in India does not enjoy a separate 'freedom of press' as enshrined by the USA constitution but the freedom of press is subsumed under the freedom of speech and expression, a fundamental right. However, there are many curbs on the Indian media. For instance, Radio news is completely banned in India with the State owned 'All India Radio' enjoying a complete monopoly over broadcasting news over the radio. Internet till 2008 was relatively free and censorship by Government sporadic. Sibal's proposition received a widespread criticism amongst the netizens, especially on Twitter.

The Vinay Rai Case: Amidst the din of censorship of the Internet, intermediaries like Facebook, Google and other companies faced a fresh jolt when Vinay Rai, editor of a Delhi-based Urdu newspaper Akbari, filed a case against them in December 2011 for allowing objectionable content up on their sites. Rai has submitted examples of what he deems as offensive content against various religions and religious figures that he found on the sites of these companies. However, Rai chose not to interact with the websites regarding this issue. He stated that the government is the ultimate authority to deal with multinationals in matters like these. Indian Penal Code has strict provisions against promotion of religious enmity in the country including Sec 153 (B), Section 298 among others.

Even as Google and Facebook have argued that they are not legally responsible for the content uploaded by the users, things don't look rosy, thanks to the cyber laws in India. The outcome of the case is still pending since the case is still with the Delhi High Court. Vijayashankar added, "Vinay Rai seems to have filed a case against content that can hurt religious sentiments of the people. There are some strong provisions in the law against hurting religious sentiments. The only fear I have is that the court should make it clear that the judgement is for this particular case alone and that the outcome of the case should not be considered as a precedent. There is a big element of public interest in this issue. It has a danger of being misinterpreted as a precedent which will affect our freedom of expression."

Indian Government asks Google to remove 'offensive' content: When the debate over Internet censorship was at its peak, Google revealed data that showed the true intentions of the Government. According to Google, the company received 68 content removal requests (which included 358 items in all) from the Government of India in the first half of 2011 (January – June) of which 51% of the

requests were adhered to. The reasons ranged from defamation, national security, government criticism amongst others. It is interesting to note that of all the requests, only one of them was attributed to National security, the main reasons cited for the amendment that happened in 2008.

In April 2011, Centre for Internet and Society, a research and advocacy organisation in India revealed that the Government of India banned around 11 websites using provisions like 69B, which aforementioned give sweeping powers to the Government.

While Google stood up to the Chinese Government refusing to adhere to the latter's censorship norms, it has not exactly shown the same spirit in India. Recently, this month, the Delhi High Court responding to a civil suit filed by Aijaz Qasmi, an Indian citizen ordered Google to remove 'offensive content' from their sites. A statement released by Google read: "This step is in accordance with Google's longstanding policy of responding to court orders." Google has already resorted to self censorship and have claimed that they will respect the law of the land. Twitter has also declared that it will censor tweets geographically.

Trivedi says, "This was bound to happen. Companies like Google, Facebook and others are business entities. They will ultimately bow down to these unfair laws. It is ultimately up to citizens of India to fight these unfair laws." Kovacs adds that, "By making intermediaries accountable for content uploaded by the users, the Government is making sure that a vast amount of internet users can be controlled and this is dangerous."

Laws for a space sans geographical boundaries

If Facebook were a country with the number of users on it, it would be the third largest country in terms of the population. Internet by its very nature has broken geographical boundaries and epitomizes the Sanskrit adage of Vasudaiva Kumtumbakam—the world is but one single family. To impose laws that are applicable to a particular geographical area to a space that knows no geography is going to be tricky indeed. While Google has announced that it will censor content as needed by the laws of the land, the same aforesaid content could be accessible in other countries. This is an exercise in futility since proxy servers could be used to access the same content from the same country where it is banned.

7.11. Summary:

The issue of internet censorship is very debatable issue worldwide and governments are using it as tool to restrict the freedom of speech and expression even I strong democracy like India. In this unit the concept of internet censorship, censorship through blocking, selective censorship and filtering, censorship and WTO, online gambling bears upon censorship, censorship and trade law, the US position specifically of censorship, and motivation for censorship are discussed at length with suitable relevant examples and legal provisions from national and international legal instruments.

7.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)

- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

7.13. Check your Progress:

A. Which of the following statements are true or false:

a. Internet censorship I India is selectively practiced by both Central and State Governments.

b. There are almost no borders on internet and we can read information from very distant countries.

c. Since the past couple of years, the instances of Internet Censorship in India have increased in manifold.

d. While India falls under 'partially free' category when it comes it to Internet freedom.

e. Internet is not a global market place.

B. Fill in the Blanks:

i. India adopted the new IT Rules, 2011, these rules ……..for internet intermediaries to remove objectionable content ……of receiving complaint.

ii. Google Transparency Report points out to the increased request from government to take down ……..and even seek information pertaining to……..

iii. China and other governments that engage in internet censorship that restricts access to information from other countries are violating……..

iv. With the development of Internet,……industry has grown very rapidly.

v. The …….has enacted two Federal Laws intended to censor offensive online content.

7.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. False

B.

1. Made it Mandatory, Within 36 hours
2. Objectionable Content, Users Account
3. WTO Commitments
4. Online Gambling
5. USA Government'

7.15. Terminal Questions

1. What is internet censorship?

2. What is censorship through blocking?
3. What is selective censorship and filtering?
4. Define censorship and WTO.
5. Define censorship and trade law.

Unit-8

Online Privacy and Security Issues

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Online Privacy and Security Issues
- Understand the remedies which are available against Infringement of Privacy
- Understand the technical and legal issues related to Online Privacy and Security Issues

Structure:

8.1. Introduction:

The stunning growth of Internet usage in some countries is also raising concerns about privacy. The qualities that make computer networks such powerful tools for improving efficiency and living standards also give them extraordinary power to collect, store, or distribute medical data, financial data, and other personal or biographical information. Many individuals and consumer groups are calling for new privacy safeguards for the Internet and other computer networks.

Personal information that may be of interest to businesses or people with malevolent aims is generated whenever people surf the Internet. Companies, for example, are able to learn a great deal about Web surfers who visit their websites. Using tracking devices known as "cookies," companies are able to track purchases and gather personal data. They can use this information to target their marketing efforts at individual consumers or groups of consumers. While some may welcome increased attention to their consumer needs, others may consider it an invasion of their privacy. There is also growing concern about what on-line and conventional stores do with the purchasing or personal data they collect during transactions. Under pressure from consumers, some stores have recently begun to develop privacy policies, but consumer groups say many of these policies fall short.

Finally, patients and consumer advocates want to set rules for the sharing of personal medical data. In each of these areas, it will be difficult to strike a balance between protecting privacy and ensuring a flow of information and data that can enhance quality of life. The same Internet-based tools that can improve education, health, and governance can also cause considerable damage when used for purposes of theft or fraud. Companies and individual computer users are being increasingly affected by computer viruses and schemes to steal data or computer identities. Companies are spending enormous amounts of time and money to protect their networks and their data. Recent polls suggest that two thirds of American companies have experienced some form of "cyber-disruption."

Resources that could be directed toward improving Internet capacity are being used to thwart cyber criminals. According to an article published in the Financial Times, the average annual cost per company of these disruptions exceeds two million dollars. The Federal Bureau of Investigation (FBI) has estimated annual losses to industry in the $10-15 billion range. Recent data forecasts that worldwide spending on security will hit $86 billion in 2016 as a result of increased concern over cyber crime from China, which has been made a priority by the Obama administration (Info security, 2012). Internet or computer service disruptions have become a major problem not only for companies, but for governments, associations, international institutions, and private citizens around the world.[35]

8.2. Online Risks:

Cyber security, phishing, worms, firewalls, Trojan horses, hackers, and viruses seem to be in the news every day. Plus warnings to update your virus protection, watch out for online scams, protect your privacy, and watch what you click on are everywhere. But what does it all mean? And what can you do to safeguard access to your computer and to protect yourself and your family? What is this all about?

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with cyber security. The Department of Homeland Security created this list of terms: Hacker, attacker, or intruder - These terms are applied to the people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results can range from mere mischief (creating a virus with no intentionally negative impact) to malicious (stealing or altering information).

Malicious code includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics:

- Viruses - This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

[35] http://www.globalization101.org/privacy-and-security-concerns/

- Worms - Worms propagate without you r doing anything. They typically start by exploiting software vulnerability (a flaw that allows the software's intended security policy to be violated). Then once the victim computer has been infected, the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.
- Trojan horses - A Trojan horse program is software that claims to do one thing while, in fact, doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending your confidential information to an intruder.
- Spyware - This sneaky software rides its way onto computers when you download screensavers, games, music, and other applications. Spyware sends information about what you're doing on the Internet to a third-party, usually to target you with pop-up ads. Browsers enable you to block pop-ups. You can also install anti-spyware to stop this threat to your privacy.
- It is probably easy for you to identify people who could gain physical access to your computer—family members, roommates, co-workers, members of a cleaning crew, and maybe some others. But identifying the people who could gain remote access to your computer becomes much more difficult. As long as you have a computer and connect it to a network or the internet, you are vulnerable to someone or something else accessing or corrupting your information. Luckily, you can develop habits that make it more difficult.
- Lock or log-off your computer when you are away from it. This prevents another person from waiting for you to leave and then sitting down at your computer and accessing all of your information.
- To be really secure, disconnect your computer from the Internet when you aren't using it. DSL and cable modems make it possible for users to be online all the time, but this convenience comes with risks. The likelihood that attackers or viruses scanning the network for available computers will target your computer becomes much higher if your computer is always connected.

- Evaluate your security settings. It is important to examine your computer's settings, especially the security settings, and select options that meet your needs without putting you at increased risk. Many, but not all Internet providers offer free security software. If you don't receive free software, you should consider buying a commercial product that includes virus scan, firewall, and pop-up blockers. You should also be aware of your Internet cookies setting. Cookies are short pieces of data used by web servers to identify users. Some cookies are useful for storing images and data from websites that you frequent, but others are malicious and collect information about you. You'll have to decide how much risk from cookies you can accept. Finally, if you install a patch or a new version of software, or if you hear of something that might affect your settings, reevaluate your settings to make sure they are still appropriate.
- Look for a privacy policy statement or seal that indicates the site abides by privacy standards. Take time to read how your privacy is protected.
- Look for signals that you are using a secure web page. A secure site encrypts or scrambles personal information so it cannot be easily intercepted. Signals include a screen notice that says you are on a secure site, a closed lock or unbroken key in the bottom corner of your screen, or the first letters of the Internet address you are viewing changes from "http" to "https."[36]

8.3. Online Privacy Issues and Online Surveillance:

Online Surveillance and Access:

The ITA also allows for the interference of user privacy online by defining broad standards of access to law enforcement and security agencies, and providing the government with the power to determine what tools individuals can use to protect their privacy. This is most clearly demonstrated by provisions that permit the interception, monitoring, and decryption of digital communications provide for the collection and monitoring of traffic data and allow the government to set the national encryption standard. In particular, the structure of these provisions and the lack of safeguards incorporated, serve as a dilution to user privacy. For example,

[36] http://www.usa.gov/topics/family/privacy-protection/online.shtml

though these provisions create a framework for interception they are missing a number of internationally recognized safeguards and practices, such as notice to the individual, judicial oversight, and transparency requirements. Furthermore, the provisions place extensive security and technical obligations on the service provider – as they are required to extend all facilities necessary to security agencies for interception and decryption, and hold the service provider liable for imprisonment up to seven years for non-compliance. This creates an environment where it is unlikely that the service provider would challenge any request for access or interception from law enforcement. Interception is also regulated through provisions and rules under the Indian Telegraph Act 1885 and subsequent ISP and UAS licenses.

Scope of Surveillance and Access:

The extent to which the Government of India lawfully intercepts communications is not entirely clear, but in 2011 news items quoted that in the month of July 8,736 phones and e-mail accounts were under lawful surveillance.

Though this number is representative of authorized interception, there have been a number of instances of unauthorized interceptions that have taken place as well. For example, in 2013 it was found that in Himachel Pradesh 1371 phones were tapped based on verbal approval, while the Home Ministry had only authorized interception of 170. This demonstrates that there are instances of when existing safeguards for interception and surveillance are undermined and highlights the challenge of enforcement for even existing safeguards.

Demonstrating the tensions between right to privacy and governmental access to communications, and at the same time highlighting the issue of jurisdiction was the standoff between RIM/BlackBerry and the Indian Government. For several years, the Indian Government has requested that RIM provide access to the company's communication traffic, both BIS and BES, as Indian security agencies have been unable to decrypt the data. Solutions that the Indian Government has proposed include: RIM providing the decryption keys to the government, RIM establishing a local server, local ISPs and telcos developing an indigenous monitoring solution. In 2012, RIM finally established a server in Mumbai and in 2013 provided a lawful interception solution that satisfied the Indian Government.

The implementation of the Central Monitoring System by the Indian Government is another example of the Government seeking greater access to communications.

The system will allow security agencies to bypass service providers and directly intercept communications. It is unclear if the system will provide for the interception of only telephonic communications or if it will also allow for the interception of digital communications and internet traffic. It is also unclear what checks and balances exist in the system. By removing the service provider from the equation the government is not only taking away a potential check, as service providers can resist unauthorized requests, but it is also taking away the possibility for companies to be transparent about the interception requests that they comply with.[37]

8.4. Privacy Policy Problem:

Although some Web sites still lack a posted privacy policy, an increasing number of sites have them — though they may require some searching to find. Once found, it's important to read the policy carefully, so that you can be sure you agree with it. Some privacy policies can be unclear, ambiguous, hard to understand, or may refer to unspecified relationships with unspecified companies. You may also need to read the "Terms and Conditions," User/Subscriber/Service Agreements, or equivalents, since these may modify the privacy policy. For example, the privacy policy at one Web site stated clearly that no information would be shared without user permission, but the accompanying subscriber agreement declared that by subscribing, users automatically gave permission for their information to be shared Regardless of the current wording of the privacy policy or other legal notices, the phrase "changes can be made at any time" is relatively common in these agreements. In fact, the agreements often state that these changes may be made without notice. Users must regularly check the notices for updates or changes. Here is one example from Amazon.com, though the company did add an "opt-out" clause: "Amazon.com does not sell, trade, or rent your personal information to others. Armand Prieditis, CEO of Unconventional Wisdom, has developed a number of questions for rating privacy policies, including the following: Is the policy prominent and easily accessible? Is it clear? Is it short? What information is collected? Is there an opt-out choice available? Is there provision for users to make

[37] http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india

changes, updates, or deletion to their personal data? Is there a contact given at the company for questions relating to their privacy practices?

In an effort to mitigate the necessity for reading multiple, often confusing, privacy policies, The World Wide Web Consortium [http://W3c.org] is developing the Platform for Privacy Preferences (P3P) [http://www.w3.org/P3P/]. Due out in the summer of 2000, P3P will enable users to choose their own preferences concerning the kind and quantity of information they are willing to provide. Users will be warned when they surf a site which has a privacy policy that goes beyond their pre-set privacy limits. At this writing Microsoft has just promised to provide free Internet tools for P3P in the fall of 2000. However, P3P is the subject of some controversy. Some critics feel that there are insufficient incentives for Web sites to enroll in the program. Junk busters president Jason Catlett said that wide adoption remains years away (*The New York Times*, 4/7/2000). Catlett said that companies are using P3P as "an excuse to use in their lobbying against enforceable privacy rights for the American consumer: a Pretext for Privacy Procrastination" [http://www.cfp2000.org/papers/catlett.pdf].

Even if you approve a site's privacy policy, what assurance do you have that the site will actually comply with its posted policy? A recent study by the California HealthCare Foundation alleges that a number of health care Web sites shared personal consumer health information with other sites in violation of its own privacy policies. The Federal Trade Commission has been asked to review these charges.

Privacy Seals — Good Housekeeping? A number of online privacy seals have been established in an attempt to reassure consumers about often confusing privacy policy provisions. These seals include TRUSTe, CPA WebTrust, BBBOnline, and SecureAssure. All of these seals set standards that participating sites must meet.

Critics charge that an inherent conflict of interest exists with certificate programs subsidized by fees from participating sites. They also charge them with a lack of enforcement actions. The programs seldom withdraw the seals, even for flagrant violations. TRUSTe in particular has been called an attempt by industry to avoid government oversight, and that it "…proves industry self-regulation on privacy won't work" (*Industry Standard*, March 20, 2000, p. 168). Independent third-party certification could be very useful in promoting consumer trust, especially regarding sensitive issues. One particularly useful application might lie in guaranteeing site

security against hacker attacks, since companies are understandably reluctant to detail security arrangements openly on their Web sites.[38]

8.5. OECD Work on Privacy:

Over many decades the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. The cornerstone of OECD work on privacy is its newly revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013). Another key component of work in this area aims to improve cross-border co-operation among privacy law enforcement authorities. This work produced an OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy in 2007 and inspired the formation of the Global Privacy Enforcement Network, to which the OECD provides support. Other projects have examined privacy notices and considered privacy in the context of horizontal issues such as radio frequency identification (RFID), digital identity management, and looked at metrics to inform policy making in these areas. The important role of privacy is also addressed in the OECD Recommendation on Principles for Internet Policy Making (2011) and the Seoul Ministerial Declaration on the Future of the Internet Economy (2008). Current work is examining privacy-related issues raised by large-scale data use and analytics. An expert roundtable was held in support of that work in March 2014. It is part of a broader project on the data-driven innovation and growth, which already produced a preliminary report identifying key issues.

The 2013 OECD Privacy Guidelines

The revisions agreed in 2013 include:

- The Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (July 2013); and
- A new explanatory memorandum providing context and rationale for the July 2013 revisions.

[38] http://www.infotoday.com/searcher/jul00/duberman&beaudet.htm

These new Guidelines constitute the first update of the original 1980 version that served as the first internationally agreed upon set of privacy principles.
Two themes run through the updated Guidelines. First is a focus on the practical implementation of privacy protection through an approach grounded in risk management. Second is the need for greater efforts to address the global dimension of privacy through improved interoperability. A number of new concepts are introduced, including:

- National privacy strategies. While effective laws are essential, the strategic importance of privacy today also requires a multifaceted national strategy co-ordinated at the highest levels of government.
- Privacy management programmes. These serve as the core operational mechanism through which organisations implement privacy protection.

- Data security breach notification. This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.

Other revisions modernise the OECD approach to transborder data flows, detail the key elements of what it means to be an accountable organisation, and strengthen privacy enforcement. As a step in a continuing process, this revision leaves intact the original "Basic Principles" of the Guidelines. On-going work by the OECD on privacy protection in a data-driven economy will provide further opportunities to ensure that its privacy framework is well adapted to current challenges.

The process to revise the Guidelines was led by the OECD's Working Party on Information Security and Privacy (WPISP) working from terms of reference released at an OECD conference on global interoperability in Mexico City in November 2011. Preparatory work for the 2013 revision was conducted in the context of the 30th anniversary of the original Guidelines, marked by a series of conferences and papers. In accordance with the terms of reference, the WPISP convened a multi-stakeholder group of experts from governments, privacy enforcement authorities, academia, business, civil society and the Internet technical community. This expert group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene, consultant to the OECD, served as rapporteur. On the basis of the work by the expert group, proposed revisions were

developed by the WPISP and approved by the Committee for Information, Computer and Communications Policy (ICCP), before final adoption by the OECD Council.

8.6. Data Leakage Protection (DLP):

Protecting data leakage for any organization has been primary concern in today's world which has rapidly increased the need for DLP solutions in market. However, the term DLP itself is used in different ways by different vendors. We at NII help you demystify the jargon and select the apt DLP solution for your organization. At the same time, just procuring and implementing a DLP solution is not the complete answer. DLP solutions are highly involved technologies and have intense implementation cycles. So a successful DLP implementation requires the right planning, resourcing, configuration, management, and monitoring to help it really protect data leakage.

How does DLP work?

Following are the various methods how data leakage protection helps your organization to protect your valuable or sensitive information which is in transit, at rest or in use.

- DLP provides a robust solution to protect data in transit [network actions] by sniffing network traffic of emails, chat messages, etc to discover content being sent across the communication channel.
- It also provides a solution to protect data at rest by scanning storage area content like USB drives, hard drives, etc and discover content from it. It is also termed as Content Discovery.
- It also provides a solution to protect data in use [endpoint actions] i.e., it protects the data which is in use by the user for example if a user has connected USB drives to the computer.

Most DLP solutions do this in combinations of the following:

1. Rule-based Regular Expressions
2. Database Fingerprinting
3. Exact File Matching
4. Partial Document Matching
5. Statistical Analysis

6. Conceptual/Lexicon
7. Categories

8.7. Message Encryption:

Sometimes you want additional protection for your e-mail communication to keep it from unwanted eyes. Encrypting an e-mail message in Microsoft Office Outlook 2007 protects the privacy of the message by converting it from (readable) plaintext into (scrambled) ciphertext. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Any recipient without the corresponding private key would see only garbled text.

- This is a separate process from digitally signing a message.
- Sending and viewing encrypted e-mail messages requires both sender and recipient to share their digital ID, or public key certificate. This means you and the recipient each must send the other a digitally signed message, which enables you to add the other person's certificate to your Contacts. Once both parties have shared certificates, sending and viewing encrypted e-mail messages between them is the same as with any other e-mail messages. You can learn about digital IDs here and learn how to get and exchange digital IDs here.
- If you send an encrypted message to a recipient whose e-mail setup does not support encryption, Outlook notifies you and offers the option of sending the message in unencrypted format.
- This process also encrypts any attachments sent with encrypted messages[39].

8.8. End to End Encryption:

"End-to-end" encryption means data leaving your browser will be encrypted until the message's intended recipient decrypts it, and that similarly encrypted messages sent to you will remain that way until you decrypt them in your browser. While end-to-end encryption tools like PGP and GnuPG have been around for a long time, they require a great deal of technical know-how and manual effort to use. To

[39] https://support.office.com/en-in/article/Encrypt-e-mail-messages

help make this kind of encryption a bit easier, we're releasing code for a new Chrome extension that uses OpenPGP, an open standard supported by many existing encryption tools. However, you won't find the End-to-End extension in the Chrome Web Store quite yet; we're just sharing the code today so that the community can test and evaluate it, helping us make sure that it's as secure as it needs to be before people start relying on it. Once we feel that the extension is ready for primetime, we'll make it available in the Chrome Web Store, and anyone will be able to use it to send and receive end-to-end encrypted emails through their existing web-based email provider. We recognize that this sort of encryption will probably only be used for very sensitive messages or by those who need added protection. But we hope that the End-to-End extension will make it quicker and easier for people to get that extra layer of security should they need it[40].

8.9. Indian Government National Cyber Security Policy, 2013:

On July 2, 2013, the Indian government released its ambitious National Cyber Security Policy 2013. The development of the policy was prompted by a variety of factors, including the growth of India's information technology industry, an increasing number of cyber attacks and the country's "ambitious plans for rapid social transformation." The policy sets forth 14 diverse objectives that range from enhancing the protection of India's critical infrastructure, to assisting the investigation and prosecution of cyber crime, to developing 500,000 skilled cyber security professionals over the next five years.

To accomplish these objectives, the policy details numerous action items for the Indian government, including:

- Designating a national agency to coordinate all cyber security matters;
- Encouraging all private and public organizations to designate a Chief Information Security Officer responsible for cyber security;
- Developing a dynamic legal framework to address cyber security challenges in the areas of cloud computing, mobile computing and social media;
- Operating a National Critical Information Infrastructure Protection Center;
- Promoting research and development in cyber security;

[40] http://googleonlinesecurity.blogspot.in/2014/06/making-end-to-end-encryption-easier-to.html

- Enhancing global cooperation in combating cyber security threats;
- Fostering education and training programs in cyber security; and
- Establishing public and private partnerships to determine best practices in cyber security.

In announcing the policy, the Indian Minister of Communications and Information Technology Kapil Sibal (Former Minister) noted that the operationalization of the policy would be challenging but ultimately necessary in order to "ensure there is no disruption of the kind that will destabilize the economy."

DSCI (Data Security Council of India) started functioning as an independent company with its own Board, and a small core team comprising technical experts, guided by the Steering Committee in August, 2008. Their guidance has enabled DSCI define its mission, which in turn helped it draw up a Work Plan, with a practical approach for involving the industry through our Content Aggregation Program. This program comprises mapping of regulations into controls, and deriving best practices from the same. The Best Practices for Data Security and Data Privacy have been developed using the experience of ISO 27001 security standard, and OECD Privacy Principles, and that of government framework implementation like FISMA in theUSA; as also the recommendations of analysts and tactical guidelines emerging over the last few years. The best practices will enable a service provider in India to be not only in compliance with regulatory requirements, but also make them really secure.

DSCI engaged with stakeholders in the US, the UK, European Union and some other countries to make them aware of the emphasis on security and privacy practices by the Indian IT/BPO industry. This was through presentations to, and discussions with, data protection authorities and clients in a number of seminars and workshops. DSCI engaged with the IT/BPO industry during the year through a number of security awareness seminars and workshops, and on the need for best practices and standards for enhancing their trustworthiness. The industry has responded favorably to the DSCI Data Protection Approach based on best practices, and its aim of becoming a self-regulatory organization.
To protect privacy of personal information from unauthorized use, disclosure, modification or misuse, DSCI conceptualized its approach towards privacy in the

DSCI Privacy Framework (DPF which is based on the global privacy best practices and frameworks. The framework was released in December, 2010. To assess the privacy implementation in an organization, DSCI Assessment Framework for Privacy (DAF-P) was released in December, 2012. It consists of two parts, with each focusing on distinct aspects of privacy implementation – one focuses on Assessment of Organizational Competence in Privacy based on practice areas defined in DPF while the other – Privacy Principles based Assessment, focuses on implementation of global privacy principles. The first part is based on the nine practice areas listed under DPF and the assessment questionnaire is thus designed to help organizations assess and mature their privacy program. The questionnaire is based on the practices defined in DPF, with suggestive guidance parameters to aid the assessors when conducting assessments. The assessment could be conducted in either modes: Self-Assessment or External Assessment. The external assessment through DSCI empanelled auditors could help organizations attain DSCI Certification. The second part is intended to help organizations assess and improve maturity in the implementation of global privacy principles across all the organizational processes that deal with personal information and in the process optimize their efforts while implementing privacy principles across global operations. DSCI has designed a training program for potential assessors to assess implementation of privacy in organizations that meets the requirements laid down in DPF.

Objectives : To equip the potential assessors with necessary knowledge and tools to assess organizations' privacy implementations in accordance with DSCI Assessment Framework for Privacy (DAF-P) and DSCI Privacy Framework . The training program intends to explain the intent behind each of the practices defined under the nine practice areas of (DPF), to help the assessors understand, analyze, investigate and appreciate the various aspects of privacy implementation within organizations. The training program aims to provide a common platform for potential assessors from different organizations to have a common understanding and expectations for privacy implementations. The program will also help organizations desirous of DSCI certification; better understand the expectation of privacy implementation, and requirements for DSCI certification

8.10. Guidelines for Cyber Café in India:

In 2011 the Guidelines for Cyber Café Rules were notified under the Information Technology Act. These Rules, among other things, require Cyber Café's to retain the following details for every user for a period of one year: details of identification, name, address, contact number, gender, date, computer terminal identification, log in time, and log out time. These details must be submitted to the same agency as directed, on a monthly basis. Cyber Cafes must also retain the history of websites accessed and logs of proxy servers installed at the cyber café for a period of one year. Furthermore, Cyber Café's must ensure that the partitions between cubicles do not exceed four and half feet in height from floor level. Lastly, the cyber café owner is required to provide every related document, register, and information to any officer authorized by the registration agency on demand. In effect, the identification and retention requirements of these rules both impact privacy and freedom of expression, as cyber cafes users cannot use the facility anonymously and all their information, including browser history, is stored on an a-priori basis. The disclosure provisions in these rules also impact privacy and demonstrate a dilution of access standards for law enforcement to users internet communications as the provision does not define:

- An authorization process by which the registration agency follows to authorize individuals to conduct inspections.
- Circumstances on which inspection of a Cyber Café by an authorized officer is necessary and permissible.
- The process for which information can be requested, and instead vaguely requires cyber café owners to disclose information "on demand".'

8.11. Summary:

There is no consensus worldwide on online privacy and securities issues due to some vested interest of industries. In this unit the concept of online risks, online privacy issue and online surveillance, privacy policy problem, OECD work on privacy, protecting data in transit, message encryption, End-to-End Encryption, Indian Government and Cyber Security Policy, 2013 and Guidelines for Cyber Security Café in India are discussed at length to understand the issue of online privacy and securities in India and worldwide.

8.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)

- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

8.13. Check your Progress:

a. Which of the following statements are true or false:
b. The stunning growth of internet usage in some countries is also raising concerns about privacy.
c. Using tracking devices known as "cookies", companies are able to track purchases and gathering personal data.
d. Cyber security, phishing, worms, firewalls, Trojan horses, hackers and viruses seem to be in the news every day.
e. Some websites still lack a posted privacy policy.
f. Over many decades the OECD has played an important role in promoting respect for privacy as fundamental value and a condition for the free flow of personal data across borders.

A. Fill in the Blanks:

i. A …….program is software that claims to do one thing while, in fact doing something different behind the scenes.
ii. Interception is also regulated through provisions and rules under the …….
iii. The cornerstone of OECD work on privacy is its newly revised …….
iv. DLP means……
v. DSCI means……..

8.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Trojan Horse
2. Indian Telegraph Act, 1885
3. Guidelines on the protection of privacy and transformer flows of personal data
4. Data Leakage Protection
5. Data Security Council of India

8.15. Terminal Questions:

1. 1.What is online risks?
2. Discuss online privacy.
3. What is OECD work on privacy?
4. Discuss Indian Government and Cyber Security Policy, 2013.
5. What are the guidelines for cyber security café in India?

Unit-9

Internal Security-Concepts, Tools and Related Issues

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Internal Security
- Understand the threats and challenges in case of intrusion in Internal Security
- Understand the technical and legal issues related to Internal Security

Structure:

9.1. Introduction:

The open nature of the Internet makes it vital for businesses to pay attention to the security of their networks. As companies move more of their business functions to

the public network, they need to take precautions to ensure that the data cannot be compromised and that the data is not accessible to anyone who is not authorized to see it. Unauthorized network access by an outside hacker or a disgruntled employee can cause damage or destruction to proprietary data, negatively affect company productivity, and impede the capability to compete. The Computer Security Institute reported in its 2010/2011 CSI Computer Crime and Security Survey (available athttp://gocsi.com/survey) that on an average day, 41.1 percent of respondents dealt with at least one security incident. Unauthorized network access can also harm relationships with customers and business partners, who might question the capability of a company to protect its confidential information. The definition of "data location" is being blurred by cloud computing services and other service trends. Individuals and corporations benefit from the elastic deployment of services in the cloud, available at all times from any device, but these dramatic changes in the business services industry exacerbate the risks in protecting data and the entities using it (individuals, businesses, governments, and so on). Security policies and architectures require sound principles and a lifecycle approach, including whether the data is in the server farm, mobile on the employee's laptop, or stored in the cloud.[41]

9.2. Internet Security: Whom should you trust?

In Forbe's recent article "Internet Security: Whom Should You Trust", the subject of knowing who to trust online when faced with the ongoing challenge of being able to authenticate legitimate entities online. In this article, we learn more about how "...internet security is all about trust at a distance" as well as what the US government is doing, particularly the 'Online Trust Alliance' (OTA) to protect its citizens from fraud and scammers online. The OTA represents over 100 companies and organizations that "...reflect the broad internet ecosystem." Combined, they have forged integral relationships with major security and virus developers, Microsoft, social networking sites and online payment systems such as Paypal. Last week at the New York Attorney General's office, they met with the FBI to discuss global cybercrime. The OTA aims to "enhance online trust" while

[41] http://www.ciscopress.com/articles/article.asp?p=1998559

encouraging vitality and innovation on the web. For business, these efforts "...translates into security, privacy, reputation and liability and money."[42]

9.3. Internet Research Ethics:

Internet research ethics is a sub discipline that fits across many disciplines, ranging from social sciences, arts and humanities, medical/biomedical, and hard sciences. Extant ethical frameworks, including consequentialism, utilitarianism, deontology, virtue ethics, and feminist ethics have contributed to the ways in which ethical issues in Internet research are considered and evaluated. Conceptually and historically, Internet research ethics is related to computer and information ethics and includes such ethical issues as data privacy and confidentiality, integrity of data, intellectual property issues, and professional standards. Throughout the Internet's evolution, there has been debate whether there are new ethical dilemmas emerging, or if the existing dilemmas are consistent across research or despite technological influence (Elgesem 2002; Walther 2002; Ess & AoIR 2002). These debates are similar to philosophical debates in computer and information ethics. For example, many years ago, Moor asked "what is special about computers" in order to understand what is ethically unique and the same question applies to Internet research (Moor 1985; Ess & AoIR 2002; King 1996).

Yet, as the Internet has evolved into a more social and communicative tool and venue, the ethical issues have shifted from purely data driven to more human-centered. "On-ground" or face-to face analogies may not be applicable to online research. For example, the concept of the public park has been used as a site where researchers can observe others, but online, the concepts of public and private are much more complex. Thus, some scholars suggest that the specificity of Internet research ethics calls for new regulatory and/or professional and disciplinary guidance. For these reasons, the concept of human subjects research policy and regulation informs this entry, along with disciplinary standards, which will explore the growing areas of ethical and methodological complexity, including personal identifiability, reputational risk and harm, notions of public space and public text, ownership, and longevity of data as they relate to Internet research. Specifically, the emergence of the social web raises issues around subject or participant

[42] https://www.scanandtrust.com/Forbes-trust.html

recruitment practices, tiered informed consent models, and protection of various expectations and forms of privacy in an ever-increasing world of diffused and ubiquitous technologies; anonymity and confidentiality of data in spaces where researchers and their subjects may not fully understand the terms and conditions of those venues or tools; challenges to data integrity as research projects can be outsourced to a mechanical turk or a bot; and jurisdictional issues as more research is processed, stored, and disseminated via cloud computing or in remote server locales, presenting myriad legal complexities given jurisdictional differences in data laws.

As a result, researchers using the Internet as a tool or a space of research—and their research ethics boards (REBs), also known as institutional review boards (IRBs) in the United States or human research ethics committees (HRECs) in other countries such as Australia—have been confronted with a series of new ethical enquiries: What ethical obligations do researchers have to protect the privacy of subjects engaging in activities in "public" Internet spaces? How is confidentiality or anonymity assured online? How is and should informed consent be obtained online? How should research on minors be conducted, and how do you prove a subject is not a minor? Is deception (pretending to be someone you are not, withholding identifiable information, etc) online a norm or a harm? How is "harm" possible to someone existing in an online space?[43]

9.4. Internet Security Issues:

All communication over the Internet uses the Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP allows information to be sent from one computer to another through a variety of intermediate computers and separate networks before it reaches its destination. The great flexibility of TCP/IP has led to its worldwide acceptance as the basic Internet and intranet communications protocol. At the same time, the fact that TCP/IP allows information to pass through intermediate computers makes it possible for a third party to interfere with communications in the following ways:

[43] http://plato.stanford.edu/entries/ethics-internet-research/

- Eavesdropping. Information remains intact, but its privacy is compromised. For example, someone could learn your credit card number, record a sensitive conversation, or intercept classified information.
- Tampering. Information in transit is changed or replaced and then sent on to the recipient. For example, someone could alter an order for goods or change a person's resume.
- Impersonation. Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
- Spoofing. A person can pretend to be someone else. For example, a person can pretend to have the email address jdoe@example.net, or a computer can identify itself as a site called www.example.net when it is not. This type of impersonation is known as spoofing.
- Misrepresentation. A person or organization can misrepresent itself. For example, suppose the site www.example.net pretends to be a furniture store when it is really just a site that takes credit-card payments but never sends any goods.

Normally, users of the many cooperating computers that make up the Internet or other networks don't monitor or interfere with the network traffic that continuously passes through their machines. However, many sensitive personal and business communications over the Internet require precautions that address the threats listed above. Fortunately, a set of well-established techniques and standards known as public-key cryptography make it relatively easy to take such precautions. Public-key cryptography facilitates the following tasks:

- Encryption and decryption allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- Tamper detection allows the recipient of information to verify that it has not been modified in transit. Any attempt to modify data or substitute a false message for a legitimate one will be detected.
- Authentication allows the recipient of information to determine its origin-that is, to confirm the sender's identity.

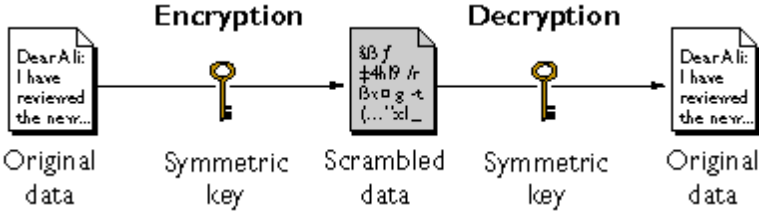
- Non repudiation prevents the sender of information from claiming at a later date that the information was never sent.[44]

9.5. Encryption and Decryption:

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. Decryption is the process of transforming encrypted information so that it is intelligible again. A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. In most cases, two related functions are employed, one for encryption and the other for decryption. With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a key that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, and in some cases impossible for all practical purposes.

The sections that follow introduce the use of keys for encryption and decryption.

- Symmetric-Key Encryption
- Public-Key Encryption
- Key Length and Encryption Strength
- Symmetric-Key Encryption: With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown in Figure 1.
-



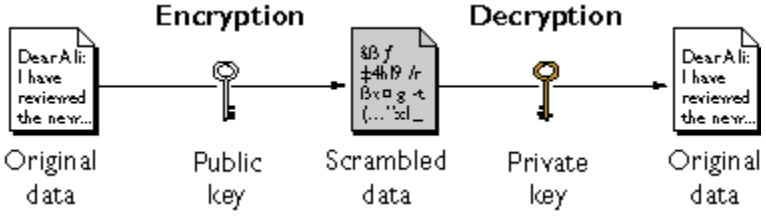
Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and

[44] https://developer.mozilla.org/en/docs/Introduction_to_Public-Key_Cryptography

decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the two parties who were originally using the key. Symmetric-key encryption plays an important role in the SSL protocol, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

Public-Key Encryption: The most commonly used implementations of public-key encryption are based on algorithms patented by RSA Data Security. Therefore, this section describes the RSA approach to public-key encryption. Public-key encryption (also called asymmetric encryption) involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret. (For more information about the way public keys are published, see "Certificates and Authentication".) Data encrypted with your public key can be decrypted only with your private key. Figure 2 shows a simplified view of the way public-key encryption works.



The scheme shown in Figure 2 lets you freely distribute a public key, and only you will be able to read data encrypted using this key. In general, to send encrypted

data to someone, you encrypt the data with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more computation and is therefore not always appropriate for large amounts of data. However, it's possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL protocol.

As it happens, the reverse of the scheme shown in Figure 2 also works: data encrypted with your private key can be decrypted only with your public key. This would not be a desirable way to encrypt sensitive data, however, because it means that anyone with your public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful, because it means you can use your private key to sign data with your digital signature-an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Firefox can then use your public key to confirm that the message was signed with your private key and that it hasn't been tampered with since being signed. "Digital Signatures" and subsequent sections describe how this confirmation process works.

Key Length and Encryption Strength

In general, the strength of encryption is related to the difficulty of discovering the key, which in turn depends on both the cipher used and the length of the key. For example, the difficulty of discovering the key for the RSA cipher most commonly used for public-key encryption depends on the difficulty of factoring large numbers, a well-known mathematical problem.

Encryption strength is often described in terms of the size of the keys used to perform the encryption: in general, longer keys provide stronger encryption. Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption. (For more information about RC4 and other ciphers used with SSL.

Different ciphers may require different key lengths to achieve the same level of encryption strength. The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the

nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values. Thus a 128-bit key for use with a symmetric-key encryption cipher would provide stronger encryption than a 128-bit key for use with the RSA public-key encryption cipher. This difference explains why the RSA public-key encryption cipher must use a 512-bit key (or longer) to be considered cryptographically strong, whereas symmetric key ciphers can achieve approximately the same level of strength with a 64-bit key. Even this level of strength may be vulnerable to attacks in the near future.

Because the ability to surreptitiously intercept and decrypt encrypted information has historically been a significant military asset, the U.S. Government restricts export of cryptographic software, including most software that permits use of symmetric encryption keys longer than 40 bits.[45]

9.6. Certificates and Authentication:

A certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Like a driver's license, a passport, or other commonly used personal IDs, a certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation. To get a driver's license, you typically apply to a government agency, such as the Department of Motor Vehicles, which verifies your identity, your ability to drive, your address, and other information before issuing the license. To get a student ID, you apply to a school or college, which performs different checks (such as whether you have paid your tuition) before issuing the ID. To get a library card, you may need to provide only your name and a utility bill with your address on it.

Certificates work much the same way as any of these familiar forms of identification. Certificate authorities (CAs) are entities that validate identities and issue certificates. They can be either independent third parties or organizations running their own certificate-issuing server software (such as Red Hat Certificate System). The methods used to validate an identity vary depending on the policies of a given CA-just as the methods to validate other forms of identification vary

[45] https://developer.mozilla.org/en/docs/Introduction_to_Public-Key_Cryptography

depending on who is issuing the ID and the purpose for which it will be used. In general, before issuing a certificate, the CA must use its published verification procedures for that type of certificate to ensure that an entity requesting a certificate is in fact who it claims to be. The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies (such as the name of an employee or a server). Certificates help prevent the use of fake public keys for impersonation. Only the public key certified by the certificate will work with the corresponding private key possessed by the entity identified by the certificate.

In addition to a public key, a certificate always includes the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, a serial number, and other information. Most importantly, a certificate always includes the digital signature of the issuing CA. The CA's digital signature allows the certificate to function as a "letter of introduction" for users who know and trust the CA but don't know the entity identified by the certificate.

Authentication Confirms an Identity:

Authentication is the process of confirming an identity. In the context of network interactions, authentication involves the confident identification of one party by another party. Authentication over networks can take many forms. Certificates are one way of supporting authentication.

Network interactions typically take place between a client, such as browser software running on a personal computer, and a server, such as the software and hardware used to host a Web site. Client authentication refers to the confident identification of a client by a server (that is, identification of the person assumed to be using the client software). Server authentication refers to the confident identification of a server by a client (that is, identification of the organization assumed to be responsible for the server at a particular network address).

Client and server authentication are not the only forms of authentication that certificates support. For example, the digital signature on an email message, combined with the certificate that identifies the sender, provide strong evidence that the person identified by that certificate did indeed send that message. Similarly, a digital signature on an HTML form, combined with a certificate that identifies the signer, can provide evidence, after the fact, that the person identified by that certificate did agree to the contents of the form. In addition to

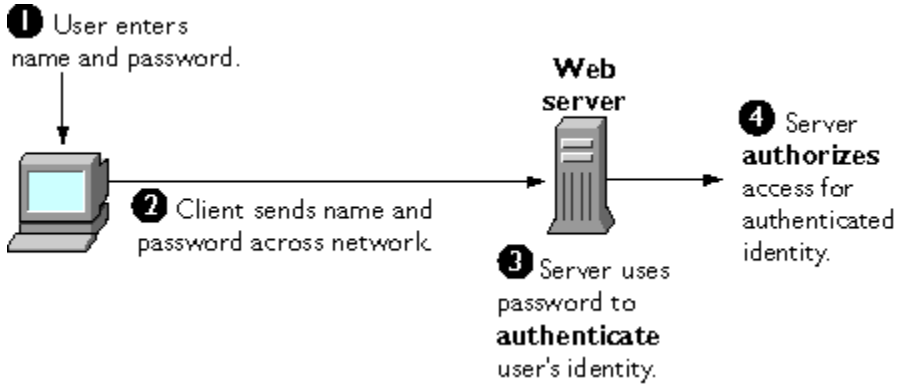
authentication, the digital signature in both cases ensures a degree of non repudiation-that is, a digital signature makes it difficult for the signer to claim later not to have sent the email or the form. Client authentication is an essential element of network security within most intranets or extranets. The sections that follow contrast two forms of client authentication:

- Password-Based Authentication. Almost all server software permits client authentication by means of a name and password. For example, a server might require a user to type a name and password before granting access to the server. The server maintains a list of names and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access.
- Certificate-Based Authentication**.** Client authentication based on certificates is part of the SSL protocol. The client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. The server uses techniques of public-key cryptography to validate the signature and confirm the validity of the certificate.

Password-Based Authentication

Figure 4 shows the basic steps involved in authenticating a client by means of a name and password. Figure 4 assumes the following:

- The user has already decided to trust the server, either without authentication or on the basis of server authentication via SSL.
- The user has requested a resource controlled by the server.
- The server requires client authentication before permitting access to the requested resource.



These are the steps shown in Figure 4:

1. In response to an authentication request from the server, the client displays a dialog box requesting the user's name and password for that server. The user must supply a name and password separately for each new server the user wishes to use during a work session.
2. The client sends the name and password across the network, either in the clear or over an encrypted SSL connection.
3. The server looks up the name and password in its local password database and, if they match, accepts them as evidence authenticating the user's identity.
4. The server determines whether the identified user is permitted to access the requested resource, and if so allows the client to access it.

With this arrangement, the user must supply a new password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

Proper implementation does not store passwords in plaintext. Instead it concatenates the password with a random per-user value (so called "salt") and stores the hash value of the result along with the salt. This makes certain kinds of brute-force atacks more difficult.

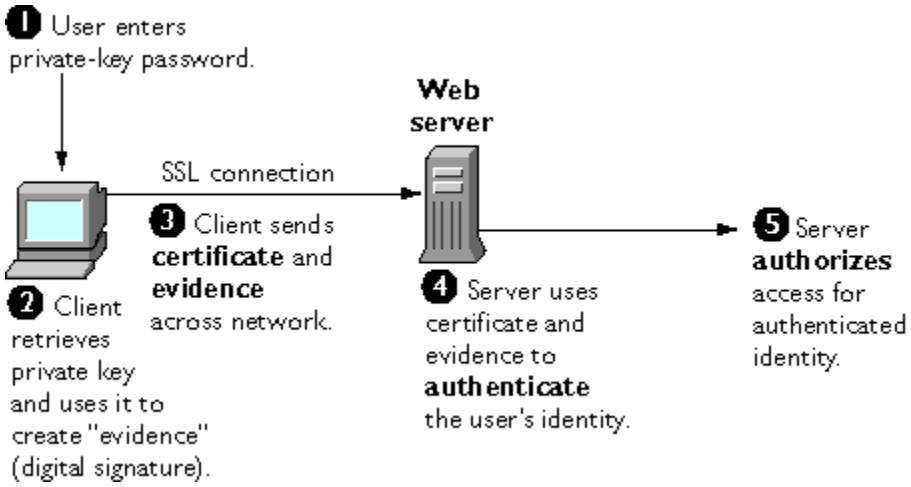
As shown in the next section, one of the advantages of certificate-based authentication is that it can be used to replace the first three steps in Figure 4 with a mechanism that allows the user to supply just one password (which is not sent across the network) and allows the administrator to control user authentication centrally.

Certificate-Based Authentication

Figure 5 shows how client authentication works using certificates and the SSL protocol. To authenticate a user to a server, a client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. For the purposes of this discussion, the digital signature associated with some data can be thought of as evidence provided by the client to the server. The server authenticates the user's identity on the strength of this evidence.

Like Figure 4, Figure 5 assumes that the user has already decided to trust the server and has requested a resource, and that the server has requested client

authentication in the process of evaluating whether to grant access to the requested resource.



Unlike the process shown in Figure 4, the process shown in Figure 5 requires the use of SSL. Figure 5 also assumes that the client has a valid certificate that can be used to identify the client to the server. Certficate-based authentication is generally considered preferable to password-based authentication because it is based on wheat the user has (the private key) as well as what the user knows (the password that protects the private key). However, it's important to note that these two assumptions are true only if unauthorized personnel have not gained access to the user's machine or password, the password for the client software's private key database has been set, and the software is set up to request the password at reasonable frequent intervals.

Neither password-based authentication nor certificate-based authentication address security issues related to physical access to individual machines or passwords. Public-key cryptography can only verify that a private key used to sign some data corresponds to the public key in a certificate. It is the user's responsibility to protect a machine's physical security and to keep the private-key password secret.

These are the steps shown in Figure 5:

1. The client software, such as Communicator, maintains a database of the private keys that correspond to the public keys published in any certificates issued for that client. The client asks for the password to this database the first time the client needs to access it during a given session-for example,

the first time the user attempts to access an SSL-enabled server that requires certificate-based client authentication. After entering this password once, the user doesn't need to enter it again for the rest of the session, even when accessing other SSL-enabled servers.

2. The client unlocks the private-key database, retrieves the private key for the user's certificate, and uses that private key to digitally sign some data that has been randomly generated for this purpose on the basis of input from both the client and the server. This data and the digital signature constitute "evidence" of the private key's validity. The digital signature can be created only with that private key and can be validated with the corresponding public key against the signed data, which is unique to the SSL session.
3. The client sends both the user's certificate and the evidence (the randomly generated piece of data that has been digitally signed) across the network.
4. The server uses the certificate and the evidence to authenticate the user's identity.

1. At this point the server may optionally perform other authentication tasks, such as checking that the certificate presented by the client is stored in the user's entry in an LDAP directory. The server then continues to evaluate whether the identified user is permitted to access the requested resource. This evaluation process can employ a variety of standard authorization mechanisms, potentially using additional information in an LDAP directory, company databases, and so on. If the result of the evaluation is positive, the server allows the client to access the requested resource.

As you can see by comparing Figure 5 to Figure 4, certificates replace the authentication portion of the interaction between the client and the server. Instead of requiring a user to send passwords across the network throughout the day, single sign-on requires the user to enter the private-key database password just once, without sending it across the network. For the rest of the session, the client presents the user's certificate to authenticate the user to each new server it encounters. Existing authorization mechanisms based on the authenticated user identity are not affected.[46]

9.7. How Certificates are used?:

[46] https://developer.mozilla.org/en/docs/Introduction_to_Public-Key_Cryptography

- Types of Certificates
- SSL Protocol
- Signed and Encrypted Email
- Form Signing
- Single Sign-On
- Object Signing

Types of Certificates

Five kinds of certificates are commonly used with Red Hat products:

- Client SSL certificates: Used to identify clients to servers via SSL (client authentication). Typically, the identity of the client is assumed to be the same as the identity of a human being, such as an employee in an enterprise. See "Certificate-Based Authentication", for a description of the way client SSL certificates are used for client authentication. Client SSL certificates can also be used for form signing and as part of a single sign-on solution.
- Examples: A bank gives a customer a client SSL certificate that allows the bank's servers to identify that customer and authorize access to the customer's accounts. A company might give a new employee a client SSL certificate that allows the company's servers to identify that employee and authorize access to the company's servers.
- Server SSL certificates**:** Used to identify servers to clients via SSL (server authentication). Server authentication may be used with or without client authentication. Server authentication is a requirement for an encrypted SSL session.

Example: Internet sites that engage in electronic commerce (commonly known as e-commerce) usually support certificate-based server authentication, at a minimum, to establish an encrypted SSL session and to assure customers that they are dealing with a web site identified with a particular company. The encrypted SSL session ensures that personal information sent over the network, such as credit card numbers, cannot easily be intercepted.

- S/MIME certificates: Used for signed and encrypted email. As with client SSL certificates, the identity of the client is typically assumed to be the same as the identity of a human being, such as an employee in an enterprise. A single certificate may be used as both an S/MIME certificate and an SSL certificate. S/MIME certificates can also be used for form signing and as part of a single sign-on solution.
- Examples: A company deploys combined S/MIME and SSL certificates solely for the purpose of authenticating employee identities, thus permitting signed email and client SSL authentication but not encrypted email. Another company issues S/MIME certificates solely for the purpose of both signing and encrypting email that deals with sensitive financial or legal matters.
- Object-signing certificates: Used to identify signers of Java code, JavaScript scripts, or other signed files. For more information, see "Object Signing".
- Example: A software company signs software distributed over the Internet to provide users with some assurance that the software is a legitimate product of that company. Using certificates and digital signatures in this manner can also make it possible for users to identify and control the kind of access downloaded software has to their computers.
- CA certificates. Used to identify CAs. Client and server software use CA certificates to determine what other certificates can be trusted. For more information .
- Example: The CA certificates stored in Communicator determine what other certificates that copy of Communicator can authenticate. An administrator can implement some aspects of corporate security policies by controlling the CA certificates stored in each user's copy of Communicator.
- SSL Protocol

The Secure Sockets Layer (SSL) protocol is a set of rules governing server authentication, client authentication, and encrypted communication between servers and clients. SSL is widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers. SSL

requires a server SSL certificate, at a minimum. As part of the initial "handshake" process, the server presents its certificate to the client to authenticate the server's identity. The authentication process uses public-key encryption and digital signatures to confirm that the server is in fact the server it claims to be. Once the server has been authenticated, the client and server use techniques of symmetric-key encryption, which is very fast, to encrypt all the information they exchange for the remainder of the session and to detect any tampering that may have occurred. Servers may optionally be configured to require client authentication as well as server authentication. In this case, after server authentication is successfully completed, the client must also present its certificate to the server to authenticate the client's identity before the encrypted SSL session can be established. For an overview of client authentication over SSL and how it differs from password-based authentication.

Signed and Encrypted Email:

Some email programs (including Messenger, which is part of Communicator) support digitally signed and encrypted email using a widely accepted protocol known as Secure Multipurpose Internet Mail Extension (S/MIME). Using S/MIME to sign or encrypt email messages requires the sender of the message to have an S/MIME certificate. An email message that includes a digital signature provides some assurance that it was in fact sent by the person whose name appears in the message header, thus providing authentication of the sender. If the digital signature cannot be validated by the email software on the receiving end, the user will be alerted. The digital signature is unique to the message it accompanies. If the message received differs in any way from the message that was sent-even by the addition or deletion of a comma-the digital signature cannot be validated. Therefore, signed email also provides some assurance that the email has not been tampered with. As discussed at the beginning of this document, this kind of assurance is known as nonrepudiation. In other words, signed email makes it very difficult for the sender to deny having sent the message. This is important for many forms of business communication. S/MIME also makes it possible to encrypt email messages. This is also important for some business users. However, using encryption for email requires careful planning. If the recipient of encrypted email messages loses his or her private key and does not have access to a backup copy of the key, for example, the encrypted messages can never be decrypted.

Form Signing:

Many kinds of e-commerce require the ability to provide persistent proof that someone has authorized a transaction. Although SSL provides transient client authentication for the duration of an SSL connection, it does not provide persistent authentication for transactions that may occur during that connection. S/MIME provides persistent authentication for email, but e-commerce often involves filling in a form on a web page rather than sending an email. The Red Hat technology known as form signing addresses the need for persistent authentication of financial transactions. Form signing allows a user to associate a digital signature with web-based data generated as the result of a transaction, such as a purchase order or other financial document. The private key associated with either a client SSL certificate or an S/MIME certificate may be used for this purpose. When a user clicks the Submit button on a web-based form that supports form signing, a dialog box appears that displays the exact text to be signed. The form designer can either specify the certificate that should be used or allow the user to select a certificate from among the client SSL and S/MIME certificates that are installed in Communicator. When the user clicks OK, the text is signed, and both the text and the digital signature are submitted to the server. The server can then use a Red Hat utility called the Signature Verification Tool to validate the digital signature.

Single Sign-On:

Network users are frequently required to remember multiple passwords for the various services they use. For example, a user might have to type a different password to log into the network, collect email, use directory services, use the corporate calendar program, and access various servers. Multiple passwords are an ongoing headache for both users and system administrators. Users have difficulty keeping track of different passwords, tend to choose poor ones, and tend to write them down in obvious places. Administrators must keep track of a separate password database on each server and deal with potential security problems related to the fact that passwords are sent over the network routinely and frequently.

Solving this problem requires some way for a user to log in once, using a single password, and get authenticated access to all network resources that user is authorized to use-without sending any passwords over the network. This capability is known as single sign-on. Both client SSL certificates and S/MIME certificates can play a significant role in a comprehensive single sign-on solution. For

example, one form of single sign-on supported by Red Hat products relies on SSL client authentication. A user can log in once, using a single password to the local client's private-key database, and get authenticated access to all SSL-enabled servers that user is authorized to use-without sending any passwords over the network. This approach simplifies access for users, because they don't need to enter passwords for each new server. It also simplifies network management, since administrators can control access by controlling lists of certificate authorities (CAs) rather than much longer lists of users and passwords. In addition to using certificates, a complete single-sign on solution must address the need to interoperate with enterprise systems, such as the underlying operating system, that rely on passwords or other forms of authentication.

Object Signing

Communicator supports a set of tools and technologies called object signing. Object signing uses standard techniques of public-key cryptography to let users get reliable information about code they download in much the same way they can get reliable information about shrink-wrapped software. Most importantly, object signing helps users and network administrators implement decisions about software distributed over intranets or the Internet-for example, whether to allow Java applets signed by a given entity to use specific computer capabilities on specific users' machines. The "objects" signed with object signing technology can be applets or other Java code, JavaScript scripts, plug-ins, or any kind of file. The "signature" is a digital signature. Signed objects and their signatures are typically stored in a special file called a JAR file. Software developers and others who wish to sign files using object-signing technology must first obtain an object-signing certificate.

9.8. Public Key Infrastructure (PKI):

A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party. A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Without PKI, sensitive information can still be encrypted (ensuring confidentiality) and exchanged, but there would be no assurance of the identity (authentication) of the other party. Any form of sensitive data exchanged over the Internet is reliant on PKI for security.

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revocation of keys and digital certificates. Digital certificates are at the heart of PKI as they affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate. A typical PKI includes the following key elements:

- A trusted party, called a certificate authority (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
- A registration authority, often called a subordinate CA, certified by a root CA to issue certificates for specific uses permitted by the root
- A certificate database, which stores certificate requests and issues and revokes certificates
- A certificate store, which resides on a local computer as a place to store issued certificates and private keys

A CA issues digital certificates to entities and individuals after verifying their identity. It signs these certificates using its private key; its public key is made available to all interested parties in a self-signed CA certificate. CAs uses this trusted root certificate to create a "chain of trust" -- many root certificates are embedded in Web browsers so they have built-in trust of those CAs. Web servers, email clients, smart phones and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs. Along with an entity's or individual's public key, digital certificates contain information about the algorithm used to create the signature, the person or entity identified, the digital signature of the CA that verified the subject data and issued the certificate, the purpose of the public key encryption, signature and certificate signing, as well as a date range during which the certificate can be considered valid.

PKI provides a chain of trust, so that identities on a network can be verified. However, like any chain, a PKI is only as strong as its weakest link. There are various standards that cover aspects of PKI -- such as the Internet X.509 Public

Key Infrastructure Certificate Policy and Certification Practices Framework (RFC2527) -- but there is no predominant governing body enforcing these standards. Although a CA is often referred to as a "trusted third party," shortcomings in the security procedures of various CAs in recent years has jeopardized trust in the entire PKI on which the Internet depends. If one CA is compromised, the security of the entire PKI is at risk. For example, in 2011, Web browser vendors were forced to blacklist all certificates issued by the Dutch CA DigiNotar after more than 500 fake certificates were discovered.[47]

9.9. Registration Authorities:

A registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. A registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. RAs are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.

Trusted certificates are typically used to make secure connections to a server over the Internet. A certificate is required in order to avoid the case that a malicious party which happens to be on the path to the target server pretends to be the target. Such a scenario is commonly referred to as a man-in-the-middle attack. The client uses the CA certificate to verify the CA signature on the server certificate, as part of the checks before establishing a secure connection. Usually, client software—for example, browsers—include a set of trusted CA certificates. That makes sense in as much as users need to trust their client software: A malicious or compromised client can skip any security check and still fool its users into believing otherwise.

The customers of a CA are server administrators who need a certificate that their servers will present to clients. Commercial CAs charge to issue certificates, and their customers expect the CA's certificate to be included by most web browsers, so that secure connections to the certified server work smoothly out of the box. The number of web browsers and other devices and applications that trust a particular

[47] http://searchsecurity.techtarget.com/definition/PKI

certificate authority is referred to as ubiquity. Mozilla, which is a non-profit organization, distributes several commercial CA certificates with its products.[1] While Mozilla developed their own policy, the CA/Browser Forum developed similar guidelines for CA trust. A single CA certificate may be shared among multiple CAs or their resellers. A root CA certificate may be the base to issue multiple intermediate CA certificates with varying validation requirements.

Aside from commercial CAs, some providers issue digital certificates to the public at no cost; a noteworthy example is CAcert. Large institutions or government entities may have their own PKIs, each including their own CAs. Formally, any site using self-signed certificates acts as its own CA too. At any rate, decent clients allow users to add or remove CA certificates at will. While server certificates usually last for a rather short period, CA certificates last much longer,[2] so, for frequently visited servers, it is less error-prone to import and trust the CA that issues their certificates rather than confirm a security exception every time the server's certificate is renewed.

A less frequent usage of trusted certificates is for encrypting or signing messages. CAs issue end-user certificates too, which can be used with S/MIME. However, encryption requires the recipient's public key and, since authors and recipients of encrypted messages presumably know one another, the usefulness of a trusted third party remains confined to the signature verification of messages sent to public mailing lists.

9.10. What to do:

Systems of defense against Internet attacks have evolved side-by-side with the aggression in a kind of serious version of the "Spy vs. Spy" cartoon series made famous by Mad Magazine. The three important actions available to individuals and businesses, however small, are 1) disciplined use of computer systems including careful password and e-mail control, 2) installation and upgrading of firewalls between internal networks and the Internet, 3) alertness to news stories about new viruses and breaches and promptly carrying out public recommendations, and 4) prompt reporting of breaches to the authorities as soon as they are detected.

The business owner has the chief responsibility to deny access to his or her systems to individuals who should not be using them. This is normally accomplished by using password control. In the modern environment we are required to use far too many passwords. Not surprisingly, we pick one we like and tend to stick with it. We use the same password for a number of different online accounts, at home, at the office. The capture of one somewhere can lead to its use elsewhere. In cases where good discipline is enforced, new passwords are issued at intervals—but people tend to forget them, with the consequence that they are often scribbled on the computer monitor lightly in pencil. Such careless practices, needless to say, are in part responsible for major breaches and much damage. Most viruses are transmitted as attachments to e-mails. Opening attachments from unknown e-mail transmitters is generally a bad idea—even when the message sounds plausible. A good rule to follow in such cases is that if the sender really wants me to open that mail, he or she will call. Idle curiosity causes many viruses to spread.

Most small businesses with networks will either engage a service firm to maintain and periodically check its system or will have in-house staff managing the function. Firewalls and virus-detection software require periodic maintenance and upgrading. Failure to do so can turn open the company's system to spammers who will use it as a transmission point—using up valuable processor power and eventually causing the company's own mail to be rejected by others—or worse. Old virus monitoring packages will be unaware of new worms, Trojan horses, and logic bombs. When news breaks indicating that some software program has a major flaw, producers of the software soon have "patches" ready to repair the vulnerability. It is a nuisance to download and install such patches, but failure to do so may be more costly. Pay me now or pay me later! Several Web sites provide free virus warnings and downloadable antivirus patches for Web browsers. Examples include www.symantec.com/avcenter and www.ciac.org. The Computer Security Institute provides annual surveys on security breaches at www.gocsi.com.

Another useful resource is the National Computer Security Association (www.ncsa.com), which provides tips on Internet security for business owners and supplies definitions of high-tech terms.

Systems breaches should be reported promptly. The business can do so by contacting US-CERT (United States Computer Emergency Readiness Team). This federal organization, formed in 2003, works with the Internet community to raise awareness of security issues and organize the response to security threats. The CERT Web site posts the latest security alerts and also provides security-related documents, tools, and training seminars. Finally, CERT offers 24-hour technical assistance in the event of Internet security breaches. Small business owners who contact CERT about a security problem will be asked to provide their company's Internet address, the computer models affected, the types of operating systems and software used, and the security measures that were in place.

For most small businesses, the Internet is a valuable resource. The effort required to play by the rules is relatively low. The costs, minimally in time, often in dollars, can be quite high even for minor problems like having one's server hijacked for spamming. When viruses destroy disks holding valuable data, costs can skyrocket. Caution, alertness, and discipline can prevent the worst of such problems. A good security policy therefore should be high on the agenda of the business owner.[48]

9.11. Summary:

Internet Security is a challenging and technical issue for all, It requires full attention of the IT experts and consensus at industry level. In this unit the concept of internet security-whom should you trust, internet research ethics, various other internet issues, encryption and decryption, certificate and authentication, how these certificates can be used and what to do are discussed at length to understand these issues with the help of relevant examples and illustrations.

[48] http://definitions.uslegal.com/i/internet-security/

9.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)

- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

9.13. Check your Progress:

A. Which of the following statements are true or false:
   a) The open nature of internet makes it vital for business to pay attention to the security of their network.
   b) Internet security is all about trust at a distance.
   c) All communication over the internet uses the Transmission on Control Protocol/Internet Protocol.
   d) Certificates work much the same way as any of these familiar forms of identification.
   e) Almost all server software permits clients authentication by means of a name and password.

B. Fill in the Blanks:

i. Internet ……..is a sub discipline that fits across many disciplines.

ii. Internet research ethics includes…… and professional standards.

iii. …….is the process of transforming information so it is un intangible to anyone but the independent recipient.

iv. A certificate is an ……used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key.

v. SMIME means…….

9.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Research Ethics
2. Data privacy and confidentiality, integrity of data, IP issues
3. Encryption
4. Electronic documents
5. Secure Multipurpose Internet Mail Extension

9.15. Terminal Questions:

1. Whom should you trust in case of Internet Security?
2. What is internet research ethics?
3. What is Encryption and Decryption?
4. Define certificate and authentication.
5. How certificates are used?

Unit-10

Accountability of Service Providers

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Accountability of Service Providers
- Understand the role of Service Providers at International Level in different countries
- Understand the technical and legal issues related to Accountability of Service Providers

Structure:

10.1. Introduction:

The advent of new forms of mass communication through technology has posed regulatory obstacles and challenges. Perhaps one of the most sensitive and problematic issues from the standpoint of the associated economic models and conflict with other constitutional rights, especially the right to freedom of expression, relates to the mechanisms for establishing liability. As is well-known, the use of digital networks has shifted the discussion regarding the multiple aspects of civil liability to a new setting, with the attendant difficulties that this brings. When it comes to the online environment, technological infrastructure does not seem to pose, at least a priori, any regulatory obstacles for the exercise of freedom of expression. Initially, with the proliferation of bulletin boards systems, and later with the emergence of mailing lists and the widespread use of email, communications became essentially decentralized and were developed through communication protocols enabling such exchanges. But it was with the technical possibilities which enabled the exchange of intangibles via digital networks and in recent years with the boom of the so-called social networks, that the regulatory importance of this infrastructure for the exercise of rights became increasingly evident. Somehow, a shared feature of these communicative acts is the need for technological infrastructure. This infrastructure, in turn, is operated by Internet services providers, which not only administer but also have power to control the flow of data across their networks. Hence the importance, from a regulatory perspective, of establishing firm criteria to ensure that net neutrality is maintained and, in this case in particular, the importance and the need to establish a system that will provide for the responsibility of those who are technically capable of controlling any uses which depart from those permitted by law. For this and other reasons, it seems that the measures taken by authorities with respect to these providers are not just desirable but also necessary to prevent any lawless actions or breaches in the course of communications taking place through this crucial infrastructure. Notably, no clear criteria have been established at the international level. In this respect, several methods have been proposed in the continent to put communications under the oversight (at least in part) of such institutions, which are still discussed with varying degree of social awareness and participation.

10.2. **Service Providers-Meaning and Definition:**

A Network Service Provider means any person who provides access to information service in an electronic form. They are the entities that provide individual and institutional subscribers with access to Internet. Section 79 of the Information Technology Act, 2000 (I.T. Act, 2000) deals with the liability of the Network Service Providers. The explanation to this section provides that 'Network Service Providers' means an 'Intermediary'. According to Section 2 (w) 'Intermediary', with respect to any particular electronic message "means any person who on behalf of another receives, stores or transmits that message or provides any service with respect to that message." Looking at the definitions, it appears that any person providing any service with respect to electronic messages including receiving, storing, transmitting it would qualify as an Intermediary. Since receiving and transmitting includes connectivity, any person providing connectivity such as an ISP or a Cyber Cafe also falls under this definition of Intermediary. But it does not mean that all intermediaries are ISPs. For e.g. a search engine like google.com is not an ISP.

Section 79 of the Act provides immunity to the ISPs in certain cases of internet wrongs even if committed through their networks provided they follow the due diligence guidelines, prescribed in detail in the Information Technology (Intermediaries guidelines) Rules, 2011 and expediently remove/disable access in case of any actual knowledge of unlawful act or on receipt of government notification to that effect. This immunity from liability, however, does not apply when the unlawful act concerns copyright or patent infringement, both of which have been specifically excluded by way of proviso to section 81 of the Act. In view of internet being one of the prime mediums for accessing, distributing and most importantly infringing copyrighted content, liability of ISPs in case of copyright infringement is fixed by the Copyright Act, 1957 mostly under Section 51(a) (ii) of the Act which, *inter alia*, holds, any person providing **"any place"** for communication of infringing work, for profit, to the public, liable of infringement unless she can prove that she was not aware or she had no reasonable grounds for believing such communication to be infringing.

10.3. **Service Providers-Global Challenges:**

Perhaps the biggest challenge for national policymakers dealing with the Internet comes from the convergence ushered in by the Net. Issues relating to the Internet economy necessarily involve inputs from the departments of commerce, broadcast media, print media, telecommunications, electronics, information, education, infrastructure, labor, and national security. Bringing together these diverse departments and finding domestic Internet policy expertise from academics or the industry is a big challenge, especially for emerging economies that have been somewhat slow to respond to the challenges of globalization and new media. Regulations governing the Internet as a medium and as infrastructure fall into the following seven categories: basic protocols, Internet service provider (ISP) infrastructure, content, user behavior, e-commerce, universal access, and national/government services. [49]

10.4. Service Providers-Indian Perspective:

The phrase "any place" has been interpreted to include web space by the judiciary making ISPs both proper and necessary parties in any copyright infringement across internet. In fact in one of the orders Madras High Court (*RK Productions v. BSNL,* Madras High Court ,Civil Suit 208/2012, O.A No. 230 of 2012) went on to suggest that without ISPs there would be no piracy across internet. Well, true but there would be no internet access as well. Hon'ble Court further expressed that since under IT Act; ISPs have the power to block any website; it is for them to ensure that any illegal or immoral content is not made available implying, a little erroneously, that it is the power of the ISPs that makes them liable for copyright infringement.

To provide relief to the ISPs the 2012 amendments to the Copyright Act introduced certain safe harbour provisions but to no avail. In a recent order by Delhi High Court in Star India Pvt. Ltd v. Haneeth Ujwal (*Star India Pvt. Ltd v. Haneeth Ujwal*, Delhi High Court, CS(OS) 2243/2014) , it was held that ISPs have an obligation to ensure that no violation of third party intellectual property rights takes place through its networks. The Court invoked the License Agreement between the Department of Telecommunications and the ISP to saddle the ISP with the responsibility of ensuring that any infringing work is not carried on its network.

[49] https://www.isoc.org/inet2000/cdproceedings/8b/8b_1.htm

Interestingly there was no mention of the recently introduced safe harbour provisions.

Indian judiciary seems to be shifting the burden of identifying infringement on ISPs which essentially is the obligation of the copyright owner ignoring the fact that ISPs lack both the institutional and logistical capacity to assimilate information of infringement across millions of URLs that can be accessed through their networks. In fact in (Kamlesh Vaswani v. Union of India *KamleshVaswani v. Union of India*, Supreme Court of India,Writ Petition (Civil) No(s). 177 of 2013), a PIL filed before Supreme Court of India in 2013 , seeking blanket ban on online pornography , ISPAI(Internet Service Provider Association of India) made an unequivocal statement before the Apex Court that without adequate legal support from the government or judiciary, ISPs cannot ban websites. Though the issue did not involve copyright infringement, however, the argument of the ISPs that "they cannot be made liable for what people do on their networks just like telecom companies are not liable for peoples' conversation" seems well founded and applicable even in instances where they are not only held responsible for copyright infringement but also obligated to identify it.[50]

Why Inadequate?: What if ISPs actually start following the regulatory mandate and start blocking websites according to their sweet will. Of course website owners can approach judiciary, argue freedom of speech and litigation can go on happily ever after. But what if website is a small start-up, wary of being involved in an expensive litigation? Who would then set right the excesses of online censorship where ISPs have an unfettered discretion in deciding who they provide access to?

Though in all the orders discussed above, judiciary has mandated ISPs to ensure no online piracy takes place, there are simply no guidelines to suggest which websites should be banned, should only infringing URLs (Uniform Resource Locators) be blocked or complete websites, what about one –off instances of infringement and do they also warrant complete ban and in case of ban - who examines its legality and what rights are available to website owners? And what if these ISPs, encouraged by such unbridled power, also start discriminating between various kinds of content, providing preferential access to some online content providers

50 http://www.mondaq.com/india/x/337668/Copyright/Indian+Regulatory+Framework+For+Internet+Service+Providers+Onerous+Yet+Inadequate

over another as per their interests and not consumers' choices? Considering that India does not have a law that makes net neutrality mandatory for ISPs it indeed is a possibility. For instance Bharti Airtel, leading ISP in India, had in 2013 tied up with Google to provide free data service up to 1GB for accessing Google search engine , Gmail and other Google + services. Considering that ISPs incur a lot of expenditure on providing an efficient bandwidth infrastructure to websites desirous of faster access, they may want to recover it by charging higher rates from them. But can such discrimination between content be justified? Wouldn't it mar the openness internet is known for. And even if allowed to an extent, it certainly needs to be regulated. But net neutrality is yet to be addressed by Indian regulatory framework pointing clearly to a regulatory gap. In the meanwhile it remains to be seen when India will do away with the ironical contrast of having an onerous yet inadequate legislation.

10.5. Internet Service Providers Association of India:

The Internet Service Providers Association of India (ISPAI) was set up in 1998 with a mission to 'Promote Internet for the benefit of all'. ISPAI is the collective voice of the ISP fraternity and by extension the entire Internet community. Over the years ISPAI has helped influence, shape and mould the telecom policies, so that ISPs and entrepreneurs in the business of Internet can setup and grow their services in an environment that is supportive and enabling. In the last 10 years of it's existence, it has been party to breaking down monopolistic structures in telecom, bringing down barriers to entry for ISPs. It helped shape India from being a bandwidth hungry to a bandwidth surplus country. it was the competitive spirit of the ISP members of ISPAI that, Internet access became so widely and cost effectively available to our countrymen. These very ISPs helped connect India to the rest of the world so effectively that today BPO and Call Centers cannot but make their global presence felt based on IP connectivity. India is today is arguably amongst the top 10 countries of the world in terms of the number of Internet users.

Today ISPAI is the recognized apex body of Indian ISPs worldwide. ISPAI has access to and interacts frequently with international bodies and platforms and is frequently consulted by them on measures for future trends and growth of

Internet. It works closely with the Government, the Regulator as well as the major Industry Chambers. It supports exchange of delegations, business visitors from across the globe which provides ISP members a chance to network widely and seek opportunities elsewhere too.

It's a platform for the Solution Provider's community such as Hardware and Software manufacturers and suppliers to gain easy access to their ISP clients, promote their products and services through personal meetings and through events supported or sponsored by ISPAI.

CODE OF CONDUCT FOR INTERNET SERVICE PROVIDERS:

1. Forward:

Start since 1998, the Internet Users in our country have grown at phenomenal rate of more than 200 % per year, and this trend is likely to continue for many years to come. It is estimated that by Mar 03 there would be approximately 30 millions Internet Users in our Country and would reach a figure of 100 millions by 2008. The Internet has thus become an important infrastructure supporting an increasingly wide spread multi-disciplinary community of researchers, scholars, businessmen, professionals, students and even households. As is true of other common infrastructure (e.g. roads, water works, power generation /distribution etc), there is widespread dependence on the Internet by its users for the support of day-to-day activities. The reliable operation of the Internet and the responsible use of its resources are of common interest and concern of its Users, Operators, Sponsors, and Society at large. It is therefore important that the Internet Service Providers understand their responsibility in this regard and follow healthy practices of self regulation. The Code of Conduct set out in this document is the voluntary response of the Internet Service Provider Association of India (ISPAI) to the rightful requirements of our Society.

2. Preamble

2.1 This Code of Conduct is open to voluntary acceptance by all Members of Internet Service Providers Association of India (ISPAI).

2.2 Members of ISPAI agree that they will abide by this Code of Conduct in letter and spirit.

2.3 Members of ISPAI understand that compliance with this Code of Conduct does not necessarily imply that they are acting within the law. Any reference in the Code of Conduct to lawfulness or unlawfulness relates solely to Indian Legal Framework.

2.4 This Code of Conduct is issued by the Executive Council of ISPAI, which is the sole authority to amend it from time to time in accordance with Rules & Regulations of ISPAI.

3. Objective

3.1. The Aim of ISPAI Code of Conduct is to enunciate and maintain high standards of Ethical and Professional Practices in the field of Internet Services.

4. Principles

4.1 In seeking to achieve its objective, the ISPAI Code of Conduct is based on the following Principles:

* Technology neutral ;
- Fair to all concerned;
- Protection of Users Data;
- Responsibility for contents on the Internet rests with the relevant Content Provider.

5. Obligatory Practices

5.1 Obligations to Law

5.1.1 ISPAI and its Members have a responsibility to adhere to law and co-operate with Law Enforcement Agencies acting within specified Indian Legal Framework.

5.1.2 Members will not knowingly permit any User or fellow Member to engage in any illegal activity in terms of the provisions of Information Technology Act 2000, ISP Policy and any other such applicable legal framework.

5.1.3 Members will follow and adhere to all jurisdictional laws pertaining to transaction reporting.

5.1.4 Members, their Services and Promotional Material will not encourage anything patently, which is in any way unlawful.

5.2 Obligations to the Public

5.2.1 Members will deal fairly with the fellow professionals and public, giving due respect to the rights and legitimate interest of others.

5.2.2 Members will endeavor to support Public Service Initiatives in harmony with the jurisdictions in which they provides their Services.

5.2.3 Members will ensure that their Services and Promotional Material does not contain anything, which may incite violence, cruelty or hatred on the basis of sexual discrimination, cast, creed or religion.

5.2.3 Members shall ensure that minors are not registered by them for Internet Services except with the explicit permission of their parents/guardian.

5.3. Obligations to own Profession

5.3.1 Members will abide by all Terms & Conditions of License Agreement in letter and spirit For Provision of Internet Services.

5.3.2 Members shall be truthful in all promotional activities and publish such information which is devoid of inaccuracies, ambiguities, exaggerations or omissions about their operations, services and pricing to the Customers and Government / Private Agencies.

5.3.3 Members will institute controls to detect and eliminate fraud and protect their data and the systems from internal and external breaches. 5.3.4 Members will co-operate with each other in investigating and preventing the instances of Hacking. .

5.3.5 Members will institute adequate control measures to prevent the unauthorized access to the resources of Internet Services.

5.3.6 Members shall ensure that that they explicitly bring to the notice of their customers, all Terms and Conditions for provision of their Services, before such customers register with the Member for their Services.

5.4 Obligations to the Customers

5.4.1. Members have a responsibility to make this Code of Conduct clear to all their Clients as well as to their Channel Partners / Distributors and indicate to them that any breached of Code of Conduct and / or violation of law will result in cessation of services.

5.4.2 Members will design and operate their Services to afford Customer's privacy and confidentiality and will post their confidentiality practices and procedures appropriately.

5.4.3 Members will follow best industry practices in offering latest Customers Filtering Software and advise them regarding any software tools, which they can use to protect their confidential data and privacy.

5.4.4 Members will follow the best industry practices in using Anti -Spamming Software, such that Customers can elect to minimize the amount of Spam sent to their e-mail account.

5.4.5 Where Internet Services involve collection of personal information such as telephone No., credit card details and addresses etc from the customers, it would be obligatory for Members to clarify to them the purpose for which such an information will be used.

6. Complaints

6.1 Since this Code of Conduct is open to voluntary acceptance by all Members of ISPAI, the Executive Council considers it prudent not to institute any Complaint Handling Procedure at the initial stage. However, this situation may be reviewed subsequently.

10.6. International Access Technologies:

The connection between your Internet enabled device and the global network is executed through a specific digital data transmission technology. It represents the transfer of information packets through an Internet Protocol route.

According to the method of data transmission, the Internet access that ISPs provide to users can be divided into several types, the most popular of which are:

Dial-up Internet access

This is the oldest method of providing access to the Internet. It uses a telephone line to perform a modem-to-modem connection. For that purpose, the user's

computer is attached to a telephone line enabled modem device, which dials into the node of the ISP and starts transferring data between the servers that store websites the user wants to see and their Internet connected device. The dial-up Internet is today considered outdated in most Internet societies due to the slow connection speed it ensures (about 40-50 kbit/s.). However, the wide availability of telephone access makes this type of Internet access the only alternative for remote areas that remain off the broadband network. It is also the least expensive Internet access service and is preferred by users on a tight budget.

DSL

DSL, short for 'digital subscriber loop' or 'digital subscriber line', is an advanced version of the dial-up Internet access method. In contrast to dial-up, DSL uses high frequency to execute a connection over the local telephone network. This allows the Internet and the phone connections to be run on one and the same telephone line. The digital subscriber line technology ensures an Asymmetric Digital Subscriber Line (ADSL), where the upload speed is lower than the download speed, and a Symmetric Digital Subscriber Line (SDSL), offering equal upload and download speeds. Of them both, ADSL is much more popular and is even known as just DSL to users.

Cable Internet

The cable Internet is among the most preferred methods for providing residential Internet access. Technically speaking, it represents a broadband Internet access method, using the high-bandwidth cable television network to transmit data between the global network and the households. To use cable Internet you will need a cable modem at home that will be connected with the CMTS (Cable Modem Termination System) of your cable ISP. The cable Internet access can be offered together with a cable television subscription and separately, for customers' convenience. The second case incurs higher subscription fees due to the extra equipment installation costs.

Wireless Broadband (WiBB)

This is a new-generation broadband Internet access technology, allowing the delivery of high-speed wireless Internet within a large area. Wireless broadband ISPs (WISPs) ensure connection speeds that come close to the wired broadband speeds provided by DSL and cable ISPs. To get wireless broadband you need to place a specific dish on your house roof or apartment balcony and point it to the

transmitter of your WISP. This type of Internet access is used as an alternative to the wired broadband connection in remote areas.

Wi-Fi Internet

Wi-Fi (from Wireless Fidelity) has become one of the most widely distributed Internet access methods, with the growing usage of portable computers and Internet enabled mobile devices, such as smart phones, PDAs, game consoles, etc. In this sense, it is the most mobile Internet access method, since you are able to use it everywhere as long as you are located within the scope of coverage, i.e. within the range of an Internet connected wireless network. Due to its ability to serve mobile devices, Wi-Fi is used in public places such as airports, hotels and restaurants to provide Internet access to customers. There are also specialized Wi-Fi hotspots where the service is either free or paid. Some of the largest cities in the world are in the process of building Wi-Fi networks that cover all the public places in the central areas.

ISDN:

Another online data transmission method worth considering is ISDN or the Integrated Services Digital Network. ISDN represents a telephone system network, integrating a high-quality digital transmission of voice and data over the ordinary phone line. Ensuring a much better data transmission over the phone line than an analog line could allow, the ISDN offers a fast upstream/downstream Internet connection speed of 128 kbit/s. This speed level can be considered as a broadband speed as opposed to the narrowband speed of standard analog 56k telephone lines.

Ethernet:

Another Internet access type worth mentioning is Ethernet - the most widespread wired LAN (local area network) technology, also used in wireless LANs. The Ethernet technology may ensure various speed levels and can thus be divided into several types: regular Ethernet, providing transmission speeds of up to 10 mbits/s, fast Ethernet, offering up to 100

mbits/s, gigabit Ethernet, supporting 1 gbit/s and 10-Gbit Ethernet, coming at up to 10 gbits/s.

10.7. Accountability and Liability of Service Providers:

When the internet first became popular in the 1990's, content creators became increasingly worried that their work would be put online and distributed without their consent (and without any return on their investment). In the real world, there's a physical cost and time investment that must be spent in copying something like a CD, and that cost is borne for each CD created. Digital content on the other hand has an almost zero "copying" cost since once the initial copy is created, millions of copies can be created without any additional cost - often with just the click of a button.

Accordingly, content providers took the stance that ISPs were similar to magazines and newspapers and must be held accountable for the material they "publish" or allowed to be published. ISPs argued that they were more akin to telephone companies, and were really just a medium to communicate through and shouldn't be held responsible for everything that passed through their system.

Ultimately, Congress stepped in and passed a series of laws including the Digital Millennium Copyright Act (DMCA), which took the side of the ISPs, but also put in place safeguards to appease content providers.

ISP's can be held liable for the copyright infringement of its users, but only in very limited circumstances. In general, there are three ways that an ISP could be liable for copyright infringement, they are:

Direct infringement : direct infringement would be if the ISP were to knowingly host copyrighted material and received a direct financial benefit from it.

Vicarious liability : an ISP could be liable vicariously if the ISP had the right and ability to control its users and received a direct financial benefit from the copyright infringement.

Contributory infringement : an ISP can be liable under a "contribution" theory of liability if the ISP has knowledge of the infringing activity and makes a material contribution (though assisting) to the copyright infringement.

Almost all cases rely on the contributory infringement theory. Direct infringement almost never occurs and vicarious liability is difficult to prove since it would be necessary to prove that the ISP had the right and ability to control its customers. Although it may be difficult to find evidence that this was the case, ISPs must still be careful because their terms of service agreement may establish that they had the right and ability to control their customers.

The DMCA generally shields ISPs from copyright infringement liability under a "safe harbor" provision. To qualify for the safe harbor's protection, an ISP must:

Lack actual knowledge of the copyright infringement;

Not be financially benefitting from the infringement;

Comply with any "notice" or "takedown" provisions for removing copyright material; and

Establish an agent for dealing with copyright infringement complaints

For example, suppose a record company named UberStars finds out that a CD by one of its recording artists has been posted on a website hosted by an ISP named MegaNet. To avoid liability, MegaNet must be unaware of the infringing material and have established an agent that UberStars can contact with a takedown notice.

Once UberStars sends the takedown notice, MegaNet must physically remove the infringing material or disable the infringing user's account and access. If MegaNet fails to either appoint an agent to contact or take the necessary steps upon receiving the takedown notice, then UberStars can sue MegaNet, and MegaNet can't use the DMCA to escape liability.

During the 1990's as the popularity of the internet grew, more and more people turned to the internet as a source of news and information which inevitably led towards the first online defamation cases. In one of the first major cases, the Drudge Report, an online site that offers political news and gossip, stated that an aide of President Clinton had a history of spousal abuse. The aide then filed suit for defamation against the Drudge Report as well as the ISP that hosted it, AOL.

If the court treated AOL as a traditional newspaper or magazine, then it would have been liable for the injuries caused by the Drudge Report's false statement. Instead, the court found that, because AOL was an ISP, it was protected by Section 230 of the Communications Decent Act (CDA). The CDA explicitly states that no ISP "shall be treated as the publisher or speaker of any information provided by another information content provider." This established the precedent that ISPs are

not like newspapers and magazines and are protected under the CDA for liability based on their user's online statements, including defamation and obscenity.

Although ISPs are generally shielded within the U.S., this is not always true abroad. The same conduct that an ISP is shielded from in the U.S. has been prosecuted in countries such as England and Germany. For example, AOL has been prosecuted for hosting defamatory remarks in England and has been prosecuted for hosting infringing material in Germany. Each country has its own laws, and these laws vary widely from country to country. Accordingly, because the internet is international in its reach, it's extremely important to know exactly what is and isn't protected in countries where you expect people to view your content.51

10.8. **Types and Categories of Service Providers:**

Internet Service Providers (ISP's), which first began to emerge in the late 1980s and early 1990s, are the businesses and organizations that provide users with Internet access and related services. These providers connect customers to customers of other service providers by way of networks. Often, Internet Service Providers (also called Internet Access Providers) are companies that provide telecommunications services including data communications access and telephone connection. The majority of telephone companies now function as Internet Access Providers as well. ISP's may be commercial, non-profit, privately owned or community-owned.

There are quite a few different types of Internet Service Providers available today, including access, mailbox, hosting, transit, virtual and free.

Access ISPs — Employ a variety of technologies to facilitate consumers' connection to their network. These technologies may include broadband or dialup. Always-on types of broadband connections comprise cable, fiber optic service (FiOS), DSL (Digital Subscriber Line) and satellite. A number of access providers also provide email and hosting services.

51 http://smallbusiness.findlaw.com/intellectual-property/isp-liability-for-the-acts-of-its-customers.html

Mailbox ISPs — Offer email mailbox hosting services and email servers to send, receive and store email. Many mailbox ISPs are also access providers.

Hosting ISPs — Offer email, File Transfer Protocol (FTP), web-hosting services, virtual machines, clouds and physical servers.

Transit ISPs —Provide large amounts of bandwidth needed to connect hosting ISPs and access ISPs together.

Virtual ISPs (VISP) — Purchase services from other ISPs to allow customers Internet access.

Free ISPs (freenets) – Provide service free of charge and often display advertisements while users are connected.

To connect your computer to the Internet, you will need an Internet Service Provider (ISP). Some companies limit their service to providing Internet access only. Others, such as a telephone or cable company, may offer Internet access as part of a larger package of services. Consider these factors when selecting a provider:

- **Speed.** If you only want to check email and read web pages, a dial-up connection may be enough. But if you want to download music or television shows or watch videos, you will need a faster connection with broadband access, such as a digital subscriber line (DSL), cable modem, or satellite.
- Availability: Which companies offer service in your area?
- Wireless access: Can you get a wireless connection for other computers in your home?
- E-mail: Do e-mail accounts come with the service? What will be the storage limit on your mailbox?
- Software: Is any software required to activate the service?
- Support: What kinds of support are available: phone, e-mail, chat, etc.? Is the support free?
- Special Features: What services are provided for spam blocking, virus protection, instant messaging and chat rooms?

- Terms of Service: Is there a limit to the amount of data you can use per month?
- Cost: What is the monthly fee for the service? Are there fees for renting a modem or set up?[52]

10.9. Case Study:

Human Rights and Internet Intermediary Regulation in Chile: On May 4, 2010 the Chilean Congress adopted a ground-breaking new law regulating Internet intermediaries' liability for online copyright infringement done by their users. This law implements Chile's obligations concerning Internet Service Providers' role in online copyright enforcement under the 2004 Chile – U.S. Free Trade Agreement. The law requires a judicial order before Internet Service Providers are required to take down allegedly copyright-infringing material from websites, disclose customer information, or terminate customers' Internet accounts.

Chapter III of the Intellectual Property Act (Articles 85L-85U) provides a set of harbors for network service providers. [LINK to Chile page] If Internet service providers comply with the conditions set out in the legislation they are exempt from financial sanctions arising from copyright infringement claims. However, Internet intermediaries are still subject to injunctions, and other reasonable judicial measures aimed at blocking online access to particular alleged copyright-infringing content.

Chile's ISP law has a unique feature that sets it apart from other similar regulatory frameworks in other countries. Chile's notice and take down procedure is subject to a final review by a judge, rather than left to the individual ISP's discretion.

This framework is grounded in Chile's human rights obligations as a signatory to the American Convention on Human Rights (sometimes referred to as the San José Pact), and in foundational principles in Chile's Constitution.

This document outlines the international human rights obligations that underpin the judicial order approach to Internet intermediary regulation taken by the Chilean government. This framework is of equal relevance to other Latin American countries that are signatories to the American Convention on Human Rights, and

[52] http://www.comcast.com/resources/internet-service-providers.html

which are party to trade agreements with the U.S., including bilateral agreements (the Chile-U.S. FTA, Peru-U.S. FTA, Colombia – U.S. FTA, [Panama – U.S. FTA]), regional agreements (CAFTA-DR), or plurilateral agreements (ACTA)); or are in the process of negotiating trade agreements with the U.S. that include provisions on ISP liability for intellectual property infringement (the Trans-Pacific Partnership Agreement).

All U.S. Free Trade Agreements since 2002 have included detailed provisions governing ISP liability for copyright infringement in the enforcement section of the chapter on intellectual property. The provisions require signatory countries to provide "legal incentives for service providers to cooperate with copyright owners in deterring the unauthorized storage and transmission of copyrighted materials" (whether or not the trading partners' national law recognizes secondary liability for copyright infringement), and to establish limitations on ISP liability where ISPs comply with detailed conditions set out in the FTA.

Although there is no obligation in any current international intellectual property treaty governing Internet service provider liability for copyright infringement, the U.S. FTAs frame these provisions as requirements for countries to implement their existing obligations as members of the World Trade Organization, under the 1994 Agreement on Trade-Related Aspects of Intellectual Property (TRIPs). The provisions in each agreement begin with wording that precisely mirrors the language of Article 41 of TRIPs:

For the purpose of providing enforcement procedures that permit effective action against any act of infringement of copyright covered under this Chapter, including expeditious remedies to prevent infringements and criminal and civil remedies, each Party shall provide, consistent with the framework set forth in this Article...

Article 17.10.23 of the intellectual property chapter of the U.S.-Chile FTA requires Chile and the U.S. to provide safe harbors against liability for copyright infringement for Internet intermediaries that make cache copies, host content at users' request, offer search services and provide links and other location tools, on the condition that they take down alleged copyright-infringing content upon receiving a valid notice from a copyright holder.

Paragraph (f) of that Article provides that:

For purposes of the notice and take down process (…) each Party shall establish appropriate procedures through an open and transparent process which is set forth

in domestic law, for effective notifications of claimed infringement, and effective counter-notifications by those whose material is removed or disabled through mistake or misidentification.

The U.S.-Chile FTA thus gives Chile and the U.S. considerable flexibility in how they implement the notice and takedown system. The requirement for "effective notifications" and "appropriate procedures" does not restrict the process to notices from private parties or administrative bodies. Given that a private party notice and takedown procedure could potentially be in conflict with the requirements for due process and judicial protection of citizens' human rights guaranteed in the Chilean Constitution and ACHR, the conclusion arrived at by the Chilean Congress and reflected in the 2010 Intellectual Property Act was that ISPs would only be required to take down allegedly infringing content upon receipt of an order from a judge, after a judicial review. .The Chilean Congress believed that this framework would provide the necessary protection for the constitutionally-guaranteed fundamental rights of citizens, while implementing Chile's obligations in the Chile-U.S. FTA.

Not Just Chile - The Relevance for Other Countries: The framework of constitutional protections and fundamental rights guarantees described above applies equally to other Latin American countries that are signatories to the American Convention on Human Rights, and other countries that have similar obligations under other regional or international instruments. Accordingly, Chile's judicial order approach to implementing ISP regulation may also be available to other countries that are considering mechanisms for implementing online intellectual property enforcement obligations in bilateral, regional and plurilateral agreements in a way that best protects citizens' rights of due process, freedom of expression, and privacy.53

10.10. Asia Pacific Regional Internet Governance Forum:

Today, Asia has the strongest growing demand for Internet addresses. That is more and more people in Asia are using the Internet. In contrast to North America and Europe, demand for the Internet in Asia is not only growing, but also growing at an accelerating rate. **Asia Pacific Regional Internet Governance Forum**

[53] https://globalchokepoints.org/human-rights-and-internet-intermediary-regulation-chile

(APrIGF) serves as a platform for discussion, exchange and collaboration at a regional level, and also where possible to aggregate national IGF discussions, ultimately advance the Internet governance development in the Asia Pacific region. In 2010, while the global IGF is already in its fifth and final year of its initial charter, and Regional IGFs have been established in many other regions, including Africa, Europe, Latin America and the Caribbean, to date, Asia has seen no parallel forum for discussing Internet governance issues at a regional level. For the first time, the APrIGF is therefore being convened with objectives to raise awareness and encourage participation from relevant stakeholders around the region on Internet governance issues, as well as to foster multi-lateral, multi-stakeholder discussion about issues pertinent to the Internet in Asia. The multi-stakeholder approach is a core principle of the APrIGF with the emphasis on the diversity of participants and openness of the discussion. Valuing the youth as an important stakeholder and the future generations of the Internet, a Youth IGF also become an integral part of the APrIGF whereby they are held in parallel annually featuring a simulation of the multi-stakeholder discussion model among the young people on various Internet governance issues.

What is Internet Governance Forum (IGF)?: Building on the United Nations (UN) Millennium Development Goals, and the mandate given at the Second Phase of the World Summit on the Information Society in Tunis in 2005, the IGF (Internet Governance Forum) is a United Nations activity initiated in 2006 as a global platform for multi-stakeholder policy dialogue on prevailing and emerging issues on Internet governance so as to foster the sustainability, robustness, security, stability and development of Internet. The annual Forum was previously held in Greece (2006), Brazil (2007), India (2008), and Egypt (2009), Lithuania (2010), Kenya (2011), Azerbaijan (2012). The Internet has become an integral part of people's life. Despite the advantages, misuses and abuses lead to social problems, such as digital divide, Internet addiction, information safety, security, privacy and other evolving issues. These issues have no respect to national borders, and therefore require collaboration between countries and territories to address. The IGF approach is an open forum for knowledge sharing between stakeholders across borders, which in turn inform local policy development.[54]

[54] http://www.aprigf.asia/about.html

10.11. Summary:

Internet Service Providers all over the world having so many issues and there is no one legal framework at national and national level to deal the problems of this sector. In this unit the concept of service provider-meaning and definition, global challenges before the service providers, the service providers in Indian perspective, The role and importance of Internet Service Providers Association of India, International access technologies, accessibility and liability of the service providers and types & categories of service providers are discussed at length for better understanding and clarity on the point.

10.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)

- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

10.13 Check your Progress:

A. Which of the following statements are true or false:

a. The advent of new forms of mass communication through technology has posed regulatory obstacles and challenges.

b. A search engine like google.com is not an Internet Service Providers (ISP).

c. The phrase “any place” has been interpreted to include web space by the judiciary.

d. ISP has an obligation to ensure that no violation of third party intellectual property rights takes place through its network.

e. DSL, short form ‘digital subscriber loop’ or ‘digital subscriber line’, is an advanced version of the dial-up internet access method.

b) Fill in the Blanks:

i. A Network Service Provider means any person……in an electronic form.

ii. ……of the IT Act, 2000 is related to liability of Network Service Provider.

iii. The IT Act, 2000 provide immunity to the ISPs in certain cases of internet wrongs even if it committed through their network provided they follow the ……...

iv. The Internet Service Providers Association of India was set up in…….with a mission to "promote internet for the benefit of all".

v. ……has become one of the most widely distributed internet access method.

10.14 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Who provides access to information
2. Section 79
3. Due diligence guidelines
4. 1998
5. WI-Fi (from Wireless Fidelity)

10.15 Terminal Questions:

1. What is the meaning and definition of Service Providers?
2. What is the position of service provider in Indian Perspective?
3. Write a note on Internet Service Provider Association of India.

4. What is the accountability and liability of service provider?
5. Discuss various types and categories of service providers.

Unit-11

Protection of Contents on Website

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Protection of Contents on Website
- Understand the concept with reference to use of Web Content
- Understand the technical and legal issues related to Protection of Contents on Website

Structure:

11.1. Introduction:

Protecting your website against theft is now considered mandatory for website owners. This is especially important for websites which are "content heavy" -

pictures, graphics, video, etc. Same as the "bricks and mortar" world, there is no 100% guarantee against online theft but there are many things you can do to protect yourself and your site. Most theft online occurs is because it is "easy" to do it. Just like leaving your front door open or your car unlocked, if you make it simple for thieves they will take advantage it.

11.2. Website Contract:

Web site terms of use or terms of service agreements represent one of the most important legal strategies for protecting content on the Internet. These agreements, whether in the form of click wrap or browse wrap agreements, are generally binding, valid, and enforceable. To be enforceable, it is critical that users have an opportunity to review the terms of use applicable to the site. If they are buried or otherwise inconspicuous, they will be more difficult to enforce. Web site terms of use should be used to manage, allocate, mitigate, limit, and avoid the legal risks related to content and to protect the intellectual property rights and other property rights in and to such content. For purposes of this article, content includes content owned by the site as well as third-party content licensed or otherwise provided to the site. Content also includes content submitted by users. Contract provisions in the Web site terms of use agreements should deal with all forms of content and the legal risks related to each form of content. The contract terms are the first level of legal defense for protecting content on the Internet.

Typically, the Web site terms of use will state in essence that: "Your use of the Web site, content and services offered on or through the Web site are subject to the terms and conditions in this Web site Terms of Use. By using the Web site, you are agreeing to be bound by and comply with the Web site Terms of Use." The Web site owner usually reserves the right to change the terms at any time to allow for new services, new concerns, and flexibility in the dynamic Internet arena. Continued use of the Web site following the posting of changes to the terms usually means that the user accepts the changes.[55]

[55] Westermeier, J.(Jay) T., The Computer & Internet Lawyer, Protecting Content on the Internet (June,2009); www.google.co.in

Content Access and Use

Web site terms of use should provide restrictions on the use of content. Typically, the term "content" will be defined broadly to include, but not be limited to, all materials, information, text, graphics, images, logos, photographs, illustrations, audio clips, video clips, and audio visual material available on the Web site. The definition of content often will include specific examples of the type of content included on the Web site. The Web site terms of use agreement is also used to provide notice that the content is protected by copyright and other intellectual property laws and that the Web site owner, its affiliates, or third-party licensors own the content. Most terms of use agreements license the applicable Web site to use third-party content submitted to the site by the user broadly.

After defining "content" and providing notice of ownership and copyright protection, the Web site terms of use will provide restrictions on what users are permitted to do with the content. An example of this type of restriction and permitted use provision is the following:

Limitations on Use: You may not modify, publish, copy, transmit, transfer, sell, reproduce, create derivative works from, license, distribute, frame, hyperlink, download, repost, perform, display or in any way commercially exploit any of the content; provided, however, you may download one copy of the content for your personal, non-commercial use only, provided that you keep intact all copyright and other proprietary notices. This provision grants a restricted copyright license permitting the user to download content for the user's personal, non-commercial use. This type of limited copyright license for content is common.

In *Southwest Airlines Co. v. BoardFirst, L.L.C.*, the court found that BoardFirst had breached Southwest's restriction to use the Web site only for "personal, non-commercial purposes." The court concluded that if BoardFirst was profiting from the deal whereby BoardFirst used the Southwest Web site to obtain Class A boarding passes for passengers, then its use would be for commercial purposes. The general rule is that, if the user exceeds the scope of the copyright license, the Web site owner may bring legal action against the user for breach of the Web site terms of use agreement and copyright infringement for unauthorized use of the content, provided that the copyright claims in and to the content have been registered with the US Copyright Office. The objective of the legal strategy is to make contract remedies as well as copyright infringement remedies available if

necessary. The greater the number of legal remedies available, the more flexibility a company will have in combating content thieves.[56]

11.3. Password Restricted Contents:

Password-Restricted Content: Some Web sites may contain password-restricted areas. Restricted areas may make it possible to protect the content in these areas by copyright and trade secret protection. Typically, the Web site terms of use agreement will provide that, if the user is registered as an authorized user to gain access to the password protected areas of the Web site, the user will agree to be entirely responsible for maintaining the confidentiality of its password and agree to notify the Web site if the password is lost, stolen, disclosed to an unauthorized third party, or otherwise may have been compromised. Password protection provides another layer of protection for content that may be useful in some circumstances. The confidentiality restrictions imposed on the user may create a relationship of confidence and trust with the user consistent with the use of trade secret protection. Content Submissions Many e-commerce business models and social networking sites encourage user submissions or user content. In most cases, the user retains ownership of his or her submitted content but grants the Web site a very broad license to use the user content. An example of this type of license follows.

By posting, uploading, inputting, providing or submitting your User Content to the Web site you are granting the Web site, its affiliated companies and necessary sub licensees permission to use your User Content in connection with the operation of the Web site business and activities, including, without limitation, the license rights to copy, distribute, transmit, publicly display, publicly perform, reproduce, edit, translate and reformat your User Content; to publish your name in connection with User Content; and the right to grant such rights to any supplier of services in connection with this Web site. This provision is a broad copyright license and also addresses potential publicity rights concerns. There are a number of other legal concerns that are frequently addressed in Web site terms of use agreements in connection with user-content submissions.

[56] Ibid

One is that the Web site owner will specifically provide that no compensation will be paid with respect to the use of user content and that the Web site owner is under no obligation to post or use any content that a user may provide and may remove any user content at any time in its sole discretion. It is very important to be able to take down or disable access to user content that may be infringing or otherwise violate the Web site terms of use. Contract provisions must be consistent with takedown obligations under the Digital Millennium Copyright Act.[3]

Scrapers, Bots, Crawlers, and Spiders: Preprogrammed bots that scrape and collect content from other sites sometimes target content. A company with an online presence needs to consider its bot policy and protection scheme as part of its overall content protection scheme, including the use of the robots.txt protocol to disallow all bots or specific bots. A company also should consider using a contract prohibition consistent with the bot policy to guard against data mining, scraping, robots, and similar content gathering or content extraction methods, such as the following:

Use of any robot, spider, site search, retrieval application or other manual or automatic device to retrieve, index, scrape, data mine or in any way gather or extract content on or available through the Site or reproduce or circumvent the navigational structure or presentation of the site without Web site Owner's express written consent is prohibited. Note that an express written consent could be set forth in the bots that are allowed in connection with the robots.txt declaration. It is important to avoid any conflicts between the contract terms and your policies.

Representation Respecting User Content: Another contract provision related to user content is for the user to provide a warranty and representation respecting the content submitted. An example of this type of provision follows. By posting, uploading, inputting, providing or submitting User Content you warrant or represent that you own or otherwise control all of the rights to your User Content as described in these Web site Terms of Use including, without limitation, all the rights necessary for you to provide, post, upload, input or submit your User Content submissions.

11.4. Display Copyright Notice to Help Prevent Content Theft:

Any thief intent on copying your material will not be thwarted by this, but I believe that it does serve to reduce theft to a degree. It also will help to protect you in the future if you need to contest the theft, by proving that you have a particular copyright date associated with your material. If you research copyright law, you don't need to have LITERALLY filed the copyright, but merely that you have displayed the copyright notice. This is because the actual filing of a copyright can be retroactive to a prior date.

Here is the traditional copyright notice format:

COPYRIGHT—– COPYRIGHT SYMBOL—— DATE—— COPYRIGHT OWNER

so that would look like this:

Copyright © 1989 My Name

The above format works for USA copyright law. However, in other countries and also for US residents who want to protect their intellectual property in other countries, it is recommended that you add "All Rights Reserved."

So the preferred format would look like this:

Copyright © 1989 My Name

All Rights Reserved

Display a Strong Warning Help Prevent Content Theft

Use text or a graphic that says clearly that copying your material is prohibited. Here are some examples to use as a reference point:

WARNING! COPYING PROHIBITED

WARNING! COPYING PROHIBITION ENFORCED

WE WILL PROSECUTE ALL INTERNET THEFT OF OUR COPYRIGHTED MATERIAL

PLEASE DO NOT COPY OUR TEXT OR IMAGES WITHOUT OUR PERMISSION

WE'RE CRACKING DOWN ON INTERNET PIRACY — DO NOT COPY OUR CONTENT

STEAL OUR CONTENT, WE'LL STEAL YOUR HAPPINESS

DO NOT COPY OUR MATERIAL

COPYING PROHIBITED

NEVER RE-POST OUR MATERIAL ON YOUR WEBSITE OR BLOG

There are actually “official” badges and widgets that you can get that do this from a few companies like CopyScape.com and our own, StopWebPirates.com

Disable Right-Click

If you have an image that you do not want people to copy, or text that you do not want people to copy, there is a way to add a bit of code to the page using Javascript to do this. But then legitimate users will be frustrated and annoyed by your decision to do this. So it is not an easy decision. Also, a crafty theft can always “view source” code and STILL get access to your text and image, so this method is definitely not fool-proof. Having said that, it will certainly deter a lot of casual copying that would occur and this may help you out.

Add the following code WITHIN the body tag to disable the mouse right-click AND keyboard copy functions.

The above solution works in most browsers, but not in all.

Embed Content in Flash

Flash can display your content and it is very difficult to copy. But the problem is that search engines do not see flash at this time and you will risk low search engine ranking.

Reduce Auto-Copying Spam Bots

Sometimes the worst offenders are automated spambots. Unfortunately, ALL of the suggestions in this section will seriously interfere with your search engine ranking. But it is worth including for situations where this is not a concern.

- Place an .htaccess file in each directory that you want to protect. An .htaccess files do many things, but in this case, it can ban specific web robots and even ban visitors with specific IP addresses and countries! Here is a great article on exactly how to do this.
- Use a Meta Tag to prevent robots from indexing your page. Place the following code into the portion of your page:
- Embed content within frames
  Search engines do not “see” content in frames so this will reduce spam bots, but also reduce your SEO.
- Password-Protect the directory that contains the web page that you want to protect.
  Clearly, nobody could copy it unless you issued the password. But, of

course, your page also won't display on search engines, so you have to really think if this is what you want. Here is a good article on how to do this.

- Use HTML Encryption Just do a search for "html encryption" and find one of many encryption generators where you just paste your html code in and receive the encrypted version. Re-paste this code to your site. The browser will display it, but spambots won't see it. (Unfortunately, search engines won't see it either!)

Use Absolute Links to Internal Pages of Your Site

Most people who steal your content will just grab it and post it on their site without adjusting the links within. If you have relative links like this:

/articles/my_amazing_ info (This is a "relative link.")

then you won't have the benefit of them linking back to your site. (At least if they have stolen your work, it would be good if they link back to you!)

But if you make your hyperlinks like this:

http://www.yourdomain.com/articles/my_amazing_ info (This is an "absolute link.")

Then at least you will get some traffic to your site and your SEO will be INCREASED.

Watermark Your Images

This is where you see a faint logo or text placed OVER the image, so that if someone tries to copy it, it will RETAIN your name or logo, or whatever you use as your watermark. There are many software programs that can help you do this. AiS Watermark Pictures Protector is one of the best watermarking programs, giving you the most control.

Use HTML Protection Software

Normally, this approach shouldn't be necessary if you implement some of the strategies listed above. But it is very handy to have a "one-stop-shop" approach if that is what you prefer.

Here are two that are high quality:

HTML-Protector

HTML Protector from AntSoft

How to Deter Image and Bandwidth Theft

"Hotlinking" is when people display your image on their website or blog by linking to the actual image on YOUR website. So even if you have granted permission to use the image, they are still "stealing" your bandwidth and slowing your own site down and costing you money. David Airey came up with a very creative solution to deal with this issue. You can see his approach here.

Another way to work around this issue is to host your images and photos on a free image-hosting site like Flikr or Picasa so that if people DO hotlink to the image, it won't slow down your servers or use up your bandwidth.

Force Thieves to at Least Link Back to You To Help Increase Traffic and SEO

Free service from EmbedAnything forces anyone copying your material to include code that links back to you. Very cool.

What if Your Content is Not Digital But Illegal Digital Copies are Being Distributed Over The Internet?

For example, what if you have written a book that is ONLY in physical form but someone made a .pdf version of this book and now you see this unauthorized digital "ebook" given away for free on hundreds of filesharing sites? That can be so frustrating. So this is not going to stop the most hardened criminal, but it is worth it to post the following warning to somewhat stem the tide:

WARNING!

This book is in printed format only. ALL DIGITAL VERSIONS ARE UNAUTHORIZED. If you upload or download an ebook version of this work, you are committing a crime and causing hardship for the author. For additional copies of this book, please see our website which will list legitimate sources to purchase: http://www.yourwebsite.com

It is suggested that you place the above warning on the title page of your book or somewhere prominently in the beginning.[57]

11.5. Fair Use Law:

Fair use provisions of the copyright law allow for limited use or distribution of copyrighted material without the author's permission. Examples of fair use of copyrighted materials include quotation of excerpts in a review, news reporting, research, or copying of a small part of a work by a teacher

[57] http://www.stopwebpirates.com/articles/protect-website-content

or student to illustrate a lesson. There is a gray area as far as how MUCH material be copied and still be considered "fair use." There are four guidelines that are usually considered in these cases:

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes. Generally, if it is for nonprofit, educational or personal uses, it is considered fair use. If it is for commercial use, then it is not.
2. The nature of the copyrighted work. If what is being quoted is factual, then it is more likely to be fair use.
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
4. The effect of the use upon the potential market for, or value of, the copyrighted work. If the copyright owner cannot be determined, then it is considered fair use, but if the material infringes on the copyright owner's sales, then it is not.

11.6. How to check if your Content Stolen[58]?:

Here are some easy tips on how to check if people have copied your copyrighted digital material on their website. Lately, people put up a website and think nothing of stealing your content. This could be the literal text of your web page that is being copied. Or, it could be FILES on your website that are also being copied and given away for free or even sold without your knowledge. You need to protect your intellectual properties by using automated duplicated content checkers or by manual techniques. With just a little effort, you can set up a variety of plagiarism checkers that will help give you peace of mind.

Manually Scan the Web for Matches to Your Page

Why can't you just type the text into google? Because google has a maximum of 32 words that you are allowed to check in one search. Many times this might be enough but what if you want to check to see if a larger amount of text is stolen?

[58] http://www.stopwebpirates.com/articles/check-stolen-content

There are many free and paid web services available for tracking and scanning your pages to check if any possible content is being stolen anywhere in the web. Some services which I suggest are:

http://www.copyscape.com

http://www.plagiarismchecker.com/

http://www.plagium.com/

http://plagiarisma.net/

Use Google Images to look for copies of your images.

Remember to use quotes around your material. So instead of typing this in:

The story of my amazing life in New York City

Type this:

"The story of my amazing life in New York City"

The reason is that with most search engines and plagiarism checkers, you want to check for ADJACENT words. Otherwise, you will get all the sites that have THE and STORY and OF and MY and AMAZING, etc. rather than those words being next to each other.

Embed Your Post With Trackable Identifiers

- Filenames. Try to use creative or unusual filenames, that sometimes might even include intentional misspellings. This way, you can search for such a file and find it more readily than a more commonly-named file.
- Create a trick link to a page of your site. Most people will just copy your material as is and not take the time to update everything. You can track inbound links with link checker sites or through your own server and thus find sites that have copied this link. The link could be a link that ONLY goes to a page of your site for this purpose, rather than to your home page, which would be harder to distinguish from legit sites.

Use a Plagiarism-Tracking Plugin

If you have a CMS-based website, like WordPress, you can easily add copy-protection software with a plagiarism-tracking plugin.

http://wordpress.org/extend/plugins/tags/plagiarism for a current list

Digital Fingerprint

Create Control Over How People Can Use Your Content

The following are WordPress plugins to help ALLOW people to copy your material in exchange for receiving proper credit or even payment!

Embed Article

iCopyright(R) Article Tools – Identify websites that re-use your content without permission and request takedown or convert them to customers.

Use An Automated Warning System

Automatic notification alerts are usually not free. But they are so very helpful because they track illegal postings of your work and send you announcements with each infraction.

http://www.google.com/alerts

http://www.copygator.com

http://plagiarismanalyzer.org

http://checkforplagiarism.net

Use Your Web Stats to Observe Inbound Links

- Use Absolute Links for HTML Pages: An absolute link is the complete URL, for example http://www.yourdomain.com/folder/page.htm. If you use relative links, it is very easy for a plagiarist to copy your web site or individual web pages to a new domain. Absolute links would require the plagiarist to work harder to remove or change all of your absolute links. Remember, a plagiarist is lazy. If the plagiarist fails to change or remove all of your links, your web stats could alert you to your stolen web content.

11.7. Copyright of Web Contents:

Copyright protection is a very important part of the program to protect content. The copyright laws protect original content. Copyrights subsist in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Originality and fixation in tangible form are the two fundamental criteria for copyright protection. Copyright rights occur *automatically* from the moment of creation and fixation in tangible form.

Originality is a constitutionally mandated prerequisite for copyright protection. For content to be considered "original," it cannot be substantially copied from another

work and it must demonstrate a modicum of creativity. This originality requirement is relatively easy to meet. The requirement does not demand that novelty or uniqueness be present. No artistic merit or beauty is required. The creativity threshold for copyrightability is quite low. A work is original in the copyright sense if it owes its originality to the author and was not copied from some preexisting work. Original content is likely to meet the originality requirements for copyright protection.

A work can incorporate existing material with the permission of the author and still be original. When an existing work is included in a new work, the copyright on the new work extends only to the original material contributed by the author. If the content on the Web site is not original, the Web site owner may still have a copyright in the compilation of the content. For compilations such as databases the originality may extend only to the selection, coordination, and arrangement of the content. If the Web site owner has contributed original content, the copyright will extend to the text, photos, graphics, and other original expressive content contributed as well as to the selection, coordination, and arrangement of the content. If the Web site owner has not contributed any original expressive content, then the Web site owner may need to rely upon a compilation copyright. For example, facts are not protectable by copyright. If the Web site owner contributes only factual content and third-party content, then under such circumstances the Web site owner may be able to use only a compilation copyright.

11.8. Copyright Registration of Web Contents:

The Copyright Office has established procedures for the copyright registration of online works made available over a communications network such as the Internet. These procedures apply to works accessed via the Internet such as Web sites, homepages, and FTP sites and files and documents transmitted and/or downloaded via the Internet. These procedures are contained in Copyright Office Circular 66-Copyright Registration for Online Works. It is also possible that Web site copyright claims may be registered in some circumstances as computer programs or as an automated database.

For all online works other than computer programs and databases the registration will extend only to the copyrightable content of the work as received in the

Copyright Office and identified as the subject of the copyright claim. For published works, the registration should be limited to the content of the work asserted to be published on the date given on the application. In other words, if you change the content after registration, the registration will not cover the new content.

If the registration is for a computer program that establishes the screen displays when a Web site is viewed (such as a program written in html), the registration will extend to the entire copyrightable content of the computer program code. The registration, however, will not extend to any Web site content generated by the program that is not present in the identifying material received by the Copyright Office and that is not described on the application. For all other computer programs that are transmitted or accessed online as well as for any online automated databases registered, the registration extends to the entire copyrightable content of the Web site (or other online work) owned by the Web site owner, even though the entire content is not required in the identifying material deposited.

One of the problems that must be addressed in any copyright registration program for Web site content is the frequency of the revisions and updates to the Web site content. Generally, copyrightable revisions to Web sites and other online works that are published on separate days must each be registered individually, with a separate application and filing fee unless the online work meets the group registration requirements for an automated database or newsletter. If the Web site content does not change significantly from day-to-day, a company can adopt a registration strategy limited to major updates. Another strategy if there are significant new content changes is to register the revised Web site every week or every month depending on the extent of the new content. A copyright registration strategy should reflect a cost/benefit analysis based on the value of the copyrightable content and the risks related to its infringement.

11.9. Disclaimer regarding Web Contents:

Disclaimers: Specific disclaimers can be used based on the nature of the content. Usually, these disclaimers are included in the Web site terms of use. They should be part of your contractual protection. One content risk relates to the accuracy of the content and the possibility of errors. For example, content providers often state that they do not warrant the accuracy, usefulness, reliability, timeliness, legality, or completeness of any of the content provided on or through the site, and do not warrant that the site will operate error-free, or that defects, errors, or omissions will be corrected, or that the site is completely secure. Similarly, one commonly used disclaimer in connection with the legal risks relating to displaying content states that the site visitors' use of content on the Web site is at the visitors' own risk and the content provided on the Web site is provided "AS IS" and "AS AVAILABLE" without any warranties as to the availability of the site and the accuracy of the content provided. These disclaimers seek to guard against detrimental reliance on the content provided. In particular, the disclaimers seek to minimize detrimental reliance by cautioning the user not to rely blindly on the content. Disclaimers may prove effective to guard against agreements created by implication since the disclaimer expressly contradicts the implications. You should use disclaimers to negate possible implications expressly.

Another use of disclaimers is to disclaim any responsibility for third-party content accessible from a Web site via links to other Web sites. With respect to links, it is also usually prudent to state that the Web site does not intend links on the site to be referrals or endorsements of the linked entities or any products or services provided by the linked entities. Disclaimers are part of an overall strategy to manage risks related to content. Merely placing disclaimers on the homepage of a multi-page site may not be sufficient, however, since visitors can access various parts of a Web site directly and different parts of a Web site may need different disclaimers based on the nature of the content, the jurisdiction to which the portion of the site is directed, and other considerations. It is also prudent in designing a Web site to provide a prominent link to Web site disclaimers and terms of use at the bottom of each Web page to emphasize their applicability to all content located anywhere on or accessible through the Web site and guard against possible deep-linking. At the same time, this practice ensures that each page from the site that is printed out by a visitor includes a reference to the disclaimers and terms of use.

Proprietary Legends: Another aspect of protecting content on the Internet is the use of trademark, copyright, and other intellectual property legends. A proprietary rights notice or legend on the homepage may not be included on specific interior pages unless referenced on each applicable page. One approach is to consider including a corporate logo on each page of a Web site so that there is no confusion as to with whom the customer is dealing as well as applicable proprietary notices and legends. In addition to your copyright notice, you may want to expressly state: "No part of this content included on this site may be reproduced, republished or redistributed without the prior written consent of the Web site Owner" and note that use of the site is governed by the Web site terms of use agreement.

Companies should take advantage of the tools available today to mark their proprietary content with electronic fingerprints and monitor cyberspace with software agents and bots to determine whether their intellectual property rights in and to their content are being infringed or abused. One recommendation is to design trademarks and logos used online purposefully to incorporate an electronic fingerprint for purposes of finding them in cyberspace. In some cases it may be important to not only establish that content is being used without authorization but also to track how the unauthorized use occurred.

Some content may be identified by a trademark or service mark. Trademark usage on the Internet should conform to common trademark usage rules. Trademarks used on Web sites should be designated with the ™ or ® symbols as appropriate, with notice of the trademark owner. There is a tendency on the Internet not to clutter Web sites with legal notices. This may prove fatal to recovery of trademark infringement damages. It is important to give notice that any trademarks relating to content have been registered.

Other Contract Provisions:

It is also important to ensure the Web site terms of use agreement includes liability limitations and other contract provisions used to manage the legal risks respecting content. These provisions may include dispute resolution provisions, including venue-selection provisions, indemnification provisions, acceptable use provisions, and other general terms and conditions. These other contract provisions may prove to be a critical part of a company's overall program to protect content on the Internet.

Information Security:

A company's overall legal strategies for content protection should be integrated with its information security plans and policies. Managing the security risks from the threats to content is a very important part of a content protection program. Prudent risk management and due care are necessary to protect the confidentiality, integrity, and availability of information content. A company should maintain an information security program containing administrative, technical, and physical safeguards appropriate to the company's size and complexity and nature and scope of its activities relating to its content protection program. Adequate security means that the company maintains effective security that is commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, impairment, modification, or destruction of information. A company should designate an employee or employees to coordinate and be accountable for the information security program integrated with and complementary to its content protection program. It should identify material internal and external risks that could result in the unauthorized disclosure, misuse, destruction, or compromise to its content and assess the sufficiency of any safeguards in place to control these risks. As part of a security program, a company should design and implement reasonable safeguards to control the risks identified through risk assessment and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures. A company should also evaluate and adjust its content information security program in light of the results of testing and monitoring any material changes to its content protection program, or any other circumstances it knows or has reason to know will have a material impact on its information security program.[59]

11.10. Remedies to Protect Web Contents:

Here are four fast (and free) things you can do to protect your property from thieves online:

[59] Westermeier, J.(Jay) T., The Computer & Internet Lawyer, Protecting Content on the Internet (June,2009); www.google.co.in

1. Include the copyright symbol on all pages of your website and your content like e-books and PDF downloads. This will deter those who innocently think it's ok to copy your stuff without realising it's an infringement.
2. Use Copyscape a duplicate content checker to search the internet for copies of your web or blog pages. You pop your page address in the search box and it will scan the web for copies. Note that it searches each page individually not a whole website.
3. If you have a WordPress site try a plug in called WP-Copyprotect. This 'locks' your blog so text and images can't be highlighted, copy and pasted. This works on the assumption that anyone wanting to steal your blog post or text from your website will be too lazy to re-type it out for themselves.

I think it's a pretty good deterrent although I don't use it myself as I'm always copying text from my website to use elsewhere and this plug in would stop me from doing that!
It may be a good solution for you if you want a hassle free way of protecting your online property.
4. Protect your online products, photos and images using a Creative Commons license. You can get one set up in seconds for free to protect ebooks, images and other materials for that extra bit of security.[60]

Ways to Protect Web Content Copyright[61]:
I. Preventative Measures: There are certain measures that can be taken to discourage plagiarism of your content by illustrating that you are aware of your rights as the content's creator.
1. Register your website with the DMCA and add one of their badges to your website to let potential copyright infringers know that you are protecting your content
2. Include a copyright notice on your website. This will show that you are aware of your legal standing as the content's creator. To intentional infringers, this will likely be enough to scare them away. To unintentional copiers, it should be a

[60] http://www.aliciacowan.com/social-media-and-digital-marketing/blogging-and-content/4-ways-to-protect-your-online-content-from-thieves
[61] http://www.ipwatchdog.com/2013/06/05/how-to-protect-the-copyright-of-my-web-content/id=40655/

reminder to them that copying your content is illegal. You can also post a DO NOT COPY badge from duplicate content checking sites like PlagSpotter to warn potential plagiarists from stealing from you.

3. A way to build proof that all your content is actually yours is by actively documenting the creative process. Save drafts of everything you post online in case you need to prove later that you are the original author.

II. Use Duplicate Content Detection and Monitoring Tools: Detecting copyright infringements and working pre-emptively against offenders can save a significant amount of time and effort, as copyright laws can become tangled and complicated. If you own a website or blog, any and all content that you created and uploaded must be monitored against takers. The internet is full of tools that can be used in the fight against copyright infringement; here are specific tools and steps that can be taken to protect your web content:

1. Use Google Search to scan the internet for unique parts of your text. Remember to use quotation marks so that the result is most accurate to your exact wording structure! Another way to do this and save time is to set Google Alerts so that each time new work that matches those search queries is published online Google will notify you on your email.

2. Monitor your content to search for plagiarism. There are various tools that allow you to search certain text and inform you if parts of it have been used elsewhere. Plagium andPlagiarisma are two such tools. If sentences used within a site have not properly attributed you, and you are the original author, you can take the needed measures and contact the plagiarist's website with further instructions.

3. You can also add your blog to the Copygator service, which monitors your blog for free and contacts you when it finds duplicate content on the internet. It labels the duplicate content as either 'exact' or 'near' to indicate whether the content has been identically copied or just share a resemblance or similar elements with one another.

4. Sometimes we unintentionally plagiarise, whether it's having just read an article and copying information without meaning to or in some other way. The PlagSpotter software provides a service similar to Copygator but also allows you to scan your web content using the batch search feature (the ability to check large numbers of URLs or your whole site) to see if you have accidentally

plagiarized. The program will indicate where the duplicate content in your post or website is and allow you to view your "plagiarism percentage". This is a handy way to ensure that you won't end up in the middle of a copyright dispute or get removed from Google's search results.

III. Take Action After Finding a Plagiarist: After discovering that someone has taken your content, you need to undertake steps to get the situation rectified. Here are some helpful guidelines on what you should do to remedy it as soon as possible.

1. Gather as much information at you can to prove that you are that content's original author. Take screenshots if possible.

2. Locate the copyright infringer's contact information. If you cannot find their information, try contacting webmasters@(whatever the domain name is). You should send a polite email specifiying that the content on their website is yours and is being used without your permission. Ask them to cease and desist and include all gathered information to show that you have evidence. In most cases the plagiarist will remove the stolen content after the first email.

3. A Whosis service can be used to find the website owner's legal name and phone number. All you have to do is insert the domain name in the search box and their name should appear. From here, you can contact them in a cordial way and ask for the content to be removed.

4. If your dialog with the offender has not been fruitful, you can contact their website's hosting company. They can also be found using a Whois service. Tell them about the situation and that the person in question is using your material without permission. They may remove the subscriber.

5. If you are still not getting any results, send the copyright offender an official "Cease and Desist" letter. With this, you can formally notify them that they must remove your content from their webpage or face impending legal action. There are many sample "Cease and Desist" letters online to help you draft one that screams "authority."

6. The DMCA's Section 512 provides "notice and takedown" procedures that give copyright holders an easy way to cut off access to content that infringes on their copyright.

7. File a copyright complaint with Google. They may remove or disable the infringing content or terminate the subscribers. The form to report such activity

and more information on Google's policy and how it relates to the Digital Millennium Copyright Act can be found here.

8. At the end, suing the plagiarist is always an option; however, this includes time and expenses, not to mention stress. It would be recommended to exhaust all other avenues before attempting a lawsuit.

11.11. Summary:

Protecting content on the Internet requires a comprehensive legal strategy depending on the nature of the content. This strategy includes contract protection, copyright protection (and possibly other intellectual property protection), Digital Millennium Copyright Act safe harbor protection and anti-circumvention protection, immunity protection and the use of disclaimers, notices, and proprietary legends. Content protection needs to take full advantage of the rights provided under these legal strategies. Contract protection should be consistent with the other forms of protection a company adopts. In this unit the important concept of website contract, password restricted content, display copyright notice to help prevent content theft, fair use law, how to check if your content is stolen, copyright of web contents, copyright registration of web contents, disclaimer regarding web content and remedies to protect web content are discussed at length for better understanding on this point.

11.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)

- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

11.13. Check your Progress:

A. Which of the following statements are true or false:

a) Protecting your website against theft is now considered mandatory for website owners.
b) Website terms of use should provide restrictions on the use of content.
c) Some website may contain password restricted areas.
d) The nature of copyrighted work, if what is being quoted is factual, then it is more likely to be fair use.
e) Create a trick link to a page of your site.

B. Fill in the Blanks:

I. Website……represents one of the most important legal strategies for protecting content on internet.
II. http://www.copyscape.com is a web site to check ……...
III. A ……should reflect a cost/benefit analysis based on the value of the copyrightable content and risks related to infringement.
IV. ……can be used based on the nature of the content.
V. Include the …….on all pages of your website and your content line e-books and PDF downloads.

11.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Terms of use or terms of service agreements
2. Plagiarism
3. Copyright registration strategy
4. Specific disclaimer
5. Copyright symbol

11.15. Terminal Questions:

1. What is website contract?
2. Define password.

3. What is fair use law?
4. How to check if your content is stolen?
5. What are the remedies to protect your web contents?

Unit-12

International Treatise on Cyber Security

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to International Treatise on Cyber Security
- Understand the nature and scope of Cyber Security in various countries
- Understand the technical and legal issues related to Cyber Security

Structure:

12.1. Introduction:

The Flame computer virus is the latest digital malware program uncovered in the escalating practice of large-scale cyber attack. Twenty times larger than its predecessor Stuxnet, the Flame virus infected computer systems throughout the Middle East. Analysts believe the Flame virus was designed for espionage purposes, some arguing that it then doesn't qualify as "cyber warfare" (though Kapersky Lab, the Russian cyber security firm that uncovered the virus, said it does). However, the motive of 2010's Stuxnet was undoubtedly malicious. The virus infected Iranian nuclear enrichment facilities—which Iran insists are for peaceful purposes, but many believe are being used to develop nuclear arms—and derailed the operations of thousands of centrifuges at multiple Iranian plants. The *New York Times* recently reported that the United States, with the help of Israel, was behind Stuxnet in a mission code-named "Olympic Games." Government sources cited in the article refused to admit responsibility for the Flame virus, however Kaspersky Lab has linked Flame to Stuxnet. The ambiguities of cyber warfare worry international law experts, diplomats, and military commanders alike. What qualifies as an act of war versus espionage? Does the law of "proportionality"—that collateral damage to civilians in battle must not be disproportionate to the military target attacked—apply to cyber war, especially since the line between civilian and military computer systems is not so clear? Should a cyber attack by a lone hacker be treated differently than that engineered by a national government? Thus some legal and cyber security experts have suggested that an international treaty, like those created to address the terms of conventional war, should be drafted to clarify the rules of cyber warfare, a few even proposing an all-out ban on the practice. Others insist that such a treaty would be difficult to even draft, and impossible to enforce.

12.2. US Cyber Security Policy[62]:

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they

[62] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas." (President Obama)

Five Things to Know: The Administration's Priorities on Cyber security:

1. Protecting the country's critical infrastructure — our most important information systems — from cyber threats.
2. Improving our ability to identify and report cyber incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.
4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

Cyberspace touches nearly every part of our daily lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. We must secure our cyberspace to ensure that we can continue to grow the nation's economy and protect our way of life.

The Administration is employing the following principles in its approach to strengthen cyber security:

- Whole-of-government approach
- Network defense first
- Protection of privacy and civil liberties
- Public-private collaboration
- International cooperation and engagement
- Protect Critical Infrastructure:

The government must work collaboratively with critical infrastructure owners and operators to protect our nation's most sensitive infrastructure from cyber security

threats. Specifically, we are working with industry to increase the sharing of actionable threat information and warnings between the private sector and the U.S. Government and to spread industry-led cyber security standards and best practices to the most vulnerable critical infrastructure companies and assets.

- The Administration issued E.O. 13636, *Improving Critical Infrastructure Cyber security*, in 2013
- The Administration launched a follow-on Cybersecurity Framework, a guide developed collaboratively with the private sector for private industry to enhance their cyber security, in 2014

Protect Critical Infrastructure:

The government must work collaboratively with critical infrastructure owners and operators to protect our nation's most sensitive infrastructure from cybersecurity threats. Specifically, we are working with industry to increase the sharing of actionable threat information and warnings between the private sector and the U.S. Government and to spread industry-led cybersecurity standards and best practices to the most vulnerable critical infrastructure companies and assets.

- The Administration issued E.O. 13636, *Improving Critical Infrastructure Cyber security*, in 2013
- The Administration launched a follow-on Cyber security Framework, a guide developed collaboratively with the private sector for private industry to enhance their cyber security, in 2014

Improve Incident Reporting and Response:

We must enhance our ability to detect and characterize cyber incidents, share information about them, and respond in a timely manner. These efforts encompass network defense, law enforcement, and intelligence collection initiatives, so we can better understand our potential adversaries in cyberspace.

- Awareness of a cyber threat or incident – and quickly acting on that information -- are critical prerequisites to effective incident response. As directed in E.O. 13636, the U.S. Government has developed systems and procedures to increase the timeliness and quality of cyber threat information shared with at-risk private sector entities. We are placing great emphasis on unity of effort by agencies with a domestic response mission

Engage Internationally:

Because cyberspace crosses every international boundary, we must engage with our international partners. We will work to create incentives for, and build consensus around, an international environment where states recognize the value of an open, interoperable, secure, and reliable cyberspace. We will oppose efforts to restrict internet freedoms, eliminate the multi-stakeholder approach to internet governance, or impose political and bureaucratic layers unable to keep up with the speed of technological change. An open, transparent, secure, and stable cyberspace is critical to the success of the global economy.

- We are continuing to pursue the policy objectives laid out in the U.S. International Strategy for Cyberspace including:
- Developing international norms of behavior in cyberspace
- Promoting collaboration in cybercrime investigations (Mutual Legal Assistance Treaty modernization)
- International cybersecurity capacity building

Secure Federal Networks

We must improve the security of all federal networks by setting clear targets for agencies and then hold them accountable to achieve those targets. We are also deploying improved technology to enable more rapid discovery of and response to threats to federal data, systems, and networks.

- The Cyber security Cross Agency Priority (CAP) Goal represents the Administration's highest cyber security priorities for securing unclassified federal networks.

Shape the Future Cyber Environment:

We are also looking to the future. We are working to develop a cyber-savvy workforce and ultimately to make cyberspace inherently more secure. We will prioritize research, development, and technology transition and harness private sector innovation while ensuring our activities continue to respect the privacy, civil liberties and rights of everyone.

- The federal government is partnering with the private sector and academia to encourage and support the innovation needed to make cyberspace inherently more secure.

- US Cyber security Policies and Initiatives:
- Presidential Policy Directive 28 (PPD-28) "Signals Intelligence Activities," 2014
- Executive Order (E.o.) 13636 "Improving Critical Infrastructure Cyber security," 2013
- Presidential Policy Directive 21 (PPD-21) "Critical Infrastructure Security and Resilience," 2013
- Presidential Policy Directive 8 (PPD-8) "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 2011
- Cyberspace Policy Review, 2009
- Cyberspace Policy Review Supporting Documents

12.3. Threats and Challenges to International Cyber Security:

With the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, cyber security is a complex transnational issue that requires global cooperation for ensuring a safe Internet. According to a 2011 Norton study, threats to cyberspace have increased dramatically in the past year afflicting 431 million adult victims globally – or 14 adults' victims every second, one million cybercrime victims every day. Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation.

To address the issues and challenges around cyber security and cybercrime, the United Nations Economic and Social Council (ECOSOC) held a Special Event on "Cyber security and Development", organized jointly by the Department of Economic and Social Affairs (DESA) and the International Telecommunication Union (ITU) on 9 December in New York. Chaired by the President of ECOSOC, with the participation of the Secretary-General of the ITU and the Chair of the

United Nations Commission on Science and Technology for Development, the special event brought together Member States, the United Nations system, the public and private sector, as well as other civil society organizations interested in the areas of cyber security and cybercrime.

The plenary and panel discussion aimed to

(1) build awareness at the international policy level by providing ECOSOC Members with a picture of the current situation and challenges concerning cyber security and its links to development;

(2) identify a range of best practice policies and initiatives in place around the world to build a culture of cyber security; and (3) explore options for a global response to rising cybercrime. Each representative on the panel discussed the multifaceted issues surrounding cyber security, and the necessity for member states, the private sector, civil society organizations and law enforcement agencies to work in concert to manage the risks of our increasing interconnectivity. Speakers discussed the role of economic disparities between nations and the fact that developing countries do not have sufficient capacity to combat cyber attacks and cybercrime, and its global threat to cyber peace. The lack of partnership between developed and developing countries could generate "safe havens", where cyber criminals can make use of the legal loopholes, and the lack of strong security measures present sometimes in developing countries to perpetrate cybercrimes. Drawing attention to challenges of protecting children online, Ms. Deborah Taylor Tate, ITU Special Envoy and Laureate for Child Online Protection, shared, "We must arm our kids with the tools, when they take their first step and click in the cyber world… Peer to peer and teaching is the best form of advocacy." She encouraged parents, community leaders and governments to access the media literacy guidelines provided online by ITU.

During the interactive session, the panelists and responding member states discussed the need for a future global convention to develop strategies including the possibility of building upon the Budapest Convention, an international treaty seeking to harmonize national criminal laws of computer crimes such as copyright infringement, fraud, child pornography, hate crimes and breaches of network security. In his concluding remarks, President of ECOSOC, H.E. Mr. Lazarous Kapambwe pressed, "We have agreed that cyber security is a global issue that can only be solved through global partnership. It affects all of our organizations…and

the United Nations is positioned to bring its strategic and analytic capabilities to address these issues."[63]

12.4. International Cooperation and Cyber Security:

Launched in 2007 by ITU Secretary-General, Dr. Hamadoun I. Touré, the ITU Global Cyber security Agenda (GCA) is a framework for international cooperation aimed at enhancing confidence and security in the information society. The GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts. Since its launch, the GCA has attracted the support and recognition of leaders and cyber security experts around the world. H.E. Dr. Óscar Arias Sánchez, Former President of the Republic of Costa Rica and Nobel Peace Laureate, and H.E. Blaise Compaoré, President of Burkina Faso, is both Patrons of the GCA. The GCA has fostered initiatives such as the Child Online Protection and the ITU-IMPACT partnership, together with the support of leading global players from all stakeholder groups, is currently deploying cyber security solutions to countries around the world. The GCA is built upon the following five strategic pillars, also known as work areas:

- Legal Measures
- Technical & Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

For the first time at the UN level, a group of governmental experts was able to agree to an important set of recommendations on norms, rules, and principles of responsible behavior by states in cyberspace. Governmental experts from the five permanent members of the UN Security Council and 10 leading cyber powers from all regions of the world have recognized that international law, including the principles of the law of state responsibility, fully apply to state behavior in cyberspace. This recognition represents a landmark step toward universal acceptance of the legal framework. The previous lack of clarity as to what rules

[63] http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

apply in cyberspace was one of the factors contributing to instability and the risk of escalation. The explicit affirmation that international law, particularly the principles of the UN Charter, is applicable to state activities in cyberspace, including to activities of nonstate actors attributable to states, will allow the international community and affected states to react to violations more effectively. In cyberspace, states have to comply with the prohibition on the use of force, the requirement to respect territorial sovereignty and independence, and the principle of settling disputes by peaceful means in the same way as in the physical world. The right, specified in Article 51 of the UN Charter, to self-defense including the use of force would apply if a cyber attack reached the level of an "armed attack." The report, however, refrained from spelling out when this could be the case as the legal debate on this issue has only just begun.

These principles of universal law go beyond restricting the use of force in cyberspace. They also cover other areas such as sovereignty and territorial integrity, which restrict the lawfulness of potentially harmful acts below the level of kinetic force. In particular, together with the customary international law principles of state responsibility, the principles of the UN Charter would limit the legitimacy of state actions purposely breaching the intellectual property of companies or the personal data of individuals. Nevertheless, legal experts need to do much more work to specify these principles and rules to cover more specifically a range of diverse actions in cyberspace. Attribution continues to be a key challenge, as legal and technical attribution are required in order to challenge a state, for example, in the Security Council, for wrongful acts in cyberspace.

Concerning cyber attacks that reach the threshold of an armed conflict, a lower threshold than armed attack, most of the 15 experts were willing to explicitly acknowledge the application of international humanitarian law to cyberspace.

Russia has accepted the application of such law to cyberspace. China, on the other hand, has repeatedly stated that it considers such explicit confirmation premature and counter to the objective of preventing a rush to offensive cyber weapons. Future work by the International Committee of the Red Cross or by nongovernmental organizations such as the East West Institute might pave the way for such a recognition by China as well. The experts group report reiterates the statement from the report of the 2010 experts group of the need for common

understandings on how such norms apply to state behavior and the use of ICTs by states, as well as the possibility of developing more-specific rules of behavior.

Building Transparency and Trust: On the controversial issue of how to deal with the increasing likelihood those countries will pursue development of cyber weapons, the group managed to take a realistic approach. In their draft code of conduct regarding the use of ICTs by states, submitted to the UN secretary-general in 2011, China and Russia suggested explicit prohibitions of what they term "information weapons" and the proliferation of their technologies.

Yet, in the course of the experts group deliberations, the Chinese and Russian representatives recognized the inherently dual nature of these technologies and joined the more pragmatic approach of starting out with traditional confidence-building measures and other cooperative measures before attempting to agree on prohibitions that are basically unverifiable. At the same time, the experts understood that confidence-building measures can be a starting point should an arms control approach become feasible in the future.

In several paragraphs, the group's 2013 report refers to language used in other treaties with arms control implications. In particular, the report calls on states to promote a "peaceful" ICT environment, which could be understood as an allusion to the so-called "peaceful purpose" clause of the Outer Space Treaty. In its approach to cyberspace issues, the experts group applies a similar concept by refraining from imposing specific prohibitions but positing the general objective of peaceful state use of cyberspace. This strengthens the ability of future agreements to cover future developments in the field.

Recognizing that confidence-building measures and the exchange of information among states are essential to increasing predictability and reducing the risks of misperception and escalation through cyberthreats, the experts group agreed on a range of voluntary measures to promote transparency and confidence among states in this area. The measures are aimed at increasing transparency and creating or strengthening communication links in order to reduce the possibility that a misunderstood cyber incident could create international instability or a crisis leading to conflict. Taken together, they represent an important foundation for bilateral, regional, and global measures to build confidence and global stability in cyberspace and to prevent unnecessary escalation of cyber security incidents.

In particular, the report recommends the following confidence-building measures:

- Exchanging views and information on national policies, best practices, decision-making processes, and national organizations and structures with regard to cyber security. As an example, the United States in 2012 and Germany in 2013 exchanged so-called white papers on cyber defense with Russia.
- Creating bilateral or multilateral consultative frameworks for confidence-building measures, for example, within the Arab League, the African Union, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Organization for Security and Co-operation in Europe (OSCE), and the Organization of American States. These frameworks could include workshops and exercises on how to prevent and manage disruptive cybersecurity incidents.
- Enhancing the sharing of information and crisis communication among states on cybersecurity incidents at three levels: between national CERTs bilaterally and within already existing multilateral CERT communities to exchange technical information about malware or other malicious indicators; through previously existing or newly created channels for crisis management and early warning to receive, collect, analyze, and share such information to help mitigate vulnerabilities and risks; and through channels for dialogue at political and policy levels.
- Increasing cooperation to address incidents that affect critical infrastructure systems, particularly those that rely on ICT-enabled industrial control systems.
- Enhancing mechanisms for law enforcement cooperation to reduce incidents that could be misunderstood as hostile state actions and that affect international security.

Although governments must take the lead in developing and implementing these measures, the group reiterates and highlights the important role the private sector and civil society should play in these efforts. In future work, governments and the private sector must undertake joint efforts to elaborate the objectives, conditions, requirements, frameworks and models of such public-private partnerships for international cyber security on a global scale. Some global ICT companies already

are engaged in this discussion. Yet, the specific roles of states and private companies and the limitations on cooperation among them in the sensitive field of cyber security need to be more clearly developed by governments and private sector stakeholders.

In its report, the experts group highlights the need for international capacity building to help states in their efforts to overcome the digital divide and to improve the security of vital ICT infrastructure. The report calls on states, working with the private sector and UN specialized agencies, to provide technical or other assistance in building capacities in ICT security. In particular, such assistance could help to strengthen national legal frameworks and law enforcement capabilities and strategies, combat the use of ICTs for criminal or terrorist purposes, and strengthen incident response capabilities, including through CERT-to-CERT cooperation.[64]

12.5. African Union Convention of Cyber Security and Data Protection:

The Convention was adopted during the 23rd Ordinary Session of the Summit of the African Union which concluded in Malabo, Equatorial Guinea on 27 June 2014. The Convention, which for the first time substantively brings the language of 'protection of personal privacy' to this level, seeks to establish a legal framework for Cyber-security and Personal Data Protection especially in the context of e-commerce. It builds on the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society. The adopted version is an improvement on the earlier version, which was widely criticized by several stakeholders, including by civil society groups, particularly for its failure to adequately protect the right to privacy.

The Convention acknowledges the importance of adherence to national constitutions and international law, for instance in its preamble the Convention states that the establishment of a regulatory framework on cyber-security and personal data protection should take into account the requirements of respect for

[64] http://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights. This requirement is emphasized more than once in the text

Importantly, the Convention enjoins states parties to establish legal and institutional frameworks for data protection and cybsecurity. However in the case of cybersecurity, states could either establish new institutions or use pre-existing ones. This requirement, if properly applied, might help bring an element of accountability in the manner in which the police and security services work and are governed on the continent.

The Convention also outlines the principles that ought to be adhered to in processing personal data, such as consent and legitimacy; lawfulness and fairness; purpose, relevance and storage of processed personal data; accuracy; transparency as well as confidentiality and security of personal data. It further enjoins state parties to prohibit any data collection and processing, without consent, that reveals racial, ethnic and regional origin, parental affiliation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject, except under certain exceptional circumstances.

Weaknesses at a glance: Firstly, given the inherent weaknesses of most African security sector mechanisms, in particular, the partisan and compromised nature of the state security and population data registration sectors, the Convention could have included a requirement for strong of judicial oversight in order to strengthen the protection of the right to privacy and restrain political influence on data management, specifically data in transit, storage, cloud or at rest.

Secondly, although the Convention enjoins state parties to enact laws that take into account their constitutions and international conventions, it only overemphasizes the African Charter. Given that the African Charter does not have an explicit right to privacy in relation to access to information and processing of personal data, this creates a gap that needs to be filled.

There are also many instances where the Convention appears to put national sovereignty and discretion over international law, for example, under Chapter 3 on Promoting cyber security and fighting cybercrime, it uses the phrases as, ‘as it deems necessary, as it deems appropriate and as it deems effective’. Such wide

discretion, gives states, especially undemocratic ones, room to abuse these powers. This is especially the case since the Convention does not explicitly outline the minimum threshold that national constitutions, legal frameworks and laws should meet and comply with. In this regard, an explicit reference to international law would have been helpful.

Giving states parties' wide discretion on the content of the laws and their constitutions is not in line with the current international best practice and recommendations on the issue. Of relevance in this instance, the Human Rights Committee provided important guidance in its General Comment 16 on the interpretation of article 17 of the International Covenant on Civil and Political Rights. According to the Committee, the term "unlawful" means that no interference can take place "except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant" [emphasis added].

Also of concern, while Article 15 relating to interconnection of personal data files is a positive development from both commercial and social protection schemes points of view, given that the Convention does not specify the minimum thresholds to be met by the proposed legal frameworks, the instances of creation of big data and data sharing without strict conditions and basic judicial supervision would certainly lead to increased state surveillance and monitoring thus leading to erosion of privacy and other civil liberties.

Such practice has been widely criticized in countries such as Zimbabwe where parliament recently passed an adverse report on the SIM card registration scheme. The scheme involved, inter alia, the creation of a shared database as envisaged under the Convention. In addition, press reports have recently reported on how Zimbabwe is allegedly setting up High Level Computer (HCL) project which entails the establishment of a super-information laboratory that would aggregate information from virtually all government departments and the private sector for planning, research and development purposes. Thought to be the first of its kind in Africa, it is also being reported how state authorities had infiltrated the facility.

The above weaknesses, are by no means a lack of acknowledgement that the African Union Convention lays a progressive foundation, s that might for the first time, encourage states to shed light on the vital area of security service which most

people perceive as dark and in need of transparency. However, on the continental level, in addition to the Convention, the African Union should take one more step by introducing the right to privacy in the African Charter. They could, for example, introduce an Optional Protocol in line with recommendations we make in our paper presented at the NGO Forum of the African Commission 55th Session.
Secondly, while most African states have taken commendable steps to include the right to privacy in their national constitutions, according to articles 'Internet Governance: Why Africa should take the lead and 'Global Data Privacy Laws: 89 Countries, and Accelerating; in Africa only 11 countries have enacted national freedom of information/ expression laws and eight African Countries on the right to privacy/ data protection. African states should therefore take immediate steps to adopt data protection laws and fortify constitutional provisions in line with the Convention, despite its weaknesses pointed out above.

12.6. Council of Europe Convention on Cyber Crime (Budapest convention):

The Budapest Convention Cybercrime, otherwise referred to as the Budapest Convention or Convention Cybercrime is the first international treaty aiming to address and tackle computer crime and the internet by harmonizing nation laws, improving investigation techniques in addition to increasing the cooperation of nations in regards to computer law.
The treaty was drafted in regards to resolving crimes committed over the internet amongst other networks, dealing with infringements of copyright, computer-related fraud, indecent images of children, hate crimes and violations against network securities. The Budapest convention on cyber crime primary aims include:

- "Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime."
- "Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form."

- "Setting up a fast and effective regime of international cooperation."
- Who has signed up to it? As of September 2012 there are a total of:
- 37 parties including 35 European nations, USA and Japan.
- 10 signatories consisting of 8 European nations, Canada and South Africa.
- 8 states intended to accede including Argentine, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.
- 55 states are or committed in becoming a party.

Many countries have been reluctant to sign the treaty on the basis that when the Budapest Convention Cybercrime was first drafted in 2001, it was tailored by and geared towards European states and is believed to be somewhat outdated. Brazil considered signing the Budapest Convention Cybercrime but later declined due to raising concerns about the conventions provisions regarding the criminalization of intellectual property infringements, which Brazil believed were not a suitable provisions for a universal model.

Worldwide there is a distinct difference of views in regards to what would make an appropriate global standard and therefore tailoring the Budapest Convention Cybercrime to suit everyone's needs globally would be a near impossible task.

With disagreements regarding the treaty's guidelines: Russia, Tajikistan and Uzbekistan sent a letter to the U.N requesting a resolution to the code of conduct in cyberspace, making provisions intended to stop terrorist's use of the internet.

Many countries including America have viewed the proposal with suspicion believing that it may have been created as an intent as a legal instrument which could be invoked to unfairly crack down on Internet based dissent. Evermore proving that coming up with a consensus for the treaty's code of conduct an extremely difficult and most likely impossible task.

As of yet, the future for Budapest Convention Cybercrime is unclear; a cybercrime law is needed but speculations as to whether Budapest should be that law is questionable.

Budapest Convention Cybercrime is the only accepted international treaty working to protect people and their rights against crimes online. Under this treaty, countries are able to define criminal conduct against and using computers, providing law enforcement with investigative tools and create points of contact for urgent cases internationally almost on a daily basis.

The number of parties that have signed up to the Budapest Convention Cybercrime and have brought their countries laws in line with the treaty's codes of conduct have increased – around 140 of the 193 members of the U.N. have been reforming their legislation relating to cybercrime, with at least 125 of them using the Budapest Convention Cybercrime as a source of inspiration. All this has contributed to the globalisation of criminal law relating to computers.

It's been reported that Microsoft have said that "The Council of Europe has succeeded because it has helped to spur governments to enact cybercrime legislation domestically and work to combat international cybercrime. It focuses on problems of cross-jurisdictional importance that serve the interests of many states rather than few." Showing that noticeable changes for the good have occurred because of the treaty.

Despite of the good that's been made, a number of States including China and Russia, want more control over the Internet, opposing against the Budapest Convention Cybercrime and wanting to call for a new international treaty instead. As of yet, there has been no consensus in this direction and probably won't be for a while; It took more than ten years to prepare the Budapest Convention on Cybercrime, negotiation of a new agreement aiming to go beyond Budapest Convention would be a difficult task. Controversy for the treaty runs a risk of not only disrupting reforms that are occurring in many countries, but also undermines all of the technical assistance activities and sharpening international divisions that have been put in place.

12.7. Cyber Defence Security: Indian Position:

India's current positions at the international level on cyber security are largely derived from the Foreign Office's inherited traditions of its multilateralism, deeply influenced since the 1970s by the North-South dimension. The national

security establishment in Delhi, however, is conscious of the urgent imperative of building domestic capabilities. The realists there have no time for grandstanding on the global stage on cyber issues. India's approach to international security issues in the past was dominated by principles of equity and non-discrimination. As a potential power in its own right, however, India might have to carve out a path that is bound to diverge from its traditional approach to international security. As in the nuclear domain, so in the cyber realm, India's national interests may not be aligned with the collective positions of the South. India's primary challenge is to bring in a measure of pragmatism to its engagement on cyber security issues that can effectively combine its traditional tenets of internationalism with the strategic dynamic unfolding in the cyber domain.

As the weakest of the major powers, India must learn to nimbly navigate the dynamic among the great powers on cyber security issues. In the past, India used to urge great powers to abide by norms in the management of security challenges, but was deeply perturbed by any collaboration between the major powers. For example, India was deeply concerned about bilateral nuclear arms control between Washington and Moscow and the implications of their joint championship of the non-proliferation regime. Today, India worries about the potential consequences of a cyber security treaty that might emerge out of bilateral negotiations between America and China. India must also be conscious of the fact that technological change and the rise of new powers generate pressures for rewriting the international rules. India has indeed stepped up its engagement with the major powers on cyber security issues. This engagement was hobbled by weak governments in Delhi that were unable to overrule individual departments in the making of important policies. With a strong central government now in place under the leadership of Narendra Modi, considerations of national security and power balances are likely to have a greater salience in India's international approach to cyber issues. As the cyber domain draws attention from the Modi government, India must necessarily look towards building functional coalitions to secure its own interests in the global arena. Any which way that India looks at cyber security issues, the US looms large. Despite being a democracy, internal security considerations often put India at odds with the US and on the same side as Russia and China on some aspects of cyber regulation. But broader considerations of international regime building on cyber security, and the new compulsions for

security partnership between Delhi and Washington in Asia, Indian Ocean and beyond, demand substantive consultations between Delhi and Washington.[65]

12.8. International Information Security(Shanghai Cooperation organization):

The agreement between the governments of state members of the Shanghai organization of cooperation about cooperation in the field of ensuring the international information security (from June 16, 2009): The governments of state members of the Shanghai organization the cooperation (SCO) which further are referred to as the Party,

Noting significant progress in development and implementation of the latest information and communication technologies and the means creating global information space,

expressing concern in the threats connected with possibilities of use of such technologies and means for the purpose of, not compatible to tasks of ensuring the international stability and safety, applicable both to civil, and to military to spheres,

giving importance of the international information security as to one of crucial elements of system of the international security,

being convinced that further deepening of trust and development of interaction of the Parties in questions of ensuring the international information security is the imperative need and is equitable to their interests,

taking also into consideration the important role of information security in providing the rights and fundamental freedoms of man and citizen,

considering recommendations of General Assembly resolutions "Achievements in the sphere of informatization and telecommunications in the context of the international security",

aiming to limit threats of the international information security, to provide interests of information security of the Parties and to create the international information circle for which are characteristic the world, cooperation and harmony,

[65] http://cyfy.org/towards-an-international-treaty-on-cyber-security-a-bilateral-dialogue-between-india-and-the-us/

wishing to create the legal and organizational basis of cooperation of the Parties in the field of providing the international information security,
agreed as follows:
Article 1. Terms and concepts
For the purposes of interaction of the Parties within accomplishment of this agreement the List of the main terms and concepts of area of ensuring the international information security according to appendix 1 to this agreement being its integral part will be used.
Contents of this list of terms and concepts can be supplemented, specified and be updated as required as agreed.
Article 2. The main threats in the field of ensuring the international information security
Realizing cooperation according to this agreement of the Party start with availability of the following main threats in the field of ensuring the international information security:
1. Development and use of the information weapon, preparation and conducting information war.
2. Information terrorism.
3. Information crime.

12.9. India Needs To Strengthen Its Cyber Security Capabilities:

India is trying to implement the Digital India project to the best of its capabilities. The success of Digital India project would depend upon maximum connectivity with minimum cyber security risks. This is also a problem for India as India has a poor track record of cyber security. For instance, the Telecom Commission has approved satellite based mobile services in India. Similarly, free wireless and Internet connectivity would also be made available to Indian people for convenience and better connectivity. However, this would raise wireless security and numerous cyber security challenges as well. Although the National Cyber Security Policy of India 2013 (NCSP 2013) was announced by Indian Government in 2013 yet its actual implementation is still missing. As a result fields

like e-governance and e-commerce are still risky and may require cyber insurance in the near future.

Cyber attacks have increased tremendously world over and India is also required to protect its cyber frontiers through techno legal measures. At the same time efforts must be made by India to formulate effective cyber crimes prevention strategy and impart cyber crime investigation training to the law enforcement agencies of India. Some specific areas against which India needs to strengthen its cyber security are cyber warfare, cyber terrorism, cyber espionage, critical infrastructure protection (PDF), international cyber security cooperation (PDF), etc. At the international level, there has been a trend to block free flow of cyber security technologies. Recently a proposal was mooted to include cyber security under the Wassenaar Arrangement that was strongly objected to be India. If accepted, export restrictions could have been placed upon cyber security technologies. India needs to strengthen its cyber security capabilities that must include both offensive and defensive cyber security capabilities. A cyber warfare policy of India (PDF) must also be formulated urgently that must include cyber security skills development objective as well.

12.10. Cyber Peace Foundation:

With the growth in internet and use of technology the world is preparing for cyber war by raising its own cyber military and cyber weapons. It has been rightly said that the fifth dimension of war would be CYBER WAR (rest 4 being land, sea, air and space), which will have a devastating effect on the world's information security. Not only that, it can result in a complete chaos as Critical Information Infrastructure of the countries would be affected. Other spheres of life also have been brought in a vast magnitude of risks and threats to the peace of the cyber society. Every action or thought is directed at controlling negativity being spread through this medium and at cyber safety. In today's world, Cyber crime, cyber bullying, Cyber war, Cyber terrorism and such anti-social issues have gained very high prominence. The world needs to realize the fact that there is a bigger role to play in using this medium for spreading and promoting Peace.

It is high time that we start taking proactive cyber security measures and also injecting peace into the cyber ecosystem. Keeping this in view, Cyber Peace

Foundation (CPF) has been setup with the goal of establishing a peaceful and harmonious cyber space. Among the very few organizations in the world working for 'Peace', the CPF is definitely the first NGO in the world to work for 'Cyber Peace'. CPF focuses on awareness, counseling, education, training and to reach out to the citizens, the governments, law enforcement agencies (LEAs), private enterprises, NGOs working in cyber crimes and cyber security, universities, cyber security experts and bug bounty hunters; to provide a common platform on a global level for ALL EXPERTS ON ONE BRIDGE. In its bid to curb the ever increasing cyber crime menace and promote cyber harmony, CPF has a CYBER PEACE CORP. We act as a point of contact for different governments, LEAs, and cyber cells to ensure peaceful settlement of any cyber related disputes. The aim of the organization is to empower all through knowledge of threats, risks and opportunities. CPF acknowledges the importance of conservation of cyber ecosystem, in the same manner as we work to protect our real world environment, and is deeply committed to this cause.

12.11. Summary:

International community developing a consensus on the cyber security but still on several issues there is no consensus. In his unit the important concepts of US cyber security policy, threats and challenges to international cyber security, international cooperation and cyber security, African Union Convention of cyber security and data protection, Council of Europe Convention on Cyber Crime (Budapest Convention), cyber defense sensitivity in Indian perspective, international information security, India needs to strengthen its cyber security capabilities, and Cyber Peace Foundation are discussed at length for better understanding in the interest to explore the various dimensions of cyber securities.

12.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)

- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)

- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

12.13. Check your Progress:

A. Which of the following statements are true or false:

a. The Flame computer virus is the latest digital malware program uncovered in the escalating practice of large scale cyber attack.
b. Cyberspace touches nearly every part of our daily lives.
c. We are working to develop a cyber savvy workforce and ultimately to make cyberspace inherently more secure.
d. The lack of partnership between developed and developing countries could generate "safe havens" for cyber criminals.
e. One international report recommends exchanging views and information on national policies, best practices & etc. with regard to cyber security.

B. Fill in the Blanks:

I. An ……..cyberspace is essential to the success of the global economy.
II. According to ……, threats to cyberspace have increased dramatically in the past.
III. The ……..enjoins state parties to establish legal and institutional frameworks for data protection and cyber security.
IV. ……..on cyber crime is the first international treaty aiming to address and tackle computer crime.
V. India is trying to implement the ……to the best of its capabilities.

12.14. Answer to Check your Progress:

A.

1. True

2. True
3. True
4. True
5. True

B.

1. Open, transparent, secure and stable
2. 2011 Norton Study
3. African Convention
4. Budapest Convention
5. Digital India Project

12.15. Terminal Questions:

1. What is US Cyber Security Policy?
2. What are the threats and challenges to international cyber security?
3. Define international cooperation and cyber security.
4. Discuss African Union Convention of Cyber Security and Data Protection.
5. What is the position of India on cyber defense security?

Unit-13

Cyber Terrorism-Meaning, Challenges and Issues

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to International Treatise on Cyber Security
- Understand the nature and scope of Cyber Security in various countries
- Understand the technical and legal issues related to Cyber Security

Structure:

13.1. Introduction:

Cyber terrorism has been around since the late 1980's, however the number of internet terrorism have only increased since the September 11

attack on the United States. Some examples of cyber terrorism activities include email bombing, hacking into government portals, banking, water and hospital websites to either generate fear or endanger the lives of many. Some of the earlier examples of cyber terrorism attack was in 1996 when a computer hacker who claimed to be linked with the White Supremacist movement had temporarily disabled and damaged a Massachusetts Internet Service Provider (ISP) while he sent out worldwide racist messages under the ISP's name. While in 1999, during the Kosovo conflict, North Atlantic Treaty Organization (NATO) computers were blasted with e-mail bombs and hit with Denial-of-Service (DoS) attacks by hackers protesting the NATO bombings. More recently, in 2000, someone hacked into Maroochy Shire, Australia waste management control system and released millions of gallons of raw sewage on the town. As there is an increase in knowledge of the usage of internet, the trend has shifted and terrorists are using cyberspace to facilitate the more traditional methods of terrorism such as bombings or spreading messages of hate. The web sites of terrorist groups in particular are used to present messages, coordinate members, and recruit young supporters. Some of these web sites are also set up as a source of financing their activities through sale of their merchandise. Countries like the United States and in the European continent and powerful Asian countries like China and India have taken their own precautions in combating cyber terrorism.

13.2. Cyber Terrorism-Meaning: According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Unlike a nuisance virus or computer attack that result in a denial of service, a cyber terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Cyber terrorism is sometimes referred to as electronic terrorism or information war.

In the wake of the recent computer attacks, many have been quick to jump to conclusions that a new breed of terrorism is on the rise and our country must defend itself with all possible means. As a society we have a vast operational and legal experience and proved techniques to combat terrorism, but are we ready to fight terrorism in the new arena – cyber space? A strategic plan of a combat operation includes characterization of the enemy's goals, operational techniques, resources, and agents. Prior to taking combative actions on the legislative and operational front, one has to precisely define the enemy. That is, it is imperative to expand the definition of terrorism to include cyber-terrorism. As a society that prides itself on impartiality of justice, we must provide clear and definitive legislative guidelines for dealing with new breed of terrorism. As things stand now, justice cannot be served as we have yet to provide a clear definition of the term. In this light, I propose to re-examine our understanding of cyber-terrorism.

There is a lot of misinterpretation in the definition cyber-terrorism, the word consisting of familiar "cyber" and less familiar "terrorism". While "cyber" is anything related to our tool of trade, terrorism by nature is difficult to define. Even the U.S. government cannot agree on one single definition. The old maxim, "One man's terrorist is another man's freedom fighter" is still alive and well.

The ambiguity in the definition brings indistinctness in action, as D. Denning pointed in her work Activism, Hactivism and Cyber terrorism, "an e-mail bomb may be considered hacktivism by some and cyber-terrorism by others". It follows that there is a degree of "understanding" of the meanings of cyber-terrorism, either from the popular media, other secondary sources, or personal experience; however, the specialists' use different definitions of the meaning. Cyber-terrorism as well as other contemporary "terrorisms" (bioterrorism, chemical terrorism, etc.) appeared as a mixture of words terrorism and a meaning of an area of application. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, who in 1997 was attributed for creation of the term "Cyberterrorism", defined cyber-terrorism as the convergence of cybernetics and terrorism. In the same year Mark Pollitt, special agent for the FBI, offers a working definition: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents."

Since that time the word cyber-terrorism has entered into the lexicon of IT security specialists and terrorist experts and the word list of mass media "professionals". One of the experts, a police chief, offers his version of definition: "Cyber-terrorism – attacking sabotage-prone targets by computer – poses potentially disastrous consequences for our incredibly computer-dependent society."

The media often use cyber-terrorism term quite deliberately: "Canadian boy admits cyberterrorism of his family: "Emeryville, Ontario (Reuter) - A 15-year-old Canadian boy has admitted he was responsible for months of notorious high-tech pranks that terrorized his own family, police said Monday". A renowned expert Dorothy Denning defined cyber-terrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives". R. Stark from the SMS University defines cyber-terrorism as " any attack against an information function, regardless of the means". Under the above-mentioned definitions of cyber-terrorism one can only point to the fact that any telecommunications infrastructure attack, including site defacing and other computer pranks, constitute terrorism. It means that cyber-terrorism has already occurred and we "live " in the epoch of cyber terror.

However, another expert, James Christy the law enforcement and counterintelligence coordinator for the DIAP (Defense-wide Information Assurance Program), which is steered by the office of the assistant secretary of defense for command, control, communications and intelligence, states that cyber-terrorism has never been waged against the United States. "Rather, recent hacking events – including a 1998 web page set up by a supporter of the Mexican Zapatistas rebel group, which led to attacks on the U.S. military from 1,500 locations in 50 different countries – constitute computer crime. William Church, a former U.S. Army Intelligence officer, who founded the Center for Infrastructural Warfare Studies (CIWARS) agrees that the United States has not seen a cyber terrorist threat from terrorists using information warfare techniques. "None of the groups that are conventionally defined as terrorist groups have used information weapons against the infrastructure" Richard Clarke, national co-ordinator for security, infrastructure protection and counterterrorism at the National Security Council offered to stop using "cyber terrorism" and use "information warfare " instead.

The above-mentioned observations drive a clear line between cyber-terrorism and cyber crime and allow us to define cyber-terrorism as: Use of information technology and means by terrorist groups and agents. In defining the cyber terrorist activity it is necessary to segment of action and motivation. There is no doubt that acts of hacking can have the same consequences as acts of terrorism but in the legal sense the intentional abuse of the information cyberspace must be a part of the terrorist campaign or an action. Examples of cyber terrorist activity may include use of information technology to organize and carry out attacks, support groups activities and perception-management campaigns. Experts agree that many terrorist groups such as Osama bin Ladenn organization and the Islamic militant group Hamas have adopted new information technology as a means to conduct operations without being detected by counter terrorist officials. Thus, use of information technology and means by terrorist groups and agents constitute cyber-terrorism. Other activities, so richly glamorized by the media, should be defined as cyber crime.[66]

13.3. Types of Cyber Terrorism

Social networking over the Internet has boomed in recent years because it allows networks of like-minded individuals to collaborate and connect, regardless of their respective geographies or physical location. Cyber terrorism as mentioned is a very serious issue and it covers vide range of attacks.

Some of the major tools of cyber crime may be- Botnets, Estonia, 2007, Malicious Code Hosted on Websites, Cyber Espionage etc.

It is pertinent to mark here that there are other forms which could be covered under the heading of Cyber Crime & simultaneously is also an important tools for terrorist activities. Here I'm going to discuss these criminal activities one by one:

Attacks via Internet : Unauthorised access & Hacking:

one of the criminal activities is unauthorized access that would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the

[66] http://www.crime-research.org/library/Cyber-terrorism.htm

desire to destruct and they get the kick out of such destruction.Trojan Attack: Trojan is a program that acts like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan Virus and Worm attack: A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus. Programs that multiply like viruses but spread from computer to computer are called as worms. E-mail related crimes: Email spoofing: Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.2. Email Spamming Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter. Sending malicious codes through email E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

After investigation about different types of Cyber terrorism which may occur for anybody or organization I would like to mention some case studies to show this definitions and theories in real life.

As you know one of the most popular forms of Cyber terrorism is to threaten a large bank. The terrorists hack into the system and then leave an encrypted message for senior directors, which threaten the bank. What adds to the difficulty to catch the criminals is that the criminals may be in another country. A second difficulty is that most banks would rather pay the money than have the public know how vulnerable they are.

13.4. Effect of Cyber Terrorism on National/International Infrastructure:

The intention of a cyber terrorism attack could range from economic disruption through the interruption of financial networks and systems or used in support of a physical attack to cause further confusion and possible delays in proper response. Although cyber attacks have caused billions of dollars in damage and affected the lives of millions, we have yet witness the implications of a truly

catastrophic cyber terrorism attack. What would some of the implications be? Direct Cost Implications

- Loss of sales during the disruption
- Staff time, network delays, intermittent access for business users
- Increased insurance costs due to litigation
- Loss of intellectual property – research, pricing, etc.
- Costs of forensics for recovery and litigation
- Loss of critical communications in time of emergency
- Indirect Cost Implications
- Loss of confidence and credibility in our financial systems
- Tarnished relationships& public image globally
- Strained business partner relationships – domestic and internationally
- Loss of future customer revenues for an individual or group of companies
- Loss of trust in the government and computer industry

New legislation is requiring system breaches to be reported (SB1386 California). Other proposed legislation would allow damages to be sought by victims of attacks that are launched from hacked web systems. California's SB 1386 is a sweeping measure that mandates public disclosure of computer-security breaches in which confidential information of any California resident may have been compromised. The bill further goes on to define personal information as an individual's first name or initial and last name in combination with a SSN, a driver's license number, or any account numbers, credit card numbers, debit card numbers, and associated passwords or codes. Think of the liability an organization would incur if their systems were compromised and thousands of individuals personal information were exposed and even exploited for financial gain – (funding terrorism).

With the "LoveBug" virus costing nearly $10 billion, it is hard to fathom the financial implications of a much more serious and comprehensive attack. Each and every day corporations in the U.S. and abroad spend millions combating the threats of cyber attacks and cyber terrorism. Corporate efforts reach tens (if not

hundreds) of billions of dollars annually and with the increased frequency of attacks, the cost will significantly increase in the coming years. As we face more and more complex attacks from professional cyber warriors, corporations will increasing seek help from the governments around the world to thwart these efforts and stem the financial bleeding.[67]

13.5. Characteristics of Cyber Terrorism:

"When is an attack in cyberspace considered to be terrorism? The question can be answered by examining what are the common elements to all terrorism. According to Vatis (2001.) acts of terrorism are:

- premeditated and not simply acts born of rage,
- political and designed to impact political structure,
- targeted at civilians and civilian installations, and
- conducted by ad hoc groups as opposed to national armies.

When these elements are applied to cyber terrorism, none of them seems to fail. Firstly, cyber terrorist attacks are premeditated and must be planned since they involve the development or acquisition of software to carry out an attack. Secondly, cyber terrorism acts are intended to corrupt / completely destroy a computer system or systems (Galley 1996.). Cyber terrorists are hackers with a political motivation, their attacks can impact political structure through this corruption and destruction (Furnell and Warren1999, 30.) Thirdly, cyber terrorist attacks often target civilian interests. Denning qualifies cyber terrorism as an attack that results in violence against persons or property, or at least causes enough harm to generate fear (Denning 2000a.). Fourthly, cyber terrorism is sometimes distinguished from cyber warfare, which is computer-based attacks orchestrated by agents of a nation-state."

13.6. Cyber Terrorism-Challenges and Problems:

Understanding why, how and with what consequences terrorists could and would want to use the cyber domain for their purposes is essential to formulating

[67] http://www.crime-research.org/library/Cyberterrorism.html

the best policy practices in preventing and managing the emergence of a cyber-empowered terrorist 'community'. Discourse analysis, epistemology and Sun Tzu's theory of war, along with other pertinent concepts of international relations provide a framework for looking at terrorists' motivations and activities in the cyber world.

Technological developments have seen the virtual domain evolve dramatically, and the 21st century marked acceleration in both- the online world and the threats that arise from it. The recent years have experiences not only an enhanced access to the internet worldwide, greater capabilities of programs and a wider range of services. Computers have also brought technical, political, social and economic problems, with malware being born at a higher frequency than the cures for it. Controls over targets and over attackers have become exceedingly difficult to achieve; and in the latter- practically impossible. More elaborate and complex hacking tendencies often target critical objects- private and public. Although for now, cyber is a domain of close attention in inter-state relations, the potential for terrorist groupings developing the capabilities, access and the motivation to target State and, indeed, private infrastructure is very serious. Many reports, research and intelligence information gathered suggest that in a couple of years from now, terrorists may acquire enough skills to use cyber space for attack purposes (Aitoro, 2009; GCN, 2012; Guneev, 2012).

The subject of cyber terrorism is situated within a very new field of research; therefore specific publications are very limited. However, positioned in a wider context, research easily overlaps with many disciplines, and these will be explored in detail. Authors, doctrines, governments and international organizations differ in opinion not only as to whether cyber terrorism is possible, but also as to the consequences of it, if taken as a plausible situation. I will provide a brief overview of the current prevailing lines of thought. Controversy in literature is largely based on the impossibility to define appropriately the terms and fit them into the existing legislation or into the policy of the state on cyber warfare.[68]

13.7. Who are Cyber Terrorists?:

[68] http://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/

A programmer who breaks into computer systems in order to steal or change or destroy information as a form of cyber-terrorism.

From American point of view the most dangerous terrorist group is Al-Qaeda which is considered the first enemy for the US. According to US official's data from computers seized in Afghanistan indicate that the group has scouted systems that control American energy facilities, water distribution, communication systems, and other critical infrastructure. After April 2001 collision of US navy spy plane and Chinese fighter jet, Chinese hackers launched Denial so Service (DoS) attacks against American web sites. A study that covered the second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks is the United States with 35.4% of the cases down from 40% for the first half of the same year. South Korea came next with 12.8%, followed by China 6.2% then Germany 6.7% then France 4%. The UK came number 9 with 2.2%. According to the same study, Israel was the most active country in terms of number of cyber attacks related to the number of internet users. There are so many groups who are very active in attacking their targets through the computers. The Unix Security Guards (USG) a pro Islamic group launched a lot of digital attacks in May 2002.Another group called World's Fantabulas Defacers (WFD) attacked many Indian sites. Also there is another pro Pakistan group called Anti India Crew (AIC) who launched many cyber attacks against India. There are so many Palestinian and Israeli groups fighting against each other through the means of digital attacks.

13.8. Computer attack and Cyber Terrorism:

A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons, and several may be within the current capabilities of some terrorist groups. Three different methods of attack are identified in this report, based on the effects of the weapons used. However, as technology evolves, distinctions between these methods may begin to blur.

- A physical attack involves conventional weapons directed against a computer facility or its transmission lines;

- An electronic attack (EA) involves the use [of] the power of electromagnetic energy as a weapon, more commonly as an electromagnetic pulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into an enemy microwave radio transmission; and
- A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organization or computer user. Other forms of CNA are enabled when an attacker uses stolen information to enter restricted computer systems.

DOD officials have stated that while CNA and EA threats are "less likely" than physical attacks, they could actually prove more damaging because they involve disruptive technologies that might generate unpredictable consequences or give an adversary unexpected advantages.

Characteristics of Physical Attack: A physical attack disrupts the reliability of computer equipment and availability of data. Physical attack is implemented either through use of conventional weapons, creating heat, blast, and fragmentation, or through direct manipulation of wiring or equipment, usually after gaining unauthorized physical access.

In 1991, during Operation Desert Storm, the U.S. military reportedly disrupted Iraqi communications and computer centers by sending cruise missiles to scatter carbon filaments that short circuited power supply lines. Also, the Al Qaeda attacks directed against the World Trade Center and the Pentagon on September 11, 2001, destroyed many important computer databases and disrupted civilian and military financial and communications systems that were linked globally. The temporary loss of communications links and important data added to the effects of the physical attack by closing financial markets for up to a week.

Characteristics of Electronic Attack (EA): Electronic attack, most commonly referred to as an Electromagnetic Pulse (EMP), disrupts the reliability of electronic equipment through generating instantaneous high energy that overloads circuit boards, transistors, and other electronics. EMP effects can penetrate computer facility walls where they can erase electronic memory, upset software, or permanently disable all electronic components. Some assert that little has been

done by the private sector to protect against the threat from electromagnetic pulse, and that commercial electronic systems in the United States could be severely damaged by limited range, small-scale, or portable electromagnetic pulse devices. Some military experts have stated that the United States is perhaps the nation most vulnerable to electromagnetic pulse attack.

A Commission to Assess the Threat from High Altitude Electromagnetic Pulse was established by Congress in FY2001 after several experts expressed concern that the U.S. critical infrastructure and military were vulnerable to high altitude EMP attack. At a July 22, 2004, hearing before the House Armed Services Committee, panel members from the Commission reportedly stated that as more U.S. military weapons and control systems become increasingly complex, they may also be more vulnerable to the effects of EMP. The consensus of the Commission is that a large-scale high altitude EMP attack could possibly hold our society seriously at risk and might result in defeat of our military forces.

However, the Department of Homeland Security (DHS) has stated that testing of the current generation of civilian core telecommunications switches now in use has shown that they are only minimally affected by EMP. DHS has also stated that most of the core communications assets for the United States are housed in large, very well constructed facilities which provide a measure of shielding against the effects of EMP.

Observers believe that mounting a coordinated attack against U.S. computer systems, using either larger-scale, smaller-scale, or even portable EMP weapons requires technical skills that are beyond the capabilities of most terrorist organizations. However, nations such as Russia, and possibly terrorist-sponsoring nations such as North Korea, now have the technical capability to construct and deploy a smaller chemically-driven, or battery-driven EMP device that could disrupt computers at a limited range.

Characteristics of Cyber attack (CNA): A computer network attack (CNA), or "cyber attack," disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output (for more detail, see Appendices A, B, and C). Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet,

send commands to spy on the contents of that computer or attack and disrupt other computers.

Cyber attacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, for the malicious code to exploit. However, as technology evolves, this distinguishing requirement of CNA may begin to fade. For example, some forms of EA can now cause effects nearly identical to some forms of CNA. For example, at controlled power levels, the transmissions between targeted microwave radio towers can be hijacked and specially designed viruses, or altered code, can be inserted directly into the adversary's digital network.[69]

13.9. Seven Types of Hacker Motivations:

There are good and bad hackers. Here is a window into what they do and why:

White Hat Hackers: These are the good guys, computer security experts who specialize in penetration testing and other methodologies to ensure that a company's information systems are secure.

These IT security professionals rely on a constantly evolving arsenal of technology to battle hackers.

Black Hat Hackers: These are the bad guys, who are typically referred to as just plain hackers. The term is often used specifically for hackers who break into networks or computers, or create computer viruses.

Black hat hackers continue to technologically outpace white hats. They often manage to find the path of least resistance, whether due to human error or laziness, or with a new type of attack.

Hacking purists often use the term "crackers" to refer to black hat hackers. Black hats' motivation is generally to get paid.

Script Kiddies: This is a derogatory term for black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves.

Hacktivists: Some hacker activists are motivated by politics or religion, while others may wish to expose wrongdoing, or exact revenge, or simply harass their

[69] http://www.history.navy.mil/library/online/computerattack.htm

target for their own entertainment. **State Sponsored Hackers:** Governments around the globe realize that it serves their military objectives to be well positioned online. The saying used to be, "He who controls the seas controls the world," and then it was, "He who controls the air controls the world." Now it's all about controlling cyberspace. State sponsored hackers have limitless time and funding to target civilians, corporations, and governments.

Spy Hackers: Corporations hire hackers to infiltrate the competition and steal trade secrets. They may hack in from the outside or gain employment in order to act as a mole. Spy hackers may use similar tactics as hacktivists, but their only agenda is to serve their client's goals and get paid.

Cyber Terrorists: These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Cyber terrorists are by far the most dangerous, with a wide range of skills and goals. Cyber Terrorists ultimate motivation is to spread fear, terror and commit murder.

13.10. Strategies to deal with Cyber Terrorism Threats:

Dealing with cyber terrorists and cyber terrorism takes a thoroughly thought-out and developed plan, and the willingness to take immediate action, preferably before a terrorist event takes place. The following is a simplistic approach to cyber security:

1. Do whatever it takes to protect the infrastructure.
2. Invest to protect your products.
3. Protect your clients, including their personal data.

Be sure that your infrastructure, whether that is your personal computer, social media and online accounts or the multibillion-dollar waterworks station is protected. Start small. Make sure that all passwords are strong by incorporating capital and lower case letters, numbers and symbols in unlikely combinations. Invest in products that increase system security, like malware protection and virus detection, and use encryption to help protect your client's personal information.

Taking security to a higher level, consider hiring an ethical hacker to attempt to gain access to your system, and patch any vulnerability immediately. Also consider insider threat monitoring to identify behaviors and anomalies with your system and to help meet human capital demands. It takes a lot of people to adequately protect

an organization, just as it takes a large number of people to complete a cyber attack. Therefore, think like a cyber terrorist to beat them at their own game. They use technologies to achieve their terrorist goals, so follow suit and use ethical technologies to battle against their unethical acts and spread security as far as possible within your organization.

Surviving Cyberterrorism

Fighting back against highly sophisticated, intelligent cyber terrorists seems to be a no-win situation, but with the proper technologies, experts and the willingness to respond, exploitation can be minimized.

The following steps teach you exactly what to do before, during and after a cyber terrorism attack.

1. Anticipate cyber attacks: The question is not if cyber terrorists are going to attack, it's when. Think about prevention strategies and what you can do now. Do not wait until you are attacked to do something about it because it will be too late.
2. Respond immediately to enhance business continuity: When attacked, the goal is to keep the business functioning as a cohesive unit at all times. This is possible if you have established your security plan and have practiced what to do before an attack rears its ugly head.
3. Monitor all systems in real time: Invest in technologies and experts to monitor your systems 24 hours a day, 7 days a week, 365 days a year.
4. Evolve: Never stop learning ways to survive cyber attacks, and always use each cyber attack as an educational tool to enhance your overall security plan.

Cyber terrorism is a 24/7, 365 days-a-year giant that never sleeps; it doesn't need to eat and it never stops preying. Developing a multifaceted, layered approach to fight against this giant will minimize exploitation of vulnerabilities, allowing people, organizations and the nation to sleep a little easier at night.[70]

13.11. Summary:

[70] http://www.csid.com/2014/03/combating-cyberterrorism-with-cyber-security/

Cyber terrorism is a very burning topic worldwide and the countries are involved to develop a concrete mechanism to combat it and its effect on state instrumentalities. In this unit the concept of cyber terrorism and its general meaning, types of cyber terrorism, effect of cyber terrorism on national arena, international infrastructure, characteristics of cyber terrorism, cyber terrorism-challenges and problems, who are cyber terrorists, computer attack and cyber terrorism, seven types of Hacker motivations, and strategies to deal with cyber terrorism threats are discussed at length to understand the issues related to cyber terrorism.

13.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)

- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

13.13 Check your Progress:

A. Which of the following statements are true or false:
   a) Some examples of cyber terrorism activities include email bombing, hacking into governmental portals/banking/ hospitals etc. websites.
   b) Cyber terrorism is premeditated and politically motivated attack against information, computer system, computer program and data.
   c) The intention of a cyber terrorism attack could range from economic disruption through the financial networks and systems.
   d) Cyber terrorism is sometimes distinguished from cyber warfare, which is computer based attacks by agents of a nation-state.
   e) A physical attack involves conventional weapons directed against a computer facility or its transmission lines.

B. Fill in the Blanks:
   I. An e-mail bomb may be considered ……by some and cyber terrorism by others.

II. ……virus costing nearly $ 10 billion, it is hard to fathom the financial implications of a much more serious and comprehensive attack.

III. A programmer who …….

IV. Information as a form of cyber terrorism.

V. ……., during operation Desert Storm, the US military reportedly disrupted Iraqi communications and computer centers.

VI. White Hat Hackers are the ……..

13.14 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Hacktivism
2. Love bug
3. Breaks into computer system in a order to steal or change or destroy
4. In 1991
5. Good Guys

13.15 Terminal Questions

1. What is the meaning and types of cyber terrorism?
2. What is the effect of cyber terrorism on national/international infrastructure?
3. What are the characteristics of cyber terrorism?
4. Who are cyber terrorist?
5. What are the seven types of hacker motivations?

Unit-14

Cyber Terrorism-Global Perspective

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Cyber Terrorism with reference to Global Perspective
- Understand the importance of Judicial Decisions delivered by various bodies
- Understand the technical and legal issues related to Cyber Terrorism with reference to Global Perspective

Structure:

14.1. Introduction:

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Computers and the internet are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier. They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life. The most deadly and destructive consequence of this helplessness is the emergence of the concept of "cyber terrorism". The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism.
The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace" is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straightjacket formula or pigeons whole. In fact, the first effort of the Courts should be to interpret the definition as liberally as possible so that the menace of cyber terrorism can be tackled stringently and with a punitive hand.
The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world.

14.2. Global Definition of Cyber Terrorism:

Although there are a number of definitions which describe the term terrorism, one of the definitions that are frequently encountered is that terrorism is "the unlawful use or threatening use of force or violence by a person or an organized group against people or property with the intention of intimidating or forcing societies or governments, often for ideological or political reasons." Interactions between human motives and information technology for terrorist activities in cyberspace or in the virtual world can be addressed as cyber terrorism. Yet this is the definition of cyber terrorism that Sarah Gordon and Richard Ford from Symantec have used in their efforts to define "pure Cyber terrorism." The cyber terrorism as a concept has various definitions, mostly because every expert in security has its own definition. This term can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This may include the use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructure, and to exchange information and perform electronic threat. This kind of security threat can manifest itself in many ways, such as hacking computer systems, programming viruses and worms, Web pages attack, conducting denial of service (DoS) attacks, or conducting terrorist attacks through electronic communications. More common are claims that cyber terrorism does not exist and that actually it is a hacking and malicious attacks. Those who support these claims do not agree with the term "terrorism" because if we take into account the current technologies for prevention and care, the likelihood of creating fear, significant physical damage or death among population using electronic means would be very small.[71]

The U.S National Infrastructure Protection Center defined the term as, "A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/ or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda."
Center for strategic and International Studies defined Cyber Terrorism as,

---

71 http://eprints.ugd.edu.mk/6849/1/CYBER%20TERRORISM%E2%80%93%20GLOBAL%20SECURITY%20THREAT%20-%20Mitko%20Bogdanoski.pdf

"The use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population ". (The center for Strategic Infrastructure Studies (NIPS), formerly a unit of the federal Bureau **of Investigation (FBI) It conducts investigations and provides a response to computer attacks.)**

A 1999 study prepared for the Defense Intelligence Agency and produced at the Naval Postgraduate School began with a disclaimer stating, "cyber terror is not a threat. At least not yet, and not for a while." Nevertheless, the authors warned, "cyber terror is indeed coming."Around the same time, Richard Clarke, who at that time was the White House special adviser for cyberspace security, preferred use of the term "info warfare" instead of cyber terrorism. More than a decade later, he still rejected the word cyber terrorism on the basis that it is a red herring that "conjure[s] up images of Bin Ladin waging war from his cave"; he did, however, caution that there may be such a term as cyber terrorism in the future. Barry Collin first introduced the term cyber terrorism in the 1980s, although just as experts have not formed a consensus definition of terrorism, there is still no unifying definition of cyber terrorism. Cyber terrorism is an even more opaque term than terrorism, adding another layer to an already contentious concept. Cyber events in general are often misunderstood by the public and erroneously reported by the media. People tend to use the terms cyber war, cyber terrorism, cybercrime, and hacktivism interchangeably, although there are important, sometimes subtle, differences.[72]

Bruce Hoffman defines terrorism as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change." If one assumes for a moment that this was the accepted definition of terrorism, then the addition of cyber to this term results in a simple, though circular definition: cyber terrorism is the use of cyber to commit terrorism. Given the range of cyber terrorism activities described in the literature and depicted in the clusters shown in Figure 1 (see PDF version), this simple definition can be expanded to: cyber terrorism is the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change.[73]

---

[72] https://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace

[73] Bruce Hoffman, Inside Terrorism (New York: Columbia University Press, 2006), p. 40

14.3. International Legal Efforts: Prior to the adoption of resolution 1373 (2001) and the establishment of the Counter-Terrorism Committee, the international community had already promulgated 12 of the current 16 international counter-terrorism legal instruments. However, the rate of adherence to these conventions and protocols by United Nations Member States was low. As a result of the attention focused on countering terrorism since the events of 11 September 2001 and the adoption of Security Council resolution 1373 (2001), which calls on States to become parties to these international instruments, the rate of adherence has increased: some two-thirds of UN Member States have either ratified or acceded to at least 10 of the16 instruments, and there is no longer any country that has neither signed nor become a party to at least one of them. Between 1963 and 2004, under the auspices of the United Nations and its specialized agencies, the international community developed 13 international counter-terrorism instruments which are open to participation by all Member States. In 2005, the international community also introduced substantive changes to three of these universal instruments to specifically account for the threat of terrorism; on 8 July of that year States adopted the Amendments to the Convention on the Physical Protection of Nuclear Material, and on 14 October they agreed to both the Protocol of 2005 to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf.

The General Assembly has focused on terrorism as an international problem since 1972 and, through the 1980s, addressed the issue intermittently through resolutions. During this period, the Assembly also adopted two instruments related to counter-terrorism: the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (in 1973) and the International Convention against the Taking of Hostages (in 1979).

In December 1994, the Assembly again directed attention to this issue through a Declaration on Measures to Eliminate International Terrorism (A/RES/49/60). In 1996, a supplement to this Declaration (A/RES/51/210) established an Ad Hoc Committee to elaborate an international convention for the suppression of terrorist bombings and, subsequently, an international convention for the suppression of acts of nuclear terrorism, to supplement related existing international instruments,

and thereafter to address means of further developing a comprehensive legal framework of conventions dealing with international terrorism. This mandate continued to be renewed and revised on an annual basis by the General Assembly in its resolutions on the topic of measures to eliminate international terrorism.

During the past decade, Member States completed work on three more counter-terrorism instruments covering specific types of terrorist activities: the 1997 International Convention for the Suppression of Terrorist Bombings; the 1999 International Convention for the Suppression of the Financing of Terrorism and the International Convention for the Suppression of Acts of Nuclear Terrorism. The last of these was adopted in April 2005 and opened for signature on 14 September 2005, the first day of the General Assembly's World Summit. During that three-day high-level meeting, it was signed by 82 Member States.

It is also within the framework of the Ad Hoc Committee that Member States have been negotiating a draft comprehensive convention on international terrorism since 2000.

14.4. Suppression of Financing to Terrorism: (UN Resolution Number 1373/2001):

Resolution 1373 (2001) Also Creates Committee to Monitor Implementation: Reaffirming its unequivocal condemnation of the terrorist acts that took place in New York, Washington, D.C., and Pennsylvania on 11 September, the Security Council this evening unanimously adopted a wide-ranging, comprehensive resolution with steps and strategies to combat international terrorism. By resolution 1373 (2001) the Council also established a Committee of the Council to monitor the resolution's implementation and called on all States to report on actions they had taken to that end no later than 90 days from today. Under terms of the text, the Council decided that all States should prevent and suppress the financing of terrorism, as well as criminalize the wilful provision or collection of funds for such acts. The funds, financial assets and economic resources of those who commit or attempt to commit terrorist acts or participate in or facilitate the commission of terrorist acts and of persons and entities acting on behalf of terrorists should also be frozen without delay. The Council also decided that States should prohibit their nationals or persons or entities in their territories from making funds, financial

assets, economic resources, financial or other related services available to persons who commit or attempt to commit, facilitate or participate in the commission of terrorist acts. States should also refrain from providing any form of support to entities or persons involved in terrorist acts; take the necessary steps to prevent the commission of terrorist acts; deny safe haven to those who finance, plan, support, commit terrorist acts and provide safe havens as well. By other terms, the Council decided that all States should prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other countries and their citizens. States should also ensure that anyone who has participated in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice. They should also ensure that terrorist acts are established as serious criminal offences in domestic laws and regulations and that the seriousness of such acts is duly reflected in sentences served. Also by the text**,** the Council called on all States to intensify and accelerate the exchange of information regarding terrorist actions or movements; forged or falsified documents; traffic in arms and sensitive material; use of communications and technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction.

States were also called on to exchange information and cooperate to prevent and suppress terrorist acts and to take action against the perpetrators of such acts. States should become parties to, and fully implement as soon as possible, the relevant international conventions and protocols to combat terrorism. By the text, before granting refugee status, all States should take appropriate measures to ensure that the asylum seekers had not planned, facilitated or participated in terrorist acts. Further, States should ensure that refugee status was not abused by the perpetrators, organizers or facilitators of terrorist acts, and that claims of political motivation were not recognized as grounds for refusing requests for the extradition of alleged terrorists. The Council noted with concern the close connection between international terrorism and transnational organized crime, illicit drugs, money laundering and illegal movement of nuclear, chemical, biological and other deadly materials. In that regard, it emphasized the need to enhance the coordination of national, sub regional, regional and international efforts to strengthen a global response to that threat to international security. Reaffirming the need to combat by all means, in accordance with the Charter,

threats to international peace and security caused by terrorist acts, the Council expressed its determination to take all necessary steps to fully implement the current resolution.

14.5. UN Action to Counter Terrorism:

Guided by Security Council resolutions 1373 (2001) and 1624 (2005), the CTC works to bolster the ability of United Nations Member States to prevent terrorist acts both within their borders and across regions. It was established in the wake of the 11 September terrorist attacks in the United States. Raimonda Murmokaitė, Ambassador and Permanent Representative of Lithuania, assumed the chairmanship of the Committee in January 2014.

The CTC is assisted by the Counter-Terrorism Committee Executive Directorate (CTED), which carries out the policy decisions of the Committee, conducts expert assessments of each Member State and facilitates counter-terrorism technical assistance to countries. Resolution 1373 (2001), adopted unanimously on 28 September 2001, calls upon Member States to implement a number of measures intended to enhance their legal and institutional ability to counter terrorist activities, including taking steps to:

- Criminalize the financing of terrorism
- Freeze without delay any funds related to persons involved in acts of terrorism
- Deny all forms of financial support for terrorist groups
- Suppress the provision of safe haven, sustenance or support for terrorists
- Share information with other governments on any groups practicing or planning terrorist acts
- Cooperate with other governments in the investigation, detection, arrest, extradition and prosecution of those involved in such acts; and
- Criminalize active and passive assistance for terrorism in domestic law and bring violators to justice.

The resolution also calls on States to become parties, as soon as possible, to the relevant international counter-terrorism legal instruments.

Resolution 1624 (2005) pertains to incitement to commit acts of terrorism, calling on UN Member States to prohibit it by law, prevent such conduct and deny safe haven to anyone "with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of such conduct."
Working Methods: In short, the work of the CTC and CTED comprises:

- Country visits - at their request, to monitor progress, as well as to evaluate the nature and level of technical assistance a given country may need in order to implement resolution 1373 (2001);
- Technical assistance - to help connect countries to available technical, financial, regulatory and legislative assistance programmes, as well as to potential donors;
- Country reports – to provide a comprehensive snapshot of the counter-terrorism situation in each country and serve as a tool for dialogue between the Committee and Member States;
- Best practices – to encourage countries to apply known best practices, codes and standards, taking into account their own circumstances and needs; and
- Special meetings – to develop closer ties with relevant international, regional and sub regional organizations, and to help avoid duplication of effort and waste of resources through better coordination

The Counter-Terrorism Committee (CTC) was established by Security Council resolution 1373 (2001), which was adopted unanimously on 28 September 2001 in the wake of the 11 September terrorist attacks in the United States. The Committee, comprising all 15 Security Council members, was tasked with monitoring implementation of resolution 1373 (2001), which requested countries to implement a number of measures intended to enhance their legal and institutional ability to counter terrorist activities at home, in their regions and around the world, including taking steps to:

- Criminalize the financing of terrorism
- Freeze without delay any funds related to persons involved in acts of terrorism
- Deny all forms of financial support for terrorist groups

- Suppress the provision of safe haven, sustenance or support for terrorists
- Share information with other governments on any groups practicing or planning terrorist acts
- Cooperate with other governments in the investigation, detection, arrest, extradition and prosecution of those involved in such acts; and
- Criminalize active and passive assistance for terrorism in domestic law and bring violators to justice.

The resolution also calls on States to become parties, as soon as possible, to the relevant international counter-terrorism legal instruments.

In September 2005, the Security Council adopted resolution 1624 (2005) on incitement to commit acts of terrorism, calling on UN Member States to prohibit it by law, prevent such conduct and deny safe haven to anyone "with respect to whom there is credible and relevant information giving serious reasons for considering that they have been guilty of such conduct." The resolution also called on States to continue international efforts to enhance dialogue and broaden understanding among civilizations. The Security Council directed the CTC to include resolution 1624 (2001) in its ongoing dialogue with countries on their efforts to counter terrorism.

The Counter-Terrorism Committee Executive Directorate (CTED):

Under resolution 1535 (2004), the Security Council established the Counter-Terrorism Committee Executive Directorate (CTED) to assist the work of the CTC and coordinate the process of monitoring the implementation of resolution 1373 (2001).

CTED became fully staffed in September 2005 and was formally declared operational in December 2005. CTED's mandate was extended until the end of 2013 by Security Council resolution S/RES/1963 (2010).

CTED comprises some 40 staff members, about half of whom are legal experts who analyze the reports submitted by States in areas such as legislative drafting, the financing of terrorism, border and customs controls, police and law enforcement, refugee and migration law, arms trafficking and maritime and transportation security. CTED also has a senior human rights officer.

CTED is divided into two sections: an Assessment and Technical Assistance Office (ATAO), which is further divided into three geographical clusters to enable

the experts to specialize in particular regions of the world, and an Administrative and Information Office (AIO).

In addition, five technical groups work horizontally across ATAO to identify issues and criteria for making assessments in their particular area of technical expertise and then disseminate these across the three clusters. The groups deal respectively with technical assistance; terrorist financing; border control, arms trafficking and law enforcement; general legal issues, including legislation, extradition and mutual legal assistance; and finally, issues raised by resolution 1624 (2005); as well as the human rights aspects of counter-terrorism in the context of resolution 1373 (2001).

Across AIO, there is also a quality control unit to improve the technical quality and consistency in language and format of CTED documents and a public communications and outreach unit to strengthen its outreach activities.

In support of the Committee's work on resolution 1624 (2005), CTED has prepared two reports (S/2006/737 and S/2008/2) summarizing the responses submitted thus far by about half of the United Nations membership

.

14.6. Cyber Terrorism viz a viz Cyber Crime:

"Cyber terrorism is also clearly an emerging threat. Terrorist groups are increasingly computer savvy, and some probably are acquiring the ability to use cyber attacks to inflict isolated and brief disruptions of US infrastructure. Due to the prevalence of publicly available hacker tools, many of these groups probably already have the capability to launch denial-of-service and other nuisance attacks against Internet-connected systems. As terrorists become more computer savvy, their attack options will only increase." (War on Terrorism, 2003) This is what Robert Mueller, FBI Director, testified on 11 February 2003 before the US Senate on a hearing about War On Terrorism against Al-Qaeda and other terrorist organizations. The US and global media organizations picked up this testimony and begun speculating on the possibility of a large-scale Cyber terrorist attack. So far, such an attack has not materialized. At the same time a similar term, Cybercrime, is used to describe criminal activities on the Internet such as identity theft, copyright infringement and bank fraud, but many times these two terms (Cybercrime and Cyber terrorism) end up been used inter-changeably and their

meaning, especially to the public, becomes blurred and unclear. Governments, policy networks and the media around the globe have engaged in an effort to build defences against Cyber attacks, bring new regulations in effect while maintaining an almost mythological atmosphere over the threats and risks of potential Cybercrime and Cyber terrorist attacks.

As the global reach of the Internet keeps growing, its effect on all areas of online human endeavour becomes more pervasive. Individuals or groups can exploit the anonymity afforded by cyberspace to engage in illegal or illicit activities that aim to intimidate, harm, threaten or cause fear to citizens, communities, organizations or countries. The virtual and physical distance between the attacker and the victim and the difficulty in tracing back the attack to an individual minimizes the inherent threat of capture to the attacker. But how are such activities defined? What is a Cybercrime and what are its characteristics? How can a Cyberterrorist be identified and what are his or her differences from a Cybercriminal? So far, the definitions for Cybercrime and Cyber terrorism in literature, government documents and everyday use have been highly varied, context-specific and emotionally loaded, which makes discourse on the subject difficult. The FBI alone has published three distinct definitions of Cyber terrorism: "Terrorism that initiates…attack[s] on information" in 1999, to "the use of Cyber tools" in 2000 and "a criminal act perpetrated by the use of computers" in 2004." (Baranetsky, 2009). Cybercrime and Cyber terrorism have been used to describe online acts such as:

- Black-hat hacking / Cracking
- Child sex offences (pornography and grooming)
- Crimes in virtual worlds
- Cyber activism / Hacktivism
- Virus writing and malware
- Cyber stalking
- Identity theft / Fraud
- Illegal financial transactions / Money laundering
- Copyright infringement
- Serious acts of cyber bullying
- Denial of service attacks
- Rogue bot-nets

Cyber terrorism usually has a stronger meaning than Cybercrime, describing acts that have similar characteristics to real-world terrorism attacks, but not always. On the other hand, Cybercrime is often used as a catch-all term to describe illegal, harmful and/or hostile activity on the Internet (including Cyber terrorism). Furthermore, other terms are sometimes used to describe similar illicit online acts, which complicate things even more, and their use is typically dependant on the context or the person/organisation that uses them. For example, a spokesperson within the military is likely to use the term Cyber warfare to describe hostile online acts between two countries and/or acts of terrorism that originate from another country and are manifested online (instead of using the term Cyber terrorism).

Before attempting to define Cyber terrorism and Cybercrime one has to reflect on the validity of the two terms. Taipale (2010) has argued that "Cyber terrorism, whatever it is, is a useless term" and he believes that, "terrorists will use any strategic tool they can" so Cyber terrorism is no more important than other forms. A similar argument could be made for Cybercrime, as Wall (2008) says, "Cybercrime is relatively meaningless by itself because it is mainly a fictional construction that has no original reference point in law, science or social action.". However, the term is gradually gaining ground in formal legal discourse due to new legislation in many countries such as Australia (Cybercrime Act 2001), Nigeria (Draft Cybercrime Act), the United States (proposed Cybercrime Act 2007) and the UK (the Home Office introduced its Cybercrime Strategy in March 2010).

An additional layer of complexity is added when one looks at the legal systems of different countries and their varied definitions of unlawful acts. It is not unusual for what one country defines as a criminal offence to merely be a civil wrong in another. The problem arises when an individual is the receiver of news about a Cyber terrorist attack in a foreign country, that would only be characterised as a hacking attempt or an Cyber activism protest in his or her own country, and vice versa. It is thus likely that a person can manifest unwarranted feelings of fear, insecurity, anxiety or panic, along with a general confusion on how to interpret the news.[74]

[74] http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/

Cybercrime and Cyber terrorism are two issues that are likely to continue to exist for many years to come and they surely must be dealt with. But this process needs to be done in a way that will ensure the growth of the Internet in an inclusive and open way, maintaining the fundamental principles that it has been built upon. One of the principal issues is the disambiguation of the terms Cybercrime and Cyber terrorism. Government bodies, policy networks, scholars, the media and the people need to engage in a global conversation that will help demythologize Cybercrime and define what constitutes a Cybercrime and how Cybercriminals should be dealt with. Cyber terrorism should be decoupled from Cybercrime and be specified in realistic terms, as to what are the probable threats of a Cyber terrorist act and to what extend society should go to face such effects. After these two terms have been clearly and unambiguously defined, people will be much better equipped to receive and comprehend related news and policies, and will be able to engage in a meaningful discourse over the subject. This will help alleviate unwarranted fears while at the same time enable individuals to make informed decisions when considering a new proposed policy by weighing its pros versus the cons and its effects on multiple levels, long and short term , instead of giving-in to fear and forfeiting their privacy and online freedom for better security.

The role of the media (television, blogs, online news outlets and more) is critical in the process of educating the public and engaging in a conversation, as they will be the mediators and curators of information and discourse on the issue. Thus, a concise and sensible approach, devoid of fear-mongering and shock practices, should be followed. Since this is an international issue, governments and policy networks across the world have to come together and discuss openly on what is better for their citizens. Scholars and academics can provide valuable expertise on technological, psychological, ethical and other issues, while highlighting any misgivings by those involved in the process. The people in their local communities, families and social networks should help and train each other to increase their peers' level of Internet literacy and highlight the advantages of the web. A higher Internet literacy level can help people protect themselves even better by taking simple security measures, such as using anti-virus software and identifying potential risks or scams in their online financial transactions.[75]

[75] http://iconof.com/blog/cybercrime-cyberterrorism-inducing-anxiety-fear-on-individuals/

14.7. Cyber Warfare and Cyber Terrorism:

Terms such as “cyber war” and “cyber terrorism” have been extensively used in the media, in the official governmental reports and amongst academics. Even if they have been often hyped, experts agree that it is unlikely that cyber war will occur in the future (Thomas Rid and Bruce Scheneier; on the contrary, Jeffrey Carr). Nonetheless, they do acknowledge that cyber threats are real and that various cyber tools and techniques are becoming increasingly important in international conflict, including those used for sabotage, espionage, and subversion. Common element between the two is the lack of an internationally accepted definition.

US government security expert Richard A. Clarke, in his book Cyber War, defines “cyber warfare” as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.” The Economist describes “cyber warfare” as “the fifth domain of warfare”.

The lack of common understanding opens various other issues:

- How it is possible to formulate a definition of “cyber war” while facing the impossibility of proving the source of an attack ?
- Which might be the implication for the right of self-defense and for the rule of engagement?
- Without a clear attribution, how it is conceivable to distinguish cyber war acts from cyber terrorism attacks?

The word “cyber terrorism” refers to two elements: cyberspace and terrorism. Mark Pollitt constructs a working definition such as the following: “Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non combatant targets by sub national groups or clandestine agents. ”This definition is necessarily narrow. For the term “cyber terrorism” to have any meaning, we must be able to differentiate it from other kinds of computer abuse such as computer crime, economic espionage, or information warfare. I would suggest that the latter is a offensive and defensive function of governments. It is first important to note that no single definition of the term “terrorism” has yet gained universal acceptance. Additionally, no single definition for the term “cyber terrorism” has been universally accepted. Also, labeling a computer attack as

"cyber terrorism" is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred.

The Stuxnet code, the cyber espionage alleged to originate in China, and the attacks to Estonia and Georgia have been widely reported as examples of cyber terrorism and possible acts of cyber war . Profound investigations of the incidents could prove neither an authorship of a sovereign state nor serious harm as a consequence of the attacks. This is one of the most fundamental problems: In the relative anonymity and complexity of the Internet and the ability to cross international borders and jurisdictions with impunity, it is very difficult to know exactly who is behind the attacks and their exact motive.[76]

14.8. International Case Study-I:

Analyzing Cyber Attacks under Jus ad Bellum- The law of war is divided into two principal areas, *jus ad bellum* and *jus in bello*. Jus ad bellum, also known as the law of conflict management, is the legal regime governing the transition from peace to war. It basically lays out when states may lawfully resort to armed conflict. Jus in bello, also known as the law of armed conflict, governs the actual use of force during war. The analysis of whether states can respond to cyber attacks with active defenses predominantly falls under jus ad bellum, since jus ad bellum sets forth the thresholds that cyber attacks must cross to be considered acts of war.

Historically, the transition from peace to war fell under the prerogative of the sovereign; however, it came under international law following World War II with the ratification of the UN Charter. Although the UN Charter is not the only source of jus ad bellum, it is the starting point for all jus ad bellum analysis. The relevant articles of the UN Charter are Articles 2(4), 39, and 51, which provide the framework for modern jus ad bellum analysis.

Cyber attacks represent a conundrum for legal scholars. Cyber attacks come in many different forms, their destructive potential limited only by the creativity and skill of the attackers behind them. Although it may seem intuitive that cyber

[76] http://www.techandlaw.net/areas-of-interest/cyberwar-and-cyberterrorism

attacks can constitute armed attacks, especially in light of their ability to injure or kill, the legal community has been reluctant to adopt this approach because cyber attacks do not resemble traditional armed attacks with conventional weapons. Further clouding the legal waters is the erroneous view of states and scholars alike on the need for states to attribute cyber attacks to a state or its agents before responding with force. Although it is true that cyber attacks do not resemble traditional armed attacks, and that cyber attacks are difficult to attribute, neither of these characteristics should preclude states from responding with force. This section explores different analytical models for assessing armed attacks, the logical meaning of the duty of prevention as it relates to cyber attacks, and the technological capacity of trace programs to trace attacks back to their point of origin. After all of these issues are examined, it becomes clear that states may legally use active defenses against cyber attacks originating from states that violate their duty to prevent them.

Cyber Attacks as Armed Attacks

Victim-states must be able to classify a cyber attack as an armed attack or imminent armed attack before responding with active defenses because, as we discussed earlier in this chapter, armed attacks and imminent armed attacks are the triggers that allow states to respond in self-defense or anticipatory self-defense. Ideally, there would be clear rules for classifying cyber attacks as armed attacks, imminent armed attacks, or lesser uses of force. Unfortunately, since cyber attacks are a relatively new attack form, international efforts to classify them are still in their infancy, even though the core legal principles governing armed attacks are well settled. Consequently, whether cyber attacks can qualify as armed attacks and which cyber attacks should be considered armed attacks are left as open questions in international law. To answer these questions, this subsection examines the core legal principles governing armed attacks, applies them to cyber attacks, explains why cyber attacks can qualify as armed attacks, and attempts to provide some insight into which cyber attacks should be considered armed attacks.

"Armed attack" is not defined by any international convention. As a result, its meaning has been left open to interpretation by states and scholars. Although this might sound problematic, it is not. The framework for analyzing armed attacks is relatively well-settled, as are the core legal principles governing its meaning. The international community generally accepts Jean S. Pictet's scope, duration, and

intensity test as the starting point for evaluating whether a particular use of force constitutes an armed attack. Under Pictet's test, a use of force is an armed attack when it is of sufficient scope, duration, and intensity. Of course, as is the case with many international legal concepts, states, nongovernmental organizations, and scholars all interpret the scope, duration, and intensity test differently.

State declarations help flesh out which uses of force are of sufficient scope, duration, and intensity to constitute an armed attack. Harkening back to the French-language version of the UN Charter, which refers to "armed aggression" rather than an "armed attack," the UN General Assembly passed the Definition of Aggression resolution in 1974. The resolution requires an attack to be of "sufficient gravity" before it is considered an armed attack. The resolution never defines armed attacks, but it does provide examples that are widely accepted by the international community. Although the resolution has helped settle the meaning of armed attacks for conventional attacks, the more technology has advanced, the more attacks have come in forms not previously covered by state declarations and practices. Consequently, states recognize that unconventional uses of force may warrant treatment as an armed attack when their scope, duration, and intensity are of sufficient gravity. As a result, states are continually making proclamations about new methods of warfare, slowly shaping the paradigm for classifying armed attacks.

Scholars have advanced several analytical models to deal with unconventional attacks, such as cyber attacks, to help ease attack classification and put the scope, duration, and intensity analysis into more concrete terms. These models are especially relevant to cyber attacks because they straddle the line between criminal activity and armed warfare. There are three main analytical models for dealing with unconventional attacks. The first model is aninstrument-based approach, which checks to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack.[14] The second is an effects-based approach, sometimes called a consequence-based approach, in which the attack's similarity to a kinetic attack is irrelevant and the focus shifts to the overall effect that the cyber attack has on a victim-state.[15] The third is a strict liability approach, in which cyber attacks against critical infrastructure are automatically treated as armed attacks, due to the severe consequences that can result from disabling those systems.[16]

Of these three approaches, the effects-based approach is the best analytical model for dealing with cyber attacks. Not only does effects-based analysis account for everything that an instrument-based approach covers, but it also provides an analytical framework for situations that do not neatly equate to kinetic attacks.[17] Effects-based analysis is also superior to strict liability because responses to cyber attacks under an effects-based approach comport with internationally accepted legal norms and customs, whereas a strict liability approach may cause victim-states to violate the law of war.[18]

Of all of the scholars who advocate effects-based models, Michael N. Schmitt has advanced the most useful analytical framework for evaluating cyber attacks. In his seminal article "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," Schmitt lays out six criteria for evaluating cyber attacks as armed attacks.[19] These criteria are severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. Taken together, they allow states to measure cyber attacks along several different axes. While no one criterion is dispositive, cyber attacks satisfy enough criteria to be characterized as armed attacks. Since their publication, Schmitt's criteria have gained traction in the legal community, with several prominent legal scholars advocating for their use. Many hope that Schmitt's criteria will help bring some uniformity to state efforts to classify cyber attacks. However, until Schmitt's criteria gain wider acceptance, states are likely to classify cyber attacks differently, depending on their understanding of armed attacks as well as their conception of vital national interest.

Classifying cyber attacks will be difficult for states to do in practice.[20] Although the initial decision to respond to cyber attacks under the law of war as a matter of policy will have to be made by state policymakers, the actual decision to use active defenses will have to be pushed down to the system administrators who actually operate computer networks. One of the challenges policymakers will face is translating international law into concise, understandable rules for their system administrators to follow, so that a state's agents comply with international law while protecting its vital computer networks. However, classifying cyber attacks as armed attacks or imminent armed attacks is only the first hurdle system

administrators must clear before responding with active defenses. The second and equally important hurdle is establishing state responsibility for the attack.[77]

14.9. International Case Study-II:

Cyber Attacks as Armed Attacks: Victim-states must be able to classify a cyber attack as an armed attack or imminent armed attack before responding with active defenses because, as we discussed earlier in this chapter, armed attacks and imminent armed attacks are the triggers that allow states to respond in self-defense or anticipatory self-defense. Ideally, there would be clear rules for classifying cyber attacks as armed attacks, imminent armed attacks, or lesser uses of force. Unfortunately, since cyber attacks are a relatively new attack form, international efforts to classify them are still in their infancy, even though the core legal principles governing armed attacks are well settled. Consequently, whether cyber attacks can qualify as armed attacks and which cyber attacks should be considered armed attacks are left as open questions in international law. To answer these questions, this subsection examines the core legal principles governing armed attacks, applies them to cyber attacks, explains why cyber attacks can qualify as armed attacks, and attempts to provide some insight into which cyber attacks should be considered armed attacks.

"Armed attack" is not defined by any international convention. As a result, its meaning has been left open to interpretation by states and scholars. Although this might sound problematic, it is not. The framework for analyzing armed attacks is relatively well-settled, as are the core legal principles governing its meaning. The international community generally accepts Jean S. Pictet's scope, duration, and intensity test as the starting point for evaluating whether a particular use of force constitutes an armed attack. Under Pictet's test, a use of force is an armed attack when it is of sufficient scope, duration, and intensity. Of course, as is the case with many international legal concepts, states, nongovernmental organizations, and scholars all interpret the scope, duration, and intensity test differently.

State declarations help flesh out which uses of force are of sufficient scope, duration, and intensity to constitute an armed attack. Harkening back to the French-language version of the UN Charter, which refers to "armed aggression"

[77] https://www.safaribooksonline.com/library/view/inside-cyber-warfare/9781449318475/ch04.html

rather than an "armed attack," the UN General Assembly passed the Definition of Aggression resolution in 1974. The resolution requires an attack to be of "sufficient gravity" before it is considered an armed attack. The resolution never defines armed attacks, but it does provide examples that are widely accepted by the international community. Although the resolution has helped settle the meaning of armed attacks for conventional attacks, the more technology has advanced, the more attacks have come in forms not previously covered by state declarations and practices. Consequently, states recognize that unconventional uses of force may warrant treatment as an armed attack when their scope, duration, and intensity are of sufficient gravity. As a result, states are continually making proclamations about new methods of warfare, slowly shaping the paradigm for classifying armed attacks.

Scholars have advanced several analytical models to deal with unconventional attacks, such as cyber attacks, to help ease attack classification and put the scope, duration, and intensity analysis into more concrete terms. These models are especially relevant to cyber attacks because they straddle the line between criminal activity and armed warfare. There are three main analytical models for dealing with unconventional attacks. The first model is an instrument-based approach, which checks to see whether the damage caused by a new attack method previously could have been achieved only with a kinetic attack. The second is an effects-based approach, sometimes called a consequence-based approach, in which the attack's similarity to a kinetic attack is irrelevant and the focus shifts to the overall effect that the cyber attack has on a victim-state. The third is a strict liability approach, in which cyber attacks against critical infrastructure are automatically treated as armed attacks, due to the severe consequences that can result from disabling those systems.

Of these three approaches, the effects-based approach is the best analytical model for dealing with cyber attacks. Not only does effects-based analysis account for everything that an instrument-based approach covers, but it also provides an analytical framework for situations that do not neatly equate to kinetic attacks. Effects-based analysis is also superior to strict liability because responses to cyber attacks under an effects-based approach comport with internationally accepted legal norms and customs, whereas a strict liability approach may cause victim-states to violate the law of war.

Of all of the scholars who advocate effects-based models, Michael N. Schmitt has advanced the most useful analytical framework for evaluating cyber attacks. In his seminal article "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," Schmitt lays out six criteria for evaluating cyber attacks as armed attacks. These criteria are severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. Taken together, they allow states to measure cyber attacks along several different axes. While no one criterion is dispositive, cyber attacks satisfy enough criteria to be characterized as armed attacks. Since their publication, Schmitt's criteria have gained traction in the legal community, with several prominent legal scholars advocating for their use. Many hope that Schmitt's criteria will help bring some uniformity to state efforts to classify cyber attacks. However, until Schmitt's criteria gain wider acceptance, states are likely to classify cyber attacks differently, depending on their understanding of armed attacks as well as their conception of vital national interest.

Classifying cyber attacks will be difficult for states to do in practice. Although the initial decision to respond to cyber attacks under the law of war as a matter of policy will have to be made by state policymakers, the actual decision to use active defenses will have to be pushed down to the system administrators who actually operate computer networks. One of the challenges policymakers will face is translating international law into concise, understandable rules for their system administrators to follow, so that a state's agents comply with international law while protecting its vital computer networks. However, classifying cyber attacks as armed attacks or imminent armed attacks is only the first hurdle system administrators must clear before responding with active defenses. The second and equally important hurdle is establishing state responsibility for the attack.[78]

14.10. International Case Study-III:

Black Ice: The Invisible Threat of Cyber-Terror, a book published in 2003 and written by Computerworld journalist and former intelligence officer Dan Verton, describes the 1997 exercise code-named "Eligible Receiver," conducted by the National Security Agency (NSA). (The following account draws from "Black

[78] https://www.safaribooksonline.com/library/view/inside-cyber-warfare/9781449318475/ch04.html

Ice," Computerworld, August 13, 2003.) The exercise began when NSA officials instructed a "Red Team" of thirty-five hackers to attempt to hack into and disrupt U.S. national security systems. They were told to play the part of hackers hired by the North Korean intelligence service, and their primary target was to be the U.S. Pacific Command in Hawaii. They were allowed to penetrate any Pentagon network but were prohibited from breaking any U.S. laws, and they could only use hacking software that could be downloaded freely from the Internet. They started mapping networks and obtaining passwords gained through "brute-force cracking" (a trial-and-error method of decoding encrypted data such as passwords or encryption keys by trying all possible combinations). Often they used simpler tactics such as calling somebody on the telephone, pretending to be a technician or high-ranking official, and asking for the password. The hackers managed to gain access to dozens of critical Pentagon computer systems. Once they entered the systems, they could easily create user accounts, delete existing accounts, reformat hard drives, scramble stored data, or shut systems down. They broke the network defenses with relative ease and did so without being traced or identified by the authorities. The results shocked the organizers. In the first place, the Red Team had shown that it was possible to break into the U.S. Pacific military's command-and-control system and, potentially, cripple it. In the second place, the NSA officials who examined the experiment's results found that much of the private-sector infrastructure in the United States, such as the telecommunications and electric power grids, could easily be invaded and abused in the same way. The vulnerability of the energy industry is at the heart of Black Ice. Verton argues that America's energy sector would be the first domino to fall in a strategic cyber terrorist attack against the United States. The book explores in frightening detail how the impact of such an attack could rival, or even exceed, the consequences of a more traditional, physical attack. Verton claims that during any given year, an average large utility company in the United States experiences about 1 million cyber intrusions. Data collected by Riptech, Inc.—a Virginia-based company specializing in the security of online information and financial systems—on cyber attacks during the six months following the 9/11 attacks showed that companies in the energy industry suffered intrusions at twice the rate of other industries, with the

number of severe or critical attacks requiring immediate intervention averaging 12.5 per company.[79]

In 1997, a Bolivian terrorist organization had assassinated four U.S. army personnel. A raid on one of the hideouts of the terrorist's yielded information encrypted using symmetric encryption. A 12-hour brute force attack resulted in the decryption of the information and subsequently led to one of the largest drug busts in Bolivian history and the arrest of the terrorists.

In 1999 hackers attacked NATO computers. The computers flooded them with email and hit them with a denial of service (DoS). The hackers were protesting against the NATO bombings in Kosovo. Businesses, public organizations and academic institutions were bombarded with highly politicized emails containing viruses from other European countries.

In 2001, in the back drop of the downturn in US-China relationships, the Chinese hackers released the Code Red virus into the wild. This virus infected millions of computers around the world and then used these computers to launch denial of service attacks on US web sites, prominently the web site of the White House.

In 2002, numerous prominent Indian web sites were defaced. Messages relating to the Kashmir issue were pasted on the home pages of these web sites. The Pakistani Hackerz Club, led by "Doctor Neukar" is believed to be behind this attack.

In May 2007 Estonia was subjected to a mass cyber-attack by hackers inside the Russian Federation which some evidence suggests was coordinated by the Russian government, though Russian officials deny any knowledge of this. This attack was apparently in response to the removal of a Russian World War II war memorial from downtown Estonia.

In December, 2010 the website of the Central Bureau of Investigation (CBI) was hacked by programmers identifying themselves as "Pakistani Cyber Army".

14.11. Summary:

Cyber attacks are one of the greatest threats to international peace and security in the 21st century. Securing cyberspace is an absolute imperative. In an ideal world, states would work together to eliminate the cyber threat. Unfortunately, our world is no utopia, nor is it likely to become one. Global

[79] http://www.usip.org/sites/default/files/sr119.pdf

cooperation may be a reality one day, but unless something changes to pressure sanctuary states into changing their behavior, there is no impetus for them to do so. The way to achieve this reality is to use active defenses against cyber attacks originating from sanctuary states. Not only will this allow victim-states to better protect themselves from cyber attacks, but it should also deter aggression and push sanctuary states into taking their international duty seriously. After all, no state wants another state using force within its borders, even electronically. Thus, the possibility that cyber attacks will be met with a forceful response is the hammer that can drive some sense into sanctuary states. In this unit the important concept of cyber terrorism in global perspective, international legal efforts, suppression of financing to terrorism, UN action to counter terrorism, cyber terrorism viz a viz cyber crime, cyber warfare and cyber terrorism and international case study are discussed at length for better clarity to understand the issues related to cyber terrorism globally.

14.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)

- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

14.13. Check your Progress:

A. Which of the following statements are true or false:

a) Cyber terrorism is premeditated use of disruptive activities.

b) The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature.

c) States were called on to exchange information and cooperate to prevent and suppress terrorist actand to take action.

d) UN resolution No. 1373 (2001) adopted unanimously on 28th September, 2001.

e) Terrorist groups are increasingly computer savvy and some probably are acquiring the ability to use cyber attacks.

B. Fill in the Blanks:

I. UN resolution No……..is related to combat terrorism globally.

II. The ……..distance between the attacker and the victim and the difficulty in tracing back the attack.

III. ……..usually has a stronger meaning than cyber crime.

IV. Terms such …….. and “cyber terrorism” has extensively used in media.

V. It is very difficult to know exactly who is behind the ……..and their exact motive.

14.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1.1371 of 2001
2. Virtual and physical
3. Cyber Terrorism
4. Cyber War
5. Cyber attacks

14.15. Terminal Questions:

1. What is the global definition of the cyber terrorism?
2. Define UN action to counter terrorism.
3. Define cyber terrorism viz a viz cyber crime.
4. What is cyber warfare and cyber terrorism?
5. Discuss any two international case studies.

Unit-15

Cyber Terrorism-Indian Perspective

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Cyber Terrorism in Indian Perspective
- Understand the nature and scope of Important Statutory Provisions
- Understand the technical and legal issues related to Cyber Terrorism with reference to Indian Perspective

Structure:

15.1. Introduction:

The threat posed by cyber terrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry.

Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyber terrorists electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself. And yet, despite all the gloomy predictions of a cyber-generated doomsday, no single instance of real cyber terrorism has been recorded. Just how real is the threat that cyber terrorism poses? Because most critical infrastructure in Western societies is networked through computers, the potential threat from cyber terrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. Terrorists, at least in theory, could thus follow the hackers' lead and then, having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies. The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyber attacks against its infrastructure. Concern about the potential danger posed by cyber terrorism is thus well founded. That does not mean, however, that all the fears that have been voiced in the media, in Congress, and in other public forums are rational and reasonable. Some fears are simply unjustified, while others are highly exaggerated. In addition, the distinction between the potential and the actual damage inflicted by cyber terrorists has too often been ignored, and the relatively benign activities of most hackers have been conflated with the specter of pure cyber terrorism.

15.2. Cyber Terrorism: Meaning and Definition under Indian Law:

Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Computers and the internet are becoming an essential part of our daily life. They are being used by individuals and societies to make their life easier.

They use them for storing information, processing data, sending and receiving messages, communications, controlling machines, typing, editing, designing, drawing, and almost all aspects of life.

The most deadly and destructive consequence of this helplessness is the emergence of the concept of “cyber terrorism”. The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism.

The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace” is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straightjacket formula or pigeons whole. In fact, the first effort of the Courts should be to interpret the definition as liberally as possible so that the menace of cyber terrorism can be tackled stringently and with a punitive hand.

The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world.

Definition of Cyber Terrorism: Before we can discuss the possibilities of “cyber terrorism, we must have some working definitions. The word “cyber terrorism” refers to two elements: cyberspace and terrorism.

Another word for cyberspace is the “virtual world” i.e. a place in which computer programs function and data moves.[5] Terrorism is a much used term, with many definitions. For the purposes of this presentation, we will use the United States Department of State definition:” The term ‘terrorism’ means premeditated,

politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents."

If we combine these definitions, we construct a working definition such as the following: "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

The basic definition of Cyber-terrorism subsumed over time to encompass such things as simply defacing a web site or server, or attacking non-critical systems, resulting in the term becoming less useful. There is also a train of thought that says cyber terrorism does not exist and is really a matter of hacking or information warfare. Some disagree with labeling it terrorism proper because of the unlikelihood of the creation of fear of significant physical harm or death in a population using electronic means, considering current attack and protective technologies.

Cyber Terrorism and IT Act, 2000:

Amendments under the Information Technology Act, 2000 has defined the term "Cyber terrorism" U/Sec. 66F. This is the first ever attempt in India to define the term. It reads as under:-

Punishment for Cyber terrorism: Whoever:

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant;

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct

obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Punishment: Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life. I.e. Imprisonment not exceeding fourteen years (Sec. 55, IPC)

This Section has defined conventional Cyber attacks like, unauthorised access, denial of service attack, etc, but as discussed above, motive and intention of the perpetrator differentiates the attack from an ordinary to an act of terrorism.

Illustration: Rohit, a Hacker, gains unauthorised access into Railway traffic control grid (the grid has been declared as Critical Information Infrastructure U/Sec. 70) and thereby strikes terror amongst people, Rohit is said to have done an act of Cyber terrorism.

15.3. Cyber Terrorism and Indian Penal Code, 1860:

Indian websites are new target of hackers: Some computer experts managed to break into the high security computer network of Bhabha Atomic Research Center but were luckily detected. "GForce," a group of anonymous hackers whose members write slogans critical of India and its claim over Kashmir, have owned up to several instances of hacking of Indian sites run by the Indian government, private companies or scientific organizations. The NAASCOM chief said Indian companies on an average spent only 0.8 percent of their technology budgets on security, against a global average of 5.5 percent.

A number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them, CBI Director, R K Ragavan said. As the hackers who broke into computer systems in India were not conniving with the Pakistani law enforcers, "One wonders what kind of cooperation we will get" Mr.

Ragavan said at a seminar on Internet security. Hackers using knowledge of software to break in and steal information from computer systems broke into at least 635 Indian internet sites last year. Mr. Raghavan said the rise of literacy in India could bring down conventional crimes but the vulnerability of computers and the Internet could make crimes over the medium more rampant.

"We at the CBI are convinced that cyber crime is the crime of the future," he said. "It is now much more easily committed and less easily identified."President of India's National Association of Software and Service Companies (NASSCOM), Dewang Mehta said the lack of uniform laws against cyber crimes involving abuse of computer systems made prosecution of cross-border hackers difficult. "Hacking is not a universal offence, and there is a problem," Mr. Mehta said.

Last year, India passed a landmark digital law that makes hacking, spreading of viruses and illegal financial transactions over the Internet punishable. It became the 12th member in a small club of nations with digital laws.

It was reported that Pakistan was making use of the computer system to promote terrorism in India.These are just some of the instances which were cited by Bhure Lal, secretary in the Central Vigilance Commission, to make a strong case for implementation of cyber laws. He was addressing the national seminar on Computer-related Crimes organized by the Central Bureau of Investigation (CBI) in the Capital today. Underlining the need for a comprehensive cyber law, he added that computer abuse can also be resorted to for cyber-terrorism.

In order to evolve effective safeguards against the menace of computer crimes, other experts various investigative agencies, including the Federal Bureau of Investigation (FBI) and Interpol, today sought specific and comprehensive cyber laws to cover all acts of computer criminals and proactive mechanisms for tackling such offences.

``It is not only difficult to detect computer crimes but also to book criminals since the laws have not kept pace with technology," Reserve Bank of India Deputy Governor S.P. Talwar said.

Stressing the need for effective security features while undertaking computerization, he said ``It is often difficult to attribute guilt using the existing statutes since the act of trespassing into a system and tampering with virtual data

may not necessarily be specifically provided for in law."
In his address, CBI Director (Former) R.K. Raghavan said the government is aware of the need for legislation in this new area of information technology and accordingly, the Department of Electronics (DoE) in consultation with other expert agencies has already drafted laws relating to this area. Realizing the threat from computer crimes, the CBI has taken a ``proactive'' lead in preparing itself to face the challenge by setting up a special Cyber Crime Unit, he said.

The RBI was also associated with the efforts of the ministries of Finance, Commerce and Law in the enactment of laws such as the Information Technology Act and the Cyber Law, Talwar said.

At the same time, he added that unless development of security features were alsoatteneded to at the same level of efficiency and equal speed, banks would be left with ``beautiful software systems for public glare and access, but totally unguarded and gullible against waiting information poachers''.

Offensive SMS can lead to 2 years in jail

With mobile phones and prepaid cell phones virtually taking over the role of a personal computer, the proposed amendments to the Information Technology Act, 2006, have made it clear that transmission of any text, audio or video that is offensive or has a menacing character can land a cellphone user in jail for two years. The punishment will also be attracted if the content is false and has been transmitted for the purpose of causing annoyance, inconvenience, danger or insult.
And if the cellphone is used to cheat someone through personation, the miscreant can be punished with an imprisonment for five years.
The need to define communication device under the proposed amendments became imperative as the current law is quiet on what kind of devices can be included under this category. The amended IT Act has clarified that a cellphone or a personal digital assistance can be termed as a communication device and action can be initiated accordingly. Accentuated by various scandals that hit the country during the past two years, including the arrest of the CEO of a well-known portal, the government has also introduced new cyber crimes under the proposed law. The amended Act, which was placed before the Lok Sabha during the recently concluded winter session, has excluded the liability of a network service provider with regard to a third party’s action. However, it has made cyber stalking, cyber defamation and cyber nuisance an offence. Anybody found indulging in all these

offences can be imprisoned for two years. The proposed changes have also sought amendments in the form of insertions in the Indian Penal Code, thereby declaring identity theft an offence. If a person cheats by using electronic signature, password or any other unique identification feature of any other person, he shall be punished with imprisonment for two years and also liable to fine.

Asking for an insertion in the Indian Penal Code as Section 502A of the law, the proposed amendments have said that whoever intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, shall be punished with two years of imprisonment and fine of Rs 2 lakh. The private parts can be either naked or undergarment clad public areas. Making the law more technologically neutral, the amended provisions have included authentication of electronic record by any electronic technique. At the moment, electronic records can be authenticated by just digital signatures, the public key infrastructure technology (PKI). With the new provisions, however, biometric factors like thumb impression or retina of an eye shall be included as techniques for authentication. Even as the law makers have tried to cover up for the lapses of the current IT Act, they seem to have made it liberal by way of reducing the punishment from three years to two years. With these changes, a cyber criminal will now be entitled to bail as a matter of right, as and when he gets arrested.

15.4. Cyber Terrorism in India and its Solution:

The menace of cyber terrorism is not the sole responsibility of State and its instrumentalities. The citizens as well as the netizens are equally under a solemn obligation to fight against the cyber terrorism. In fact, they are the most important and effective cyber terrorism eradication and elimination mechanism. The only requirement is to encourage them to come forward for the support of fighting against cyber terrorism. The government can give suitable incentives to them in the form of monetary awards. It must, however, be noted that their anonymity and security must be ensured before seeking their help. The courts are also empowered to maintain their anonymity if they provide any information and evidence to fight against cyber terrorism. The problem of cyber terrorism is multilateral having varied facets and dimensions. Its solution requires rigorous application of energy and resources. It must be noted that law is always seven steps behind the

technology. This is so because we have a tendency to make laws when the problem reaches at its zenith. We do not appreciate the need of the hour till the problem takes a precarious dimension. At that stage it is always very difficult, if not impossible, to deal with that problem. This is more so in case of offences and violations involving information technology. A timely and appropriate legislation is always a good step forward to fight cyber terrorism. India has to cover a long gap before it can secure its traditional boundaries and cyber space.[80]

15.5. Case Study-I:

Cyber laws need to keep pace with technological changes, focusing on mobile internet and social media misuse to redefine cyber terror, war or naxalism:

The arrest of Mehdi Masoor Biswas, the man behind the Twitter handle @ShamiWitness, as the "IS tweeter" and "suspected jihadi" places questions about whether tweeting constitutes an act of terror before an Indian court of law. When it comes to that, it will not be about "police claims" or "intelligence sources", but about hard facts, evidence and the letter of the law to answer how "complicit to terror" the tweeter and his tweets were.

One of the police officers who interrogated Mehdi admitted that this is a "test case" because it's the first time that they actually have "no real world connect yet" and "only a Twitter account" to prove involvement in a terror case. For instance, Mehdi, despite his "open ideological support" is not an "enrolled or registered member of the IS", neither is there any evidence to prove that "he was taking directions or was involved in any other real world activity for the IS". He was a "lone ranger" and pretty much operated on his own and so far there is no evidence to prove that his involvement was beyond his tweets, he added. But then, there are thousands of "lone rangers" in the cyber world claiming to represent hundreds of "rabid and terrorist" ideologies and hence the question – how much of evidence can tweets alone be in a case of this nature?

A Mumbai-based lawyer specializing in cyber laws, Pawan Duggal, says that this case is not just about tweets and terrorism, but about Indian cyber laws and their ability to deal with such incidents. "Under the language of Section 66 F of the Information Technology Act a mere tweet alone does not fulfil the parameters of

[80]http://ptlbindia.blogspot.in/2009/11/cyber-terrorism-in-india-and-its.html

cyber terrorism" and this only shows "the need to revisit the law to define and bring into focus the use of social media for cyber terrorism," he argued. Mr. Duggal added that "the law was amended in 2008 and since then much has changed in terms of technology and this only shows that cyber laws need to keep pace with quick technological changes" and that there is an "urgent need to focus on mobile internet and social media misuse to redefine cyber terror, war or naxalism."

However, in the present backdrop, the key in front of investigators is to prove a "real world link". Investigators say that at the least, they can charge Mehdi for being a 'propagandist' for the IS, furthering their cause to wage a war against the regimes in Syria and Iraq. "We have evidence, some even through public tweets by IS fighters that he was a radicalizing agent and a motivator, which is abetting the crime," said an official. The police are also banking on the 14,000 plus private direct messages on Twitter to prove that he incited men to fight for the IS, which they claim is enough to charge him under Section 39 of UAPA, 2004 and Section 125 of IPC for supporting a terror outfit and abetting to wage a war against a friendly Asian ally. While the IS itself was not declared a "banned outfit" under Indian law at the time of Mehdi's arrest, investigators argue that it was declared a "terrorist outfit" by the United Nations and had carried out "extreme acts of terror." It automatically meant that support to it can be construed as an "act of terror" under the UAPA, they argued.

However, Bengaluru-based lawyer Jaffer Shah, who will represent Mehdi in the case, said that this case raised a "fundamental question" on whether expression of "opinion and ideological support and re tweeting or tweeting information" can be considered a case of waging a war against a friendly Asiatic ally, constituting cyber terrorism under the IT Act. Mr. Shah further argued that the case would determine "where we then draw the distinction between thousands of hate or war mongering tweets that are put out and an act of terror". "The police seem to have declared that expressions of ideological support and opinion in favour of the IS were acts of terror, our defence is to question that premise," he added.

In this context, several Supreme Court judgements are cited by legal experts, including the 2007 order in the Arup Bhuyan vs. State of Assam case, in which a two- judge bench ruled that even "mere membership of a banned organisation will not make a person a criminal unless he resorts to violence or incites people to

violence or creates public disorder by violence or incitement to violence." Noted human rights lawyer Anand Grover said: "Unless there is direct involvement in an act it is difficult to prove these cases" and they fall in a "grey area."

By Mehdi's own admission to interrogators, he had "no interest in creating a movement on Indian soil" and the case against him is in the context of a "friendly Asiatic ally." Mr. Grover points out that such cases are an "open question determined by a political context" on what constitutes an "act of terrorism" and what does not.

By any yardstick, this is a complex case that has emerged around a man, who through several thousand tweets, had declared and expressed support for a violent "terrorist" movement. While the evidence against Mehdi would be the key for investigators, the case itself could have much larger ramifications on defining use or abuse of the social media; it could redefine just how far a tweet can go in a "war against any nation"![81]

15.6. Case Study-II:

India must wake up to cyber-terrorism' (Haris Zargar, Indo-Asian News Service, April 02, 2013): In early March, suspected Chinese hackers breached the computers of India's top military organisation, the Defence Research and Development Organisation (DRDO), in what was touted to be amongst the biggest such security breaches in the country's history. Former Defence Minister A.K. Antony ordered a probe into the matter, though an official statement denied any sensitive file had been compromised. India has seen many such attacks on its critical installations and the misuse of social media and Internet has brought home the threat of cyber-terrorism, which cyber security experts say the country is poorly equipped to handle. Experts believe the country is vulnerable to such cyber-terrorism attacks with some countries and vested interest groups bent on espionage and destruction.

According to Supreme Court lawyer and leading cyber law expert Pavan Duggal, while the threat of cyber attacks remains "imminent", the country lacks an institutionalized mechanism of a cyber army to deal with the threat. "The recent DRDO breach was a classical case of cyber war attack rather than mere hacking. It was an attack on India's critical information infrastructure. Cyber warfare as a phenomenon is not covered under the

[81] http://www.thehindu.com/sunday-anchor/terror-on-twitter-the-life-and-crimes-of-mehdi/article6731135.ece

Indian cyber law. Clearly, the country's cyber security is not in sync with the requirements of the times," Duggal told IANS.

Over the past few years, India has witnessed a growing number of cyber assaults, with government departments, particularly defence establishments, coming under attack. Last year, hacker group 'Anonymous' carried out a series of Distributed Denial of Service (DDoS) attacks against a number of government websites, in retaliation against the alleged Internet censorship. Hackers from Algeria also carried out an attack on websites run by the DRDO, the Prime Minister's Office and various other government departments last year. A group called 'Pakistan Cyber Army' had also hacked into several Indian websites. "The threat landscape remains very threatening," said cyber law and cyber security expert Prashant Mali. "India is awakening to the global threat of cyber warfare now. Our cyber security is still ineffective as mass awakening towards it is missing or inadequate. Even though NTRO and DRDO are mandated with cyber offensive work, only time will show effectiveness of these organisations," Mali told IANS.

Usually, cyber attacks follow the same modus operandi. An email is sent to an individual or small group, within an organisation. Efforts are made to make the email look legitimate, that is, it will appear as though it was sent by somebody the recipient trusts and the content of the mail will often be related to the recipient's area of interest. In order to install the malware, the user is tricked into either clicking a malicious link or launching a malicious attachment. In the more sophisticated attacks, the attacker will use a new "zero day vulnerability", in which attackers send email attachments which when opened, exploit vulnerabilities in the Web browsers.

According to CERT-In (the Indian Computer Emergency Response Team), which is a government-mandated information technology security organization; an estimated 14,392 websites in the country were hacked in 2012 (till October). In 2011, as many as 14,232 were hacked, while the number of websites hacked in 2009 stood at 9,180. About 16,126 websites were hacked in 2010. With cyber security impacting the country's security, Shivshankar Menon, the national security adviser, announced last month that the government is putting in place a national cyber security architecture to prevent sabotage, espionage and other forms of cyber threats.

"The past few years have witnessed a dramatic shift in the threat landscape. The motivation of attackers has moved from fame to financial gain and malware has become a successful criminal business model with billions of dollars in play. We have now entered a third significant shift in the threat landscape, one of cyber-espionage and cyber-sabotage,"

Shantanu Ghosh, vice president at India Product Operations-Symantec corporation, which developed Norton AntiVirus, told IANS. Ghosh said cyber security questions are no longer an exotic topic focussing primarily on spam messages and personal computers but have started to impact on the national security and defence capability of a country. Rikshit Tandon, consultant at Internet and Mobile Association of India (IAMAI) and advisor to the Cyber Crime Unit of the Uttar Pradesh Police, said: "Cyber terrorism is a grave threat not only to India but to the world." "It can come to any country and, yes, proactive measures by government and consortium of countries needs to be taken as a collective effort and policy since internet has no geographical boundaries," Tandon told IANS. Experts say the country spends a small amount of money on cyber security. The budget allocation towards cyber security was Rs.42.2 crore ($7.76 million) for 2012-13, as against Rs.35.45 crore in 2010-11. In comparison, the US spends several billion dollars through the National Security Agency, $658 million through the Department of Homeland Security and $93 million through US-CERT in 2013.

15.7. Case Study-III:

Ahmadabad Blast Case Study:

Ahmadabad is the cultural and commercial heart of Gujarat state, and one of the largest cities of India. On July 26, 2008, a series of 21 bomb blasts hit Ahmedabad within a span of 70 minutes. 56 people were killed and over 200 people were injured. Several TV channels stated that they had received an e-mail from a terror outfit called Indian Mujahidin claiming responsibility for the terror attacks.

First Mail was sent on 26th July, 2008 from Email Id “alarbi_gujarat@yahoo.com” from IP Address. 210.211.133.200 which traced to Kenneth Haywood’s House at Navi Bombay. His Unsecured WIFI router was misused by terrorists to send terror mail from his router. As log system is disabled, Police were unable to find out the details of the MAC address of the culprit.

Second Mail was sent on 31st July, 2008 from “alarbi_gujarat@yahoo.com” from IP Address: 202.160.162.179 which traced out to Medical College at Vaghodiya, Baroda, Gujarat. It was little bit difficult to trace this mail as the mail has been sent using proxy server & fake mail script but finally Police with the help of Cyber experts traced out the original IP address.

Third Mail was sent on 23rd August, 2008 from "alarbi.alhindi@gmail.com" from IP address: 121.243.206.151 which traced to Khalsa College at Bombay. Again Unsecured WIFI router was misused to send an email.

Forth Mail was sent on 13th September, 2008 from "al_arbi_delhi@yahoo.com" which traced to Kamran Power Limited at Bombay. In this case also WIFI router was misused to send the threatening mail.[82]

15.8. Case Study-IV:

26/11 Attack Case Study:

Mumbai is the capital state of Maharashtra state and largest city in India. Attack was made on 26 November 2008 and lasted until 29 November. Attacks consist of more than ten coordinated shooting and bombings.

An FBI witness had investigated that terrorists were in touch with their handlers in Pakistan through Callphonex using VOIP.

Wanted accused in the 26/11 attack case had communicated with terrorists using an email ID which was accessed from ten IP addresses –

Five from Pakistan, two USA, two Russia and one Kuwait.

Kharak_telco@yahoo.com was the email ID used by wanted accused while communicating with terrorists via Voice over Internet Protocol (VoIP) through New Jersey-based Callphonex. According to the owner of "Callphonex", on October 20, he had received a mail from name "Kharak Singh", expressing desire to open an account with Callphonex. Accused has used following services of Callphonex:-

- 15 calls from computer to phone,
- 10 calls to common client accounts and
- Direct inward dialing

They have accessed the email ID from ten IP addresses of which, five belonged to Pakistan. One of the addresses (118.107.140.138) was traced to Col R Sadat Ullah of Special Communication Organisation, Qasim Road, Rawalpindi, Pakistan. Three addresses were traced to World Call network Operations and the fifth came from Sajid Iftikar, EFU House, Jail Road in Pakistan. Other five IP addresses, from

[82] http://www.lawyersclubindia.com/articles/Cyberterrorism-in-India-With-special-emphasis-on-Ahmadabad--2059.asp#.VKexZNKUdZ0

where the email address "kharak_telco@yahoo.com" was accessed, were traced to FDC Servers.net in Chicago (USA), Ahemed Mekky in Kuwait and Vladimir N Zernov at Joint Stock Company, Moscow.[83]

15.9. Case Study-V:

2008: Year of cyber terrorism[84]: (By Pavan Duggal Jan 08 2009):

The year 2008 was also one in which various cyber crimes occupied centrestage. Various instances of identity theft and phishing were reported, though under-reported figures far outstripped the reported instances. Amid all this, Indian cyber law continued to appear toothless. Meanwhile, as internet 2.0 became more prominent in India, social networking cyber crimes, including misuse of personal information posted on such sites was reported frequently. The misuse of personal information by tampering and amending the same, has grown tremendously. The year was also the year of cyber terrorism. Whether it was Bangalore or Delhi, the bomb blasts were preceded by e-mails announcing the impending acts. It was the year when cyber terrorists became far more adventurous. The inability of the law enforcement agencies to nab cyber criminals and take effective action exposed the inadequacies of our laws. Cyber terrorism once again came to the fore in India in the form of the Mumbai attacks. The terrorists were extremely technology savvy, and were using satellite phones with impunity.It was the year, when pushed by the Mumbai attacks, the government swung into action and got the amendments to the Information Technology Act, 2000 passed in both the houses of Parliament. Clearly, the factum of the passage of the Information Technology Amendment Act, 2008 in both the houses without discussion, demonstrates the truth of the dictum that history repeats itself.

In 2000, the IT Act was passed without any discussion in both the houses of Parliament. The same was repeated in India in December 2008. As a result, rather than dealing with cyber terrorism in a comprehensive manner, the IT Act amendments have only got one provision on cyber terrorism. There appears to be no sign of any lessons learnt from the Mumbai attacks. These amendments are now

[83] http://www.lawyersclubindia.com/articles/Cyberterrorism-in-India-With-special-emphasis-on-Ahmadabad--2059.asp#.VKexZNKUdZ0

[84] http://www.mydigitalfc.com/opinion/2008-year-cyber-terrorism-270

waiting for the President's assent. It was also the year in which network service providers started feeling the heat of the process of law. Various litigations were filed insisting upon them to disclose third party information rendered and made available in their computer systems. A network service provider got a taste of the result of giving wrong subscriber information to the law enforcers.

The year brought home the truth that if network service providers are negligent about giving correct subscriber information to the law enforcement agencies, they need to face potential legal consequences, both civil and criminal. This is all the more so, as under the IT Act, 2000, these providers are made liable for all third party data and information made available by them. However, they can exit from their liability, provided they are able to prove two conditions. The first condition is that the network service provider has to prove that he had no knowledge of any contravention of law. The second condition is that the provider has to prove that despite due diligence, it could not prevent the commission of an offence or contravention of law. In 2008, India organised big international events pertaining to IT and internet. In February 2008, the Delhi meeting of the Internet Corporation For Assigned Names And Numbers (Icann) was held. Towards the end of December 2008, the government organised the Internet Governance Forum in Hyderabad. The forum is of tremendous significance in terms of giving a common platform to all stakeholders of the internet to discuss issues pertaining to internet law and policy. It was also a landmark year for judgements given under the Information Technology Act. 2000. In February 2008, L Prakash, an orthopedic surgeon, was sentenced to life on the charges of online obscenity. In May, the Delhi High Court gave a landmark judgment in the Baazee.com case. The CEO of the portal was arrested in 2004 for hosting a message relating to the DPS MMS on its website. In this case, the government levied criminal charges and filed a charge sheet. This was challenged before the Delhi High Court, which declined to quash the cyber criminal charges of online obscenity and directed the accused to face criminal trial. The matter is now pending in the Supreme Court. The common result of this judgment is that principles of law for electronic information, as enshrined in the Act, have been upheld. The year 2008 was an adventurous year as far as cyber law jurisprudence in India is concerned. The cyber legal developments that took place will provide the foundation for subsequent growth and development

of Indian cyber law jurisprudence in 2009. It will be interesting to see how this year deals with the challenges pertaining to the internet, cyber space and the world wide web.

15.10. Summary:

The concept of cyber terrorism in Indian perspective is also very important aspect. In this unit the various important concept of cyber terrorism-meaning and definition in Indian perspective under Indian law, cyber terrorism under the Information Technology Act, 2000, cyber terrorism and Indian Penal Code, 1860, cyber terrorism in India and its solution in present situation and case studies are discussed to understand in the interest of students.

15.11. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)

- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

15.12. Check your Progress:

A. Which of the following statements are true or false:

a) The threat posed by cyber terrorism has grabbed the attention of the mass media, the security community and the IT industry.

b) The expression “cyber terrorism” includes an intentional negative and harmful use of the information technology.

c) The law dealing with cyber terrorism is however, not adequate to meet the precarious intention of these cyber terrorist.

d) Cyber terrorism includes attempting to penetrate or access a computer resource without authorisation.

e) The NASSCOM chief said Indian companies on an average spent only 0.8 percent of their technology budgets on security, against a global average of 5.5%.

B. Fill in the Blanks:

I. ……of the Information Technology Act, 2000 is related to cyber terrorism.

II. The section defines…….like, unauthorised access, denial o service attack etc.

III. The menace of cyber terrorism is not the sole responsibility of ……

IV. A……legislation is always a good step forward to fight cyber terrorism.

V. Whoever commits or compromises to commit cyber terrorism shall be punishable with imprisonment which…….

15.13. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Section 66F
2. Conventional cyber attacks
3. States and its instrumentalities
4. Timely and appropriate
5. May extend to imprisonment for life

15.14. Terminal Questions:

1. What is meaning and definition of cyber terrorism in Indian perspective?
2. Discuss cyber terrorism under IT Act, 2000.
3. Discuss cyber terrorism and Indian Penal Code, 1860.

4. Discuss Case Study-I and II.
5. Discuss case study-III and IV.

Unit-16

Cyber Terrorism and Human Rights

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters related to Cyber Terrorism and Human Rights
- Understand the importance of Human Rights with reference to Cyber Terrorism
- Understand the technical and legal issues related to Cyber Terrorism with reference to Cyber Terrorism

Structure:

16.1. Introduction:

The issue of terrorism and human rights has long been a concern of the United Nations. Following the terrorist attacks of 11 September 2001and

subsequent surge in acts of terrorism worldwide, it has become even more urgent. While condemning terrorism unequivocally and recognizing the duty of States to protect those living within their jurisdictions from terrorism, the United Nations has placed a priority on the question of protecting human rights in the context of counter-terrorism measures. The defense of human rights and upholding the rule of law while countering terrorism is indeed at the heart of the United Nations Global Counter-Terrorism Strategy. Member States acknowledged that effective counter-terrorism measures and the protection of human rights were not conflicting goals but complementary and mutually reinforcing aims. They pledged to take measures aimed at addressing violations of human rights and to ensure that any measures taken to counter terrorism comply with their human rights obligations.

A concrete endorsement by Member States of the need to make the protection of human rights an integral part of the international fight against terrorism was demonstrated by the creation in 2005 of a post of Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. The Special Rapporteur, operating under the new Human Rights Council, works to identify, exchange and promote best practices on measures to counter terrorism that respect human rights and fundamental freedoms. The Special Rapporteur also addresses allegations of human rights violations in the course of countering terrorism. He conducts visits to selected individual countries and has engaged in correspondence with more than 40 countries about their laws and practices. He reports regularly both to the Human Rights Council and to the General Assembly, including on selected thematic issues and his country visits.

16.2. International Conventions on Terrorism-I:

Summary of the 14 major legal instruments and additional amendments dealing with terrorism:

1. 1963 Convention on Offences and Certain Other Acts Committed On Board Aircraft (Aircraft Convention):
    - Applies to acts affecting in-flight safety;

- Authorizes the aircraft commander to impose reasonable measures, including restraint, on any person he or she has reason to believe has committed or is about to commit such an act, where necessary to protect the safety of the aircraft; and
- Requires contracting States to take custody of offenders and to return control of the aircraft to the lawful commander.

2. 1970 Convention for the Suppression of Unlawful Seizure of Aircraft (Unlawful Seizure Convention):
   - Makes it an offence for any person on board an aircraft in flight to "unlawfully, by force or threat thereof, or any other form of intimidation, [to] seize or exercise control of that aircraft" or to attempt to do so;
   - Requires parties to the convention to make hijackings punishable by "severe penalties"
   - Requires parties that have custody of offenders to either extradite the offender or submit the case for prosecution; and
   - Requires parties to assist each other in connection with criminal proceedings brought under the Convention.
   - 2010 Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft
   - Supplements the Convention for the Suppression of Unlawful Seizure of Aircraft by expanding its scope to cover different forms of aircraft hijackings, including through modern technological means;
   - Incorporates the provisions of Beijing Convention relating to a threat or conspiracy to commit an offence.
3. 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Civil Aviation Convention):
   - Makes it an offence for any person unlawfully and intentionally to perform an act of violence against a person on board an aircraft in flight, if that act is likely to endanger the safety of the aircraft; to place an explosive device on an aircraft; to attempt such acts; or to be an accomplice of a person who performs or attempts to perform such acts;

- Requires parties to the Convention to make offences punishable by "severe penalties"; and
- Requires parties that have custody of offenders to either extradite the offender or submit the case for prosecution.

4. 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons (Diplomatic Agents Convention):
   - Defines an "internationally protected person" as a Head of State, Minister for Foreign Affairs, representative or official of a State or international organization who is entitled to special protection in a foreign State, and his/her family; and
   - Requires parties to criminalize and make punishable "by appropriate penalties which take into account their grave nature" the intentional murder, kidnapping or other attack upon the person or liberty of an internationally protected person, a violent attack upon the official premises, the private accommodations, or the means of transport of such person; a threat or attempt to commit such an attack; and an act "constituting participation as an accomplice".
5. 1979 International Convention against the Taking of Hostages (Hostages Convention):
   - Provides that "any person who seizes or detains and threatens to kill, to injure, or to continue to detain another person in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage commits the offence of taking of hostage within the meaning of this Convention".
6. 1980 Convention on the Physical Protection of Nuclear Material (Nuclear Materials Convention):
   - Criminalizes the unlawful possession, use, transfer or theft of nuclear material and threats to use nuclear material to cause death, serious injury or substantial property damage.

- Amendments to the Convention on the Physical Protection of Nuclear Material
- Makes it legally binding for States Parties to protect nuclear facilities and material in peaceful domestic use, storage as well as transport; and
- Provides for expanded cooperation between and among States regarding rapid measures to locate and recover stolen or smuggled nuclear material, mitigate any radiological consequences or sabotage, and prevent and combat related offences.

7. 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Extends and supplements the Montreal Convention on Air Safety) (Airport Protocol):
   - Extends the provisions of the Montreal Convention to encompass terrorist acts at airports serving international civil aviation.

16.3. International Conventions on Terrorism-II:

8. 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention):

- Establishes a legal regime applicable to acts against international maritime navigation that is similar to the regimes established for international aviation; and
- Makes it an offence for a person unlawfully and intentionally to seize or exercise control over a ship by force, threat, or intimidation; to perform an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of the ship; to place a destructive device or substance aboard a ship; and other acts against the safety of ships.
- 2005 Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
- Criminalizes the use of a ship as a device to further an act of terrorism;

- Criminalizes the transport on board a ship various materials knowing that they are intended to be used to cause, or in a threat to cause, death or serious injury or damage to further an act of terrorism;
- Criminalizes the transporting on board a ship of persons who have committed an act of terrorism; and
- Introduces procedures for governing the boarding of a ship believed to have committed an offence under the Convention.

9. 1988 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (Fixed Platform Protocol):

- Establishes a legal regime applicable to acts against fixed platforms on the continental shelf that is similar to the regimes established against international aviation.
- 2005 Protocol to the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf
- Adapts the changes to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation to the context of fixed platforms located on the continental shelf.

10. 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention):

- Designed to control and limit the use of unmarked and undetectable plastic explosives (negotiated in the aftermath of the 1988 Pan Am flight 103 bombing);
- parties are obligated in their respective territories to ensure effective control over "unmarked" plastic explosive, i.e., those that do not contain one of the detection agents described in the Technical Annex to the treaty;
- Generally speaking, each party must, inter alia, take necessary and effective measures to prohibit and prevent the manufacture of unmarked plastic explosives; prevent the movement of unmarked plastic explosives into or out of its territory; exercise strict and effective control over possession and transfer of unmarked explosives made or imported prior to

the entry into force of the Convention; ensure that all stocks of unmarked explosives not held by the military or police are destroyed, consumed, marked, or rendered permanently ineffective within three years; take necessary measures to ensure that unmarked plastic explosives held by the military or police are destroyed, consumed, marked or rendered permanently ineffective within fifteen years; and, ensure the destruction, as soon as possible, of any unmarked explosives manufactured after the date of entry into force of the Convention for that State.

11. 1997 International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention):

- Creates a regime of universal jurisdiction over the unlawful and intentional use of explosives and other lethal devices in, into, or against various defined public places with intent to kill or cause serious bodily injury, or with intent to cause extensive destruction of the public place.

12. 1999 International Convention for the Suppression of the Financing of Terrorism (Terrorist Financing Convention):

- Requires parties to take steps to prevent and counteract the financing of terrorists, whether direct or indirect, through groups claiming to have charitable, social or cultural goals or which also engage in illicit activities such as drug trafficking or gun running;
- Commits States to hold those who finance terrorism criminally, civilly or administratively liable for such acts; and
- Provides for the identification, freezing and seizure of funds allocated for terrorist activities, as well as for the sharing of the forfeited funds with other States on a case-by-case basis. Bank secrecy is no longer adequate justification for refusing to cooperate.

13. 2005 International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Terrorism Convention):

- Covers a broad range of acts and possible targets, including nuclear power plants and nuclear reactors;
- Covers threats and attempts to commit such crimes or to participate in them, as an accomplice;

- Stipulates that offenders shall be either extradited or prosecuted;
- Encourages States to cooperate in preventing terrorist attacks by sharing information and assisting each other in connection with criminal investigations and extradition proceedings; and
- Deals with both crisis situations (assisting States to solve the situation) and post-crisis situations (rendering nuclear material safe through the International Atomic Energy Agency (IAEA).

14. 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (New civil aviation convention):
    - Criminalizes the act of using civil aircraft as a weapon to cause death, injury or damage;
    - Criminalizes the act of using civil aircraft to discharge biological, chemical and nuclear (BCN) weapons or similar substances to cause death, injury or damage, or the act of using such substances to attack civil aircraft;
    - Criminalizes the act of unlawful transport of BCN weapons or certain related material;
    - A cyber attack on air navigation facilities constitutes an offence;
    - A threat to commit an offence may be an offence by itself, if the threat is credible.
    - Conspiracy to commit an offence, or its equivalence, is punishable.

16.4. Cyber Terrorism and Right to Privacy:

The law of privacy is the recognition of the individual's right to be let alone and to have his personal space inviolate. The right to privacy as an independent and distinctive concept originated in the field of Tort law. In recent times, however, this right has acquired a constitutional status [Rajagopal Vs State of TN [(1994) 6 SCC 632], the violation of which attracts both civil as well as criminal consequences under the respective laws. Modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Right to privacy is a part of the right to life and personal liberty enshrined under Article 21 of the Constitution

of India. With the advent of information technology the traditional concept of right to privacy has taken new dimensions, which require a different legal outlook. To meet this challenge recourse of Information Technology Act, 2000 can be taken. The various provisions of the Act protect the online privacy rights of the net users. These rights are available against private individuals as well as against cyber terrorists. Section 1 (2) read with Section 75 of the Act provides for an extra-territorial application of the provisions of the Act. Thus, if a person (including a foreign national) contravenes the privacy of an individual by means of computer, computer system or computer network located in India, he would be liable under the provisions of the Act. This makes it clear that the long arm jurisdiction is equally available against a cyber terrorist, whose act has resulted in the damage of the property, whether tangible or intangible.[85]

16.5. Human Rights and Universal Declaration of Human Rights:

Universal Declaration of Human Rights in its Preamble talks about a "freedom from fear and want". Freedom from fear is mostly a term of psychological nature, however, it is being used very widely nowadays especially in cases of terrorism. Article 3 of the Declaration sets the right to "security of person". As we know, term "person" also includes an environment (s)he exists in, different from the term "individual" which under one of the concepts imagines it as something abstract, apart from any other surrounding conditions. So protecting a personal security would also mean protecting his (her) social, economical and other connections, "threads" established with the environment. As long as in modern reality these are sometimes predominantly based on technology, computers or internet, cyber-terrorism protection also deals with "security of person".

Article 5 with its protection against "degrading treatment". Personal harm is also a part of degradation and treating a person in a current way is something that may be provided by cyber-criminal act as it was proven above. One important provision that is Article 12 of the Declaration. It states: "No one shall be

[85] http://www.legalserviceindia.com/article/l349-Cyber-Terrorism-&-Various-Legal-Compliances.html

subjected to arbitrary interference with his privacy, nor to attacks upon his honour or reputation". "Privacy" is defined as "the quality or state of being apart from company or observation" which in combination with another definition of "freedom from unauthorized intrusion" given by the same source, also includes the privacy of computer-stored data and a right to enjoy it's private state of non-interference without personal will of the possessor.

Article 17 sets a right to property and a restriction to deprive anyone from possessed property. Property is defined as "anything that is owned by a person or entity" , including two types of it: "real property" and "personal property". Personal property or "personality" includes "movable assets which are not real property, money, or investments.

Article 19, however, plays a different role in this topic and is mostly associated with internet use by terrorists in general.[86]

16.6. Human Rights, United Nations and Cyber World:

Human Rights Protection in Cyberspace is urgently needed at National and International level. The call is for the United Nations to take that is "Slow" in this regard. No time in the history of Internet and Cyberspace the need for Protection of Human Rights in Cyberspace is more than the present times.
If the United Nations believes in Human Rights, it must start thinking towards its new form in this Internet Era. There is no reason why Human Rights in Cyberspace must be given any lesser importance than its traditional Human Rights. After all Human Rights like Right to Speech and Expression, Right to Information, Right to Know, Privacy Rights, etc are similar in Cyberspace. Rather violation of Human Rights in Cyberspace is much easier and more frequent. What is most surprising is why UN has still not considered Cyberspace as an essential part of human life. If we analyse the trends World over, technology has been increasingly used to violate Human Rights in Cyberspace. Thus, UN must urgently protect Human Rights in Cyberspace.
Even the World community on Human Rights, Cyber Law and Cyber Security must start thinking in this direction as issues like Cyber Warfare, Cyber Terrorism, Cyber Espionage, Cyber Crimes, E-Surveillance, Unlawful

[86] http://www.legalserviceindia.com/article/l349-Cyber-Terrorism-&-Various-Legal-Compliances.html

Interceptions, etc are "Transnational" in nature. If different Countries would have different laws for these issues, it would be very difficult to truly enforce protective provisions against these menaces at National and International levels. This is the reason why we must a "Harmonised Legal Framework" in this regard, preferably under the regime of United Nation's Human Rights Organisation. The Governments all over the World are engaging in illegal and unlawful phone tapping and interceptions. This is violating various Human Rights that must be addressed immediately by the International Community.

The present UN Framework for Human Rights can be "Suitably Amended" to accommodate Human Rights in Cyberspace. Almost all the Countries of the World are Member of UN and this would extend Human Rights Protection in Cyberspace to their Citizens automatically. The call is for UN to take and the sooner it is taken by it the better it would for Citizens' Worldwide. Take the example of India. The Cyber Law of India is violating various Human Rights in Cyberspace. This is the main reason why we started the exclusive Cyberspace Human Rights Protection Centre of India. So much offensive is the Cyber Law of India that it deserves to be repealed. Further, Indian Government launched Projects like Aadhar, National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network and Systems (CCTNS), National Counter Terrorism Centre (NCTC), Central Monitoring System (CMS), Centre for Communication Security Research and Monitoring (CCSRM), etc. None of them are governed by any Legal Framework and none of them are under Parliamentary Scrutiny.

If there is no "Internationally Acceptable Standard" for Protection of Human Rights in Cyberspace, Countries like India would keep on enacting and applying the Draconian Laws like Information Technology Act, 2000, Indian Telegraph Act, 1885, Official Secrets Act, etc. Finally, UN has shown some inclination in this regard. UN now considers Internet access a Human Right and considers disconnecting people from the Internet as a violation of Human Rights and International Law. A Report by the UN Human Rights Council's 17th Session underscored the "unique and transformative" nature of the Internet allowing individuals to exercise a range of Human Rights, and to promote the progress of society as a whole.[87]

[87] http://ictps.blogspot.in/2011/06/united-nations-and-human-rights-in.html

16.7. Foreign Terrorist Fighters:

UN Security Council Resolution 2178 on Foreign Terrorist Fighters-New York, NY-September 24, 2014:

Resolution 2178 requires countries to take certain steps to address the FTF threat, including to prevent suspected FTFs from entering or transiting their territories and to implement legislation to prosecute FTFs. It also calls on states to undertake various steps to improve international cooperation in this field, such as by sharing information on criminal investigations, interdictions and prosecutions. In this resolution, for the first time ever, the Council underscores that Countering Violent Extremism (CVE) is an essential element of an effective response to the FTF phenomenon. Resolution 2178 also focuses existing UN counterterrorism bodies on the FTF threat, providing a framework for long-term monitoring and assistance to countries in their efforts to address this threat.

Adopted under Chapter VII of the UN Charter, this resolution:

1. Reaffirms that Member States must comply with their human rights obligations when fighting terrorism and notes that a failure to do so contributes to radicalization.
2. Defines the term Foreign Terrorist Fighter as "individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict."
3. Expresses particular concern about the FTFs who have joined the Islamic State in Iraq and the Levant (ISIL), Al-Nusrah Front, and other groups associated with Al-Qaida.
4. Expresses concern over the use of the internet to incite others to commit terrorist acts and underlines the need to prevent terrorists from exploiting technology to incite support for terrorist acts, while at the same time respecting human rights and fundamental freedoms.
5. Notes the work of other multilateral bodies, including INTERPOL and other UN agencies, and the recent adoption by the Global Counterterrorism Forum (GCTF) of recommended good practices to respond to the FTF threat.

6. Demands FTFs disarm and cease all terrorist acts and participation in armed conflict.
7. Calls upon countries to require their airlines to provide advance passenger information to detect the travel of UN-listed terrorists.

Obligations

8. Requires countries to prevent and suppress recruiting, organizing, transporting, and equipping of FTFs, and the financing of FTF travel and activities.
9. Requires countries to have laws that permit the prosecution of:

- Their nationals and others departing their territories who travel or attempt to travel for terrorism purposes;
- The wilful provision or collection of funds by their nationals or in their territories with the intent or knowledge that they will be used to finance travel of FTFs;
- The wilful organization or facilitation by their nationals or in their territories of such travel.

10. Requires countries to prevent the entry or transit of individuals believed to be traveling for terrorism-related purposes.

International Cooperation

11. Calls upon countries to improve international, regional, and sub-regional cooperation to prevent FTF travel, including through increased information-sharing.
12. Highlights the need for countries to comply with their existing obligations regarding cooperation in terrorism-related criminal investigations and proceedings with respect to investigations and proceedings involving FTFs.
13. Encourages INTERPOL to intensify its efforts to respond to the FTF threat.
14. Calls upon countries to help each other build capacity to address the FTF threat and welcomes bilateral assistance to do so.

Countering Violent Extremism in Order to Prevent Terrorism

15. Underscores that Countering Violent Extremism (CVE) is an essential element of responding to the FTF threat.

16. Calls upon States to enhance CVE efforts and take steps to decrease the risk of radicalization to terrorism in their societies, such as engaging relevant local

communities, empowering concerned groups of civil society, and adopting tailored approaches to countering FTF recruitment.

UN Engagement

17. Directs UN counter-terrorism bodies to focus attention on the FTF threat, enabling the international community to assess compliance with this resolution and to target assistance to those countries that need help enforcing its provisions.

18. Requests a report from the UN within 180 days to assess comprehensively the FTF phenomenon and recommend actions to enhance the response to the threat.

16.8. United Nations Counter Terrorism Resolution:

The United Nations Global Counter-Terrorism Strategy was unanimously adopted by the General Assembly in 2006, representing a milestone in the domain of multilateral counter-terrorism initiatives. Pursuant to the Strategy, Member States resolved, inter alia:

(a) To consistently, unequivocally and strongly condemn terrorism in all its forms and manifestations, committed by whomever, wherever and for whatever purposes, as it constitutes one of the most serious threats to international peace and security;

(b) To take urgent action to prevent and combat terrorism in all its forms and manifestations;

(c) To recognize that international cooperation and any measures that [they] undertake to prevent and combat terrorism must comply with [their] obligations under international law, including the Charter of the United Nations and relevant international conventions and protocols, in particular human rights law, refugee law and international humanitarian law;

(d) To work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to "(a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (b) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard" [emphasis added].

Several Security Council resolutions adopted in recent years require States to cooperate fully in the fight against terrorism, in all its forms. In particular,

resolutions 1373 (2001) and 1566 (2004), adopted under Chapter VII of the Charter of the United Nations, require legislative and other action to be taken by all Member States to combat terrorism, including through increased cooperation with other Governments in the investigation, detection, arrest, extradition and prosecution of those involved in terrorist acts; and call upon States to implement the international conventions and protocols relating to terrorism.

Another key Security Council resolution relating to terrorist activity that may be conducted by means of the Internet is resolution 1624 (2005), which addresses the incitement and glorification of terrorist acts. In its fourth preambular paragraph, the Council condemns "in the strongest terms the incitement of terrorist acts "and repudiates" attempts at the justification or glorification (apologie) of terrorist acts that may incite further terrorist acts". In paragraph 1, it calls upon all States to adopt such measures as may be necessary and appropriate, and in accordance with their obligations under international law, to prohibit by law and prevent incitement to commit a terrorist act or acts.

Recent United Nations reports and resolutions have specifically acknowledged the importance of countering terrorist use of the Internet as a key part of a comprehensive counter-terrorism strategy. In his 2006 report to the General Assembly entitled "Uniting against terrorism: recommendations for a global counter-terrorism strategy", the Secretary-General explicitly stated: "The ability to generate and move finances, to acquire weapons, to recruit and train cadres, and to communicate, particularly through use of the Internet, are all essential to terrorists." The Secretary-General went on to assert that the Internet was a rapidly growing vehicle for terrorist recruitment and dissemination of information and propaganda, which must be countered through coordinated action by Member States, while respecting human rights and other obligations under international law.

In its resolution 1963 (2010), the Security Council expressed "concern at the increased use, in a globalized society, by terrorists of new information and communications technologies, in particular the Internet, for the purposes of the recruitment and incitement as well as for the financing, planning and preparation of their activities." The Council also recognized the importance of cooperation among Member States to prevent terrorists from exploiting technology, communications and resources.

16.9. Policy and Legislative Framework:

In order to provide effective criminal justice responses to threats presented by terrorists using the Internet, States require clear national policies and legislative frameworks. Broadly speaking, such policies and laws will focus on:

(a) Criminalization of unlawful acts carried out by terrorists over the Internet or related services;

(b) Provision of investigative powers for law enforcement agencies engaged in terrorism-related investigations;

(c) Regulation of Internet-related services (e.g. ISPs) and content control;

(d) Facilitation of international cooperation;

(e) Development of specialized judicial or evidential procedures;

(f) Maintenance of international human rights standards.

UN in its 2011 publication, Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects, the Working Group on Countering the Use of Internet for Terrorist Purposes of the Counter-Terrorism Implementation Task Force identified three broad strategic approaches by which States might counter terrorist activities over the Internet; involving the use of:

(a) General cyber crime legislation;

(b) General (non-Internet-specific) counter-terrorism legislation;

(c) Internet-specific counter-terrorism legislation

Another useful resource for policymakers and legislators, referred to in Countering the Use of the Internet for Terrorist Purposes is the Toolkit for Cybercrime Legislation, developed under the auspices of ITU. In addition to other model criminal provisions, the Toolkit contains several specific terrorist-related offences, including section 3 (f), which deals with unauthorized access to, or acquiring computer programs for, the purpose of developing, formulating, planning, facilitating, assisting in the commission of, conspiring to commit or committing acts of terrorism.

16.10. Case Study of UK:

R v. Tsouli and others: This well-known case from the United Kingdom involved three defendants—Younes Tsouli, Waseem Mughal and Tariq al-Daour—who were initially indicted on 15 counts. Prior to trial, Tsouli and Mughal pleaded guilty to a charge of conspiracy to defraud. During the trial, having heard the prosecution evidence, all three pleaded guilty to a charge of inciting terrorismoverseas, and Al-Daour pleaded guilty to a charge of conspiracy to defraud.

Between June 2005 and their arrest in October 2005, the defendants were involved in the purchase, construction and maintenance of a large number of websites and Internet chat forums on which material was published that incited acts of terrorist murder, primarily in Iraq. The cost of purchasing and maintaining the websites was met from the proceeds of credit card fraud. The material on the websites included statements that it was the duty of Muslims to wage armed jihad against Jews, crusaders, apostates and their supporters in all Muslim countries and that it was the duty of every Muslim to fight and kill them wherever they were, civilian or military. In the Internet chat forums, individuals disposed to join the insurgency were provided with routes by which to travel into Iraq and manuals on weapons and explosives recipes. Extreme ideological material demonstrating adherence to the espoused justification for the acts of murder that the websites and chat forums incited was recovered from the home of each defendant. Al-Daour organized the obtaining of stolen credit cards, both for his own purposes and for providing Mughal with funds for the setting up and running of the websites. Al-Daour had

also been involved in further credit card fraud; the proceeds of which were not applied to the support of the websites. The loss to the credit card companies from this aspect of the defendants' fraudulent activity was £1.8 million. Among the evidence was a list made by Tsouli in his handwriting and found in his desk on which he had written the details of a number of websites and of stolen credit cards. This revealed 32 separate websites provided by a number of different web-hosting companies that Tsouli had set up or attempted to set up, mostly in the last week of June 2005 but continuing into July and into August. The creation and administration of these websites were funded by the fraudulent use of credit card details that had been stolen from account holders, either by direct theft of computer records, by hacking or by some fraudulent diversion within the financial

institutions. These credit card details had been passed on to Tsouli by the other two defendants.

The websites created by Tsouli were used as a vehicle for uploading jihadist materials, which incited acts of violence outside the United Kingdom in Iraq. Access to the sites was restricted to those who had been issued with usernames and passwords. This was done, the trial judge found, to make it more difficult for the web-hosting companies and the law enforcement agencies to know what was being posted on the sites. On 5 July 2007, Tsouli was sentenced to 10 years of imprisonment and 3½ years (concurrently) on two counts. Mughal to 7½ years of imprisonment and 3½ years (concurrently) on two counts and al-Daour, to 6½ years of imprisonment and 3½ years (concurrently).

16.11. Summary:

The concept of human rights in the perspective of the cyber terrorist is little different globally and some time they are claiming themselves as freedom fighters and fighting for religious cause. In this unit the important concept of the cyber terrorism and human rights in the form of international conventions on terrorism, cyber terrorism and right to privacy, human rights and UDHR, human rights, UN and cyber world, foreign policy and legislative framework and case study of UK are discussed at length to understand the issues.

16.12. Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)

- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

16.13. Check your Progress:

I. Which of the following statements are true or false:

a. The issue of terrorism and human rights has long been concern of the United Nations.
b. The right to privacy as an independent and distinctive concept originated in the field of tort law.
c. Human rights protection in cyber space is urgently needed at national and national level.
d. The UN Global Counter Terrorism Strategy was unanimously adopted by the General Assembly in 2006.
e. Resolution 2178 requires countries to take certain steps to address the FTF (Foreign Terrorist Fighters).

A. Fill in the Blanks:

I. Extends the provisions of the ……..to encompass terrorist acts at airports international civil aviation.

II. ……International Convention for the Suppression of Terrorist Bombings is related to Terrorist Bombing Conventions.

III. ……International Convention for the Suppression od Acts of Nuclear is related to Terrorism (Nuclear Terrorism Convention).

IV. ……of the Universal Declaration of Human Rights sets the right to "security of person".

V. UN Security Council Resolution No. 2178 is related to……..

16.14. Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Montreal Convention
2. 1997
3. 2005

4. Article 3
5. Foreign Terrorist Fighters

16.15. Terminal Questions:

1. How many international Conventions on Terrorism?
2. Define terrorism and right to privacy.
3. What is UN resolution No. 2178?
4. What is UN Counter Terrorism Resolution?
5. Write a case study of UK?

Unit-17

Role of International Organizations in Cyber Crimes

Objectives:

After going through this unit you should be able to:

- Understand the issues and subject matters under the scope of International Organizations with reference to Cyber Crimes
- Understand the role and importance of various international Organizations in Combat Cyber Crimes
- Understand the technical and legal issues related to Cyber Crimes

Structure:

17.1. Introduction:

In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years. By the year 2017, it is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population. By the year 2020, the number of networked devices (the 'internet of things') will outnumber people by six to one, transforming current conceptions of the internet. In the hyper connected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity. 'Definitions' of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime'.

Over 90 per cent of responding countries report that cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. Responding countries estimate that the proportion of actual cybercrime victimization reported to the police ranges upwards from 1 per cent. One global private sector survey suggests that 80 per cent of individual victims of core cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. Authorities in all regions of the world highlighted initiatives for increasing reporting, including online and hotline reporting systems, public awareness campaigns, private sector liaison, and enhanced police outreach and information sharing. An incident-driven response to cybercrime must, however, be saccompanied by medium and long-term tactical investigations that focus on

crime markets and criminal scheme architects. Law enforcement authorities in developed countries are engaged in this area, including through undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and P2P services. Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence, and from internal resource, capacity and logistical limitations. Suspects frequently use anonymization and obfuscation technologies, and new techniques quickly make their way to a broad criminal audience through online crime markets.

INTERPOL and Cyber Crimes: Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual.

These crimes can be divided into three broad areas:

Attacks against computer hardware and software, for example, botnets, malware and network intrusion;

Financial crimes, such as online fraud, penetration of online financial services and phishing;

Abuse, especially of young people, in the form of grooming or ‘sexploitation’.

New trends in cybercrime are emerging all the time, with costs to the global economy running to billions of dollars.

In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing criminal organizations working with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. Highly complex, these cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

INTERPOL's role: INTERPOL is committed to becoming a global coordination body on the detection and prevention of digital crimes through its INTERPOL Global Complex for Innovation (IGCI), currently being constructed in Singapore.

A key component of this new cutting-edge research and development facility is the INTERPOL Digital Crime Centre. This new centre provides proactive research into new areas and latest training techniques, and coordinates operations in the field.

Our main initiatives in cybercrime focus on:

Harmonization

Capacity building

Operational and forensic support.

While effective law enforcement is an essential component to fighting cyber threats, we also recognize the importance of engaging all stakeholders – from the private sector, academia and public institutions –who are working towards the common goal of a safer cyberspace.

It is important to harmonize efforts across different sectors in order to share expertise while avoiding duplication of activities already in progress. In this way, police may efficiently focus their resources on fighting cybercrime, as we work with other stakeholders to develop a holistic and coordinated response.

By encouraging the creation of dedicated cybercrime investigation units, and updating legal frameworks, INTERPOL will build a proactive facilitation role in fighting cybercrime.

The main services of the harmonization include:

National cyber review – a comprehensive audit of national legislation, police infrastructure and technical capacity, with accompanying recommendations;

Cyber security strategy development – working with regulatory bodies to develop global strategies as well as advising individual countries on their national approach;

International advocacy on cyber legislation and governance – representing the law enforcement perspective in the development of new and updated legislation;

Research and innovation – combining police research with similar activities in other sectors.

At INTERPOL, we work to ensure that police keep pace with technological developments and have the required expertise and skills to deal with evolving digital crime at the national and international levels.

We provide a range of training courses, targeted to the needs of participants, covering topics such as emerging trends in cybercrime, investigation techniques, digital forensics and more.

Training takes the form of e-learning modules, classroom-based sessions and workshops and can lead to professional certification. 'Train-the-trainer' courses are particularly valuable as they enable participants to pass on their new skills and knowledge to their colleagues.

Increasingly, INTERPOL's cybercrime training portfolio is developed and delivered with input from academia, computer emergency response teams (CERT), national police and the private sector.

We support member countries during cyber investigations and help coordinate joint operations.

Cyber Fusion Centre

This provides essential assistance to INTERPOL's member countries during all stages of an investigation. Functioning in a similar manner to INTERPOL's Command and Coordination Centre, the Cyber Fusion Centre provides real-time monitoring and analysis of malicious internet activity, giving member countries the intelligence and expertise required to be more effectively investigate digital crimes.

Digital Forensic Laboratory

This laboratory works to build national digital forensic capacity through training, while at the same time providing practical forensic support to member countries during investigation.

Regional coordination

Working Groups have been created to facilitate the development of regional strategies, technologies and information on the latest crime trends and methods.

There are regional working parties for:

Africa

Americas

Europe and Asia

Middle East and North Africa.

The main activities of the working parties are based around operations, training and finding solutions to emerging threats.

17.2 Federal Bureau of Investigation (FBI) and Cyber Crimes-I[88]:

Computer Intrusions:

Every day, criminals are invading countless homes and offices across the nation—not by breaking down windows and doors, but by breaking into laptops, personal computers, and wireless devices via hacks and bits of malicious code.

The collective impact is staggering. Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

Today, these computer intrusion cases—counterterrorism, counterintelligence, and criminal—are the paramount priorities of our cyber program because of their potential relationship to national security.

Combating the threat. In recent years, we've built a whole new set of technological and investigative capabilities and partnerships—so we're as comfortable chasing outlaws in cyberspace as we are down back alleys and across continents. That includes:

- A Cyber Division at FBI Headquarters "to address cyber crime in a coordinated and cohesive manner";
- Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with "agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud";

[88] http://unchronicle.un.org/article/fighting-industrialization-cyber-crime/

- New Cyber Action Teams that "travel around the world on a moment's notice to assist in computer intrusion cases" and that "gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy;"
- Our 93 Computer Crimes Task Forces nationwide that "combine state-of-the-art technology and the resources of our federal, state, and local counterparts";
- A growing partnership with other federal agencies, including the Department of Defense, the Department of Homeland Security, and others—which share similar concerns and resolve in combating cyber crime.

17.3 Federal Bureau of Investigation (FBI) and Cyber Crimes-II[89]:

Holiday Shopping Tips: The FBI reminds holiday shoppers to beware of cyber criminals who are out to steal money and personal information. Scammers use many techniques to defraud consumers, from phishing e-mails offering too good to be true deals on brand-name merchandise to offering quick cash to victims who will re-ship packages to additional destinations. Previously reported scams are still being executed today.

While monitoring credit reports on an annual basis and reviewing account statements each month is always a good idea, consumers should keep a particularly watchful eye on their personal credit information at this time of year. Scrutinizing credit card bills for any fraudulent activity can help to minimize victims' losses. Unrecognizable charges listed on a credit card statement are often the first time consumers realize their personally identifiable information has been stolen.

Bank transactions and correspondence from financial institutions should also be closely reviewed. Bank accounts can often serve as a target for criminals to initiate account takeovers or commit identity theft by creating new accounts in the victims' name. Consumers should never click on a link embedded in an e-mail

[89] http://unchronicle.un.org/article/fighting-industrialization-cyber-crime/

from their bank, but rather open a new webpage and manually enter the URL (web address), because phishing scams often start with phony e-mails that feature the bank's name and logo.

When shopping online, make sure to use reputable sites. Often consumers are shown specials on the web, or even in e-mail offers, that look too good to be true. These sites are used to capture personally identifiable information, including credit card numbers, addresses and phone numbers to make fraudulent transactions. It's best to shop on sites with which you are familiar and that have an established reputation as trusted online retailers, according to the MRC, a nonprofit that supports and promotes operational excellence for fraud, payments and risk professionals within e-Commerce.

If you look for an item or company name through a search engine site, scrutinize the results listed before going to a website. Do not automatically click on the first result, even if it looks identical or similar to the desired result. Many fraudsters go to extreme lengths to have their own website appear ahead of a legitimate company on popular search engines. Their website may be a mirrored version of a popular website, but with a slightly different URL.

Purchases made on these sites could result in one or more of the following consequences: never receiving the item, having your credit card details stolen, or downloading malware/computer virus to your computer. Before clicking on a result in a search engine, inspect the URL of the destination website. Look for any misspellings or extra characters such as a period or comma as these are indicative of fraud. When taken to the payment page of a website, again verify the URL and ensure it is secure by starting with "HTTPS," not just "HTTP."

Here are some additional tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files; the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.

- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- Log on directly to the official website for the business identified in the e-mail instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency that requires your attention, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Remember if it looks too good to be true, it probably is.

17.4 Federal Bureau of Investigation (FBI) and Cyber Crimes-III[90]:

Internet Fraud: Listed below are tips to protect yourself and your family from various forms of Internet fraud.

For information on the most common complaints and scams, see the annual reports of the Internet Crime Complaint Center, or IC3, a partnership of the FBI and the National White Collar Crime Center. Also see its information on Internet Crime Schemes and its Internet Crime Prevention Tips.

Use our online tips form or the IC3 website to report potential cases of cyber fraud.

Tips for Avoiding Internet Auction Fraud:

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website/company takes if a problem occurs and consider insuring the transaction and shipment.

[90] http://unchronicle.un.org/article/fighting-industrialization-cyber-crime/

- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller.
- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Be cautious when dealing with sellers outside the United States. If a problem occurs with the auction transaction, it could be much more difficult to rectify.
- Ask the seller about when delivery can be expected and whether the merchandise is covered by a warranty or can be exchanged if there is a problem.
- Make sure there are no unexpected costs, including whether shipping and handling is included in the auction price.
- There should be no reason to give out your social security number or driver's license number to the seller.
- Tips for Avoiding Non-Delivery of Merchandise:
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.

- Check with the Better Business Bureau from the seller's area.
- Check out other websites regarding this person/company.
- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about returns and warranties.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card numbers.
- Consider using an escrow or alternate payment service.
- Tips for Avoiding Credit Card Fraud:
- Don't give out your credit card number online unless the site is a secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.
- Don't trust a site just because it claims to be secure.
- Before using the site, check out the security/encryption software it uses.
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.

- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the seller's area.
- Check out other websites regarding this person/company.
- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card number.
- Keep a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.
- Tips for Avoiding Investment Fraud:
- Don't judge a person or company by their website. Flashy websites can be set up quickly.
- Don't invest in anything you are not absolutely sure about. Do your homework on the investment and the company to ensure that they are legitimate.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about all the terms and conditions.
- Tips for Avoiding Business Fraud:

- Purchase merchandise from reputable dealers or establishments.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent.
- Tips for Avoiding the Nigerian Letter or "419" Fraud:
- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.

17.5 Fighting the Industrialization of Cyber Crime:

When we talk about the digital underground economy, what we mean is a collection of self-sufficient global networks that operate mostly in closed Internet forums and facilitate an array of cybercrimes including banking attacks, payment card frauds, identity theft and other online intrusions. Stolen personal and financial data is retailed on these forums.

The sophistication of this criminal business model is such that members of these networks are able to focus on specific tasks including producing malicious code or delivery mechanisms for attacks. There are even specialists who are dedicated to the generation of payment card authentication numbers and the recruitment of money mules, individuals who turn the proceeds of cybercrime into hard cash—sometimes without knowing that they are engaging in criminal activity.

Cybercriminal businesses are constantly innovating. As well as making extensive use of social media to distribute scams and links to malicious software, they scan the environment to identify new software vulnerabilities, new environments popular with Internet users and new attack vectors. Among the more ingenious forms of scam in recent years is police ransom ware. This malicious software locks the user's computer until a fine is paid to an online bank account. The insignia and branding of legitimate law enforcement agencies are reproduced to convince the user that they are dealing with the real police in their home country, an impression reinforced by the translation of the notification into the appropriate language. The user is informed that they have engaged in criminal activity online, for instance downloading of child abusive material or pirated audiovisual files.

By playing on the fear and guilt of the victims, this kind of cybercrime has proven to be highly lucrative. The law enforcement community, supported by the European Cybercrime Centre (EC3) at Europol and Interpol, is making tangible progress against the criminal groups engaged in ransom ware distribution. In February 2013, Operation Ransom, led by the Spanish police, resulted in 11 arrests for the production, development and distribution of this type of malware, and the arrest of another 10 individuals involved in the financial side of the scam. Investigations are ongoing.

Networks of many thousands of infected computers which essentially serve as zombies to conduct attacks on other systems, botnets have accelerated cybercrime's industrialization more than any other tool. Before the rise of botnets, victims of cybercrime were targeted one by one, requiring much greater time and effort on the part of criminals. Today, spam delivery and Distributed Denial of Service attacks that stop government and commercial websites by flooding them with Internet traffic are particularly reliant on botnets for their processing power. Your personal computer, notebook or smartphone may well have been exploited in this way.

Botnets are not only powerful but highly cost-effective, with prices dipping to $150 in recent months. And just as legitimate businesses are moving their computing to the Cloud, so too can we expect to see Cloud botnets in the very near future—highly dynamic entities that will quickly change location, thereby requiring timely and concerted international cooperation to dismantle.

Meanwhile, the Internet has increasingly become designated as critical infrastructure. It is also a technology on which the vast majority of critical infrastructures rely, including power supply, health-care provision and emergency communications.

As a world citizen in 2013, you may be forgiven for thinking that the threat from cybercrime is not real or at least overhyped. While statistics cited in the popular media routinely refer to many millions of infected computing devices and billions of US dollars lost through intrusions or online frauds, the immediate impact of these is rarely felt by the average Internet user, who will be reimbursed by their financial services provider and may feel no need to report the crime to the police. In contrast to, say, online child sexual exploitation, cybercrime to date has, for the most part, not incurred significant harm on its victims.

However, this is likely to change in the very near future. The increasing dependence of vulnerable citizens on Internet-enabled medical devices such as heart pacemakers, defibrillators and insulin pumps, combined with ageing populations in many parts of the world, highlight the importance of awareness-raising and digital hygiene for older members of society. This may sound like science fiction, but I am speaking from experience. My own father was fitted with a wireless-enabled pacemaker but had no idea of the potential consequences of not keeping his anti-virus software up to date. And not everyone has the luxury of a cybercrime investigator in their family.

Law enforcement has been fully aware of the threat from cybercrime for over a decade but it has taken some time for cybercrime to enjoy priority in terms of resourcing. Around the world, cybercrime-fighting capabilities are developing at very different speeds. Wherever I travel in my work for EC3, I have yet to visit a law enforcement agency that claims to have sufficient resources to combat the threat or to effectively manage workloads amounting to scores of investigations which often require the examination of terabytes of data. Local and national agencies operating in isolation are undoubtedly not making the best use of their resources.

When we will look back on 2013 and 2014, we will view these years as landmarks in the fight against cybercrime. In January 2013, EC3 opened its doors. Based at Europol in The Hague, the centre provides specialist operational support and intelligence coordination to cybercrime investigations in the 27 European Union

member states and, in turn, harnesses their capability and expertise to deliver more comprehensive and targeted responses to online threats.

In 2014, Interpol's new Digital Crime Centre will be operational at its Global Complex for Innovation in Singapore. In the development of both centres, strong emphasis has been placed on delivering collaborative responses which draw on the full range of cybersecurity stakeholders, including industry, academia and civil society organizations, as well as government authorities.

EC3, for example, has partnered with the International Cyber Security Protection Alliance (ICSPA). Supported by the Prime Minister of the United Kingdom, David Cameron, it is an initiative that brings together law enforcement and the Internet security industry in the delivery of global capacity-building and cybercrime prevention. Under the auspices of ICSPA, EC3 is leading Project 2020 by looking at scenarios which anticipate the future of cybercrime and seek to prepare citizens, businesses and governments by using arresting awareness-raising materials, such as movies and animations. When technology evolves as quickly as the Internet, it pays to be one step ahead.

No one can accurately predict the future, but we can be reasonably confident that some emerging technologies will be more prominent in 2020. Augmented reality is already apparent in the form of smartphone applications which deliver online information about the user's physical location: think tailored reviews for local restaurants and apps which map the night sky wherever you are, but head-mounted displays such as Google Glass are set to integrate this augmented content more fully into our experience of the offline world.

The Internet of Things is the phrase often used to describe the incorporation of Internet connectivity into a plethora of previously unconnected devices, such as home appliances and clothing. In combination with a further increase in Radio Frequency Identification tagging, the global proliferation of Internet-enabled sensors has the potential to deliver considerable innovation in supply and distribution chains, while the advent of 3-D printing may well be a catalyst for new manufacturing models.

None of these technologies will operate in isolation; rather, they will be part of a single ecosystem. Add to this smart home technology the insights to be gained from big and intelligent data, and the long-awaited emergence of virtual reality in the form of remote presence technologies such as beaming, and it is evident that

even more data will be generated by all of us, all of the time. This will continue to be attractive to cybercriminals, requiring enhanced protection by service providers and even greater levels of international cooperation by those charged with investigating breaches, and hold cybercriminals to account.

Legislation around the globe will not only need to catch up but also keep pace with criminal misuse of emerging technologies. There is now a real risk that, without harmonization, countries with lower levels of cybersecurity, weaker cybercrime legislation and diminished law enforcement capability will become safe havens for cybercriminals for many years to come.

International cooperation is already essential to successfully investigating and prosecuting cybercrime. However, we also need to think smarter, beyond the traditional criminal justice practices of apprehending, prosecuting and convicting individuals. Effective disruption and prevention measures are, and will continue to be, possible. International organizations like Europol, Interpol and the United Nations are force multipliers in the delivery of effective multi-sector initiatives to dismantle botnets, reduce the profits of the digital underground economy and actively engage citizens in protection against attacks.

The fight against cybercrime also requires specialist information hubs and intelligence coordination. Very often it is only at the international level that analysts can gain an accurate picture of the extent and harm of a cybercriminal group's activities. The law enforcement and security communities, for instance, need organizations like Europol, Interpol, United Nations Office on Drugs and Crime, and United Nations Interregional Crime and Justice Research Institute to help them make sense of the threat, and make crucial links between offences in often very disparate parts of the world.

For a number of years, the international community has described cybercrime as borderless. It is now time to walk the walk and provide truly coordinated responses which are not only timely but responsive to changes in Internet technologies. By working together with a shared goal for a safer Internet, we will ensure not only that we meet current threats as effectively as possible, but that we will also be fit for the future.[91]

[91] http://unchronicle.un.org/article/fighting-industrialization-cyber-crime/

17.6 United Nations and Cyber Crimes:

The United Nations has in the General Assembly, Resolution 65/230, initiated a study of the problem of cybercrime, in order to convene an open-ended intergovernmental expert group to conduct a comprehensive study on the problem of cybercrime as well as they response to it. The study group is organized by by the UNODC in Vienna,

«with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime».

The expert group had the First Session in Vienna, January, 2011. A questionnaire was in February 2012 sent to all United Nations Member States, the private sector, IGOs and academia. Regional workshops were also organized.

The Second Session was held in Vienna February 25-28, 2013. The drafting and recommendations of the study was discussed, and The Session decided on the way forward.

General Assembly

The General Assembly has in 2010 adopted the Resolution 65/230 based initially on the Salvador Declaration Article 42. A draft Resolution by the Commission on Crime Prevention and Criminal Justice in Article 8 was based on the Salvador Declaration Article 42 (2010). The Resolution made a proposal to establish as follows:

An open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examening options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

The Resolution was adopted by the Commission, and later by the United Nations General Assembly in its Resolution 65/230.

A Resolution on combating the criminal misuse of information technologies was adopted by the General Assembly on December 4, 2000 Resolution 55/63, including as follows:

"(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.
(d) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized."
Resolution 56/121 was adopted on December 19, 2001, including recommendations on the prevention and combat criminal misuse of information technologies.
United Nations Office for Drugs and Crime (UNODC): The United Nations Congress on Crime Prevention and Criminal Justice have looked at technical issues and criminal enforcement of computer misuse for at least the last four Congresses. The United Nations adopted in 1990 a resolution on computer crime legislation at the 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba. The most recent 12th Congress in Salvador, Brasil, (2010) focused on issues of cybercrime a several events. The Congress reports and background papers are both available from the United Nations Office on Drugs and Crime.

17.7 UN efforts on Protecting Children from Cyber Crime:

In May 2011, the United Nations Commission on Crime Prevention and Criminal Justice published a report from its twentieth meeting in Vienna, focusing on the growing problem of cyber crime against children. The CCPCJ, a subsidiary body of the Economic and Social Council and the governing body of the U.N. Office on Drugs and Crime , undertakes international action to combat national and transnational crime, promoting the role of criminal law to prevent illegal trafficking in natural resources, crime prevention in urban areas, and improving the efficiency and fairness of criminal justice systems. This *Insight* focuses on the thematic discussion of the twentieth meeting: Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children.€ •

Virtual Crime, Real Victims: The Executive Director of UNODC, Yury Fedotov, opened the twentieth meeting of the CCPCJ by framing the scope of cyber crime against children. He emphasized that with nearly two billion internet users worldwide, there are â□ œgreater opportunities [for criminals] to entrap new

victims, including children. Specifically, new information technologies are being misused to commit crimes such as: (a) child exploitation; (b) production, distribution, and possession of child pornography; (c) exposure to harmful content; (d) grooming, harassment, and sexual abuse; and (e) cyber bullying.

The latest technologies make it easier for criminals to contact children in ways that were not previously possible. Children are particularly vulnerable to the exploitation of online predators because they rely heavily on networking websites for social interaction. Offenders use false identities in chat rooms to lure victims into physical meetings, thus connecting the worlds of cyber and physical crime. When this happens, virtual crime often leads to traditional forms of child abuse and exploitation such as trafficking and sex tourism. The victims of online exploitation must live with their abuse for the rest of their lives. It is widely believed that exposure to certain content and easy contact with criminals online may affect the integral development of children. And once information and images are online, they remain online forever and are available to an increasing number of persons. Experts at the CCPCJ twentieth meeting reminded delegates that online images of abuse are the result of actual, physical crimes.

Crime without Borders: Criminal enterprises benefit from the relative anonymity the internet provides. Law enforcement authorities struggle to locate offenders because of the ability to conceal online identities and shield unlawful activities with security programs. This anonymity is compounded by a strategic use of internet service providers in multiple jurisdictions. When a perpetrator suspects that law enforcement in one jurisdiction is tracking his/her activity, he/she need only relocate the criminal enterprise to an ISP beyond the reach of those authorities. As a result, swift action is required to attribute cyber exploitation of children to users before they can transfer to the relative safety of a different ISP. Criminals also frustrate law enforcement by developing new means to further their misconduct. Commercial websites once served as the major source of online exploitative images of children, where individuals paid a fee to access site content. These groups are now moving toward smaller social networks, image-sharing sites, free hosting platforms, and hacked websites. The less formal, peer-to-peer networks do not leave a money trail, making it more difficult for law enforcement to identify online perpetrators.

17.8 Asia Pacific Economic Cooperation and Cyber Crimes:

In the Asia-Pacific region, the APEC coordinates its 21 member economies to promote cyber security and to tackle the risks brought about by cybercrime. The APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002, supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for the APEC's endeavor for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and education, and wireless security.The Ministers and Leaders of APEC have made a commitment to "endeavour to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003."

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003. The economies proposed corresponding projects in information-security task groups. For example, the U.S. proposed a project in the E-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the

development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime. In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional cooperation, law-enforcement construction, and the capacity building of the investigators.

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and to endeavor to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)." However, due to the great difference between member economies within the APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of the APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors).[92]

17.9 European Union and Cyber Crimes:

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field. In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on

[92] http://www.webology.org/2007/v4n3/a45.html

the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1). The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the member states' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the EU Forum on Cybercrime, organized by the EC, and where the primary discussion was about the retention of traffic data (EU Forum on Cybercrime, 2001).

In April 2002, the Commission of the European Communities presented a proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February 2005. The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious

damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences." It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime. After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision.

17.10 Summary:

The role of international organization is very crucial and important to combat the cyber terrorism and cyber crime globally. In this unit the important concept of INTERPOL and cyber crime, Federal Bureau of Investigation (FBI) and cyber crime, fighting the industrialization of cyber crime, UN and cyber crimes, Un efforts on protecting children from cyber crimes, Asia-Pacific Economic Cooperation and cyber crime and European Union and Cyber Crimes are discussed at length to understand the various issues related to cyber crime worldwide.

17.11 Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)

- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)
- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

17.12 Check your Progress:

A. Which of the following statements are true or false:

a) In 2011, at least 2.3 billion people, the equivalent of more than one third of the population, had access to the internet.
b) Cyber crime is fast growing area of crime.
c) Cybercrime includes attacks against computer hardware and software.

d) Legislation around the globe will not only need to catch up but also keep pace with criminal mis use of emerging technologies.
e) In the Asia-Pacific Region, the APEC coordinates the 21 member economies to promote cyber security and to tackle the risked brought about by cyber crime.'

B. Fill in the Blanks:

I. Cyber crime includes abuse especially of …….., in the form of 'grooming' or 'exploitation'.
II. Cyber criminal businesses are ……..
III. In……., INTERPOL's new Digital Crime Center will be operational as its Global Complex for Innovation in Singapore.
IV. ICSPA means…….
V. The USN General Assembly,……. Initiated a study of the problem of cyber crime.

17.13 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. Young People
2. Constantly Innovating
3. 2014
4. International Cyber Security Protection Alliance
5. Resolution 65/230

17.14 Terminal Questions:

1. Discuss INTERPOL and cyber crime.

2. Discuss in detail FBI and cyber crime.
3. Discuss UN and cyber crime.
4. What are the efforts of UN on protecting children from cyber crimes?
5. Discuss in detail Asia-Pacific Economic Cooperation and cyber crime.

Unit-18

Case Studies and Cyber Crimes

Objectives:

After going through this unit you should be able to:

- Understand the Cyber Crimes through various International Case Studies
- Understand the Cyber Crimes through various Indian Case Studies
- Understand the technical and legal issues related to Case Studies

Structure:

18.1. Introduction:

McAfee and CSIS: Stopping Cybercrime Can Positively Impact World Economies (Economic Impact of Cybercrime Estimated at $445 billion Worldwide, and between 15% and 20% of the value created by the Internet)=SANTA CLARA, Calif. — June 9, 2014 — A new report from the

Center for Strategic and International Studies (CSIS) and sponsored by McAfee, part of Intel Security, shows the significant impact that cybercrime has on economies worldwide. The report, "Net Losses – Estimating the Global Cost of Cyber crime," concludes that cybercrime costs businesses approximately $400 billion worldwide, with an impact on approximately 200,000 jobs in the U.S., and 150,000 jobs in the EU.

The most important cost of cybercrime comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth. Studies estimate that the Internet economy annually generates between $2 trillion and $3 trillion, a share of the global economy that is expected to grow rapidly. Based on CSIS estimates, cybercrime extracts between 15% and 20% of the value created by the Internet. Cybercrime's effect on intellectual property (IP) is particularly damaging, and countries where IP creation and IP-intensive industries are important for wealth creation lose more in trade, jobs and income from cybercrime than countries depending more on agriculture or industries of low-level manufacturing, the report found. Accordingly, high-income countries lost more as a percent of GDP than low-income countries – perhaps as much as 0.9 percent on average.

"Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors," said Jim Lewis of CSIS. "For developed countries, cybercrime has serious implications for employment. The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment."

Economic Impacts on both Businesses and Consumers

CSIS researchers found that the United States notified 3,000 companies in 2013 that they had been hacked, with retailers leading as a favorite target for hackers. In the U.K., retailers reportedly lost more than $850 million to hackers. Australian officials reported that large scale attacks have occurred against an airline, hotel chains and financial services companies, costing an estimated $100 million. With proper protections in place, these losses could be avoided.

The report found that global losses connected to "personal information" breaches could reach $160 billion. Forty million people in the U.S., roughly 15 percent of the population, have had their personal information stolen by hackers. The study

tracked high-profile breaches around the world: 54 million in Turkey; 20 million in Korea; 16 million in Germany and more than 20 million in China.

Part of the losses from cybercrime are directly connected to what experts call "recovery costs," or the digital and electronic clean-up that must occur after an attack has taken place. The McAfee-CSIS report discovered that while criminals will not be able to monetize all the information they steal, their victims must spend significant resources as if they could.

In Italy, for example, actual hacking losses totaled $875 million, but the recovery, or clean-up costs, reached $8.5 billion. In other words, there can be a tenfold increase between the actual losses directly attributed to hackers and the recovery companies must implement in the aftermath of those attacks. Turning from Losses to Potential Economic Gains Governments are beginning serious, systematic efforts to collect and publish data on cybercrime to help countries and companies make better choices about risk and policy. Improved international collaboration, as well as public/private partnerships is also beginning to show tangible results in terms of reducing cybercrime. Last week, 11 nations announced the takedown of a crime ring associated with the Game Over Zeus bonnet.

"It's clear that there's a real tangible economic impact associated with stopping cybercrime," said Scott Montgomery, chief technology officer, public sector at McAfee. "Over the years, cybercrime has become a growth industry, but that can be changed, with greater collaboration between nations, and improved public private partnerships. The technology exists to keep financial information and intellectual property safe, and when we do so, we create opportunities for positive economic growth and job creation worldwide."[93]

18.2. Cyber Crime in UK-Case Study:

Cybercrime in UK – case study:

To contextualize the effect of cyber crime, it's interesting to consider the data available for a country like the United Kingdom. It's one of the nations with the highest technological penetration levels. The data published in a recent study conducted by cyber security experts at the University of Kent is more shocking. Over 9 million adults in Britain have had online accounts hacked, and 8% of the

[93] http://www.mcafee.com/in/about/news/2014/q2/20140609-01.aspx

UK netizens are revealed to have been victims of cyber crime in the past year. 2.3% of the population reported losing more than £10,000 to online fraudsters.

The main crime suffered by UK online users is the hacking of their web services accounts. Those include online banking, email, and social media. In nearly 33% of the cases, the offense was repeated.

In 2011, the UK government documented in an official report that the overall cost of cyber crime economy was £27 billion a year. Identity theft was most common crime, accounting for £1.7 billion. That was followed by online scams, with £1.4 billion. Cyber crime in the UK was most insidious for organizations, private businesses and government offices, suffering high levels of cyber espionage and intellectual property theft. Social media is a primary target for emerging cybercrime in the UK. Malicious code is used by criminal gangs to exploit social networks for banking fraud or for phishing campaigns. A new trend has emerged in recent months. The same malicious code is used by criminals to hack victims' accounts, for the creation of bogus social network 'likes' that could be used to generate buzz for a company or individual.

Fake "likes" were sold by lots of 1,000 per unit, underground. RSA estimated that 1,000 Instagram "followers" could be bought for $15 (£9.50), and 1,000 Instagram "likes" cost $30 (£19). These are more profitable for sales. Consider, when selling credit card numbers, they're sold for $6 (£3.80) for a lot of 1,000 numbers.

"It seems online crime has a clear impact on the lives of average UK citizens, with their accounts and credentials being compromised significantly and in some cases multiple times. Cybercrime may not yet have hit a large proportion of the British public, but successful attacks do tend to lead to substantive financial damage," said Dr Julio Hernandez-Castro and Dr Eerke Boiten, from the University of Kent's Interdisciplinary Centre for Cyber Security Research.

Cybercrime as service:

The terms "Attack-as-a-Service," "Malware-as-a-Service," and "Fraud-as-a-Service" are used to qualify models of sale in which cybercriminals sell or rent their colleagues hacking service and malicious code, to conduct illegal activities. The concept is revolutionary, the black market offers entire infrastructures to service malware (e.g.bullet-proof hosting or rent compromised machines

belonging to huge bonnets), and outsourcing and partnerships services, including software development, hacking services, and, of course, customer support.

The majority of these services are presented in the underground economy, based on a subscription or flat-rate fee model, making them convenient and attractive. The principal cost of arranging criminal activities is shared between all customers. This way, service providers could increase their earnings, and clients benefit from a sensible reduction of their expenditure, with the knowledge needed to manage illegal businesses. These services are characterized by their ease of use and a strong customer orientation. They typically have a user-friendly administration console and dashboard for the control of profit. The diffusion of the cloud computing paradigm has brought numerous advantages to IT industry, but also new opportunities for cyber criminals. The term "Attack-as-a-Service" is referred to as the capability of criminal organizations to offer hacking services. The majority of cases exploit cloud based architectures.

Cyber criminals offer entire botnet and control infrastructures, hosted on cloud architectures for lease or sale. Compromised machines could be used to steal information from the victims (e.g. banking credentials, sensitive information) or to launch massive DdoS attacks against specific targets. The prices for attacks on commission are widely variable. Some services are totally free, such as a subscription for IMDDOS. Meanwhile, it costs between $150 and $400 to crack e-mail passwords in less than 48 hours. One of the most interesting studies proposed regarding cyber crime offers was presented by Fortinet in December 2012. The report produced by the security firm describes the model of "Crime-as-a-Service" in particular, providing a detailed price list for principal hacking services offered in "Attacks-as-a-Service," with some interesting data:

- *Consulting services such as botnet setup, $350-$400*
- *Infection/spreading services, under $100 per a thousand installs*
- *Botnets and rental, Direct Denial of Service (DdoS), $535 for 5 hours a day for one week, email spam, $40 per 20,000 emails, and Web spam, $2 per thirty posts.*
- *Blackhat Search Engine Optimization (SEO), $80 for 20,000 spammed backlinks.*

- *Inter-Carrier money exchange and mule services, 25% commission.*
- *CAPTCHA breaking, $1 per a thuosand CAPTCHAs, done by recruited humans.*
- *Crimeware upgrade modules: Using Zeus modules as an example, they range anywhere from $500 to $10,000.*

The above deliverables are provided using different modalities, such as renting, buying or leasing to respond to the client's needs. No doubt, despite different terms adopted to describe similar practices, the models behind them appear to be winning.

Trends and forecast:

Technologies such as mobile and social networking are increasingly threatened by cyber criminals. They're "adapting" consolidated attack methods to those platforms, and are defining new offensive strategies. *"The proliferation of mobile devices will lead to an amplification of abuse based on knowledge/attack vectors targeting to social media."* According to security experts and security firms, black market offers support the growth of cyber threats within the cyber crime ecosystem.

As reported in ENISA Threat Landscape, Mid Year 2013, the following top threats are candidates to dominate the criminal landscape in the medium term:

- **Drive-by-exploits:** Browser-based attacks still remain the most reported threats, and Java remains the most exploited software for this kind of threat.
- *Worms/Trojans:* Sophisticated malware is used by cyber criminals and governments for various purposes, such as offensive attacks, cyber espionage, and sophisticated cyber scams. Cyber crime makes extensive use of malware, especially for banking fraud. The mobile platform and social network situation is very concerning. Those platforms are exploited to spread large-scale malicious agents.
- **Code Injection: A**ttacks are notably popular against web Content Management Systems (CMSs). Due to their wide use, popular CMSes constitute a considerable attack surface that has drawn the attention of

cyber-criminals. Cloud service providing networks are increasingly used to host tools for automated attacks.

Botnets, Denial of Services, rogueware/scareware, targeted attacks, identity theft and search engine poisoning will continue to represent a serious menace to the IT community.[94]

18.3. Selected Asia-Pacific Cases:

1. In Australia's largest copyright infringement case, three university students received criminal sentences for running a Web site called MP3/WMA Land, which offered more than 1,800 pirated songs for download. In light of their age at the time and the fact that they never profited from their actions, the court warranted 18-month suspended sentences for two of the students and an additional fine of US$5,000 for one of them. Moreover, one student and a third participant were given 200 hours of community service.
2. Reportedly, China has become a leading exporter of counterfeit and pirated goods to the world. The U.S. industry estimates the value of counterfeit goods in China at US$19 billion to US$24 billion, with losses to U.S. companies exceeding US$1.8 billion a year. The severe piracy problems derive from a combination of cultural, historic and economic factors and are further aggravated by inconsistent, weak enforcement by officials. File-sharing Web sites and networks such as Jelawat and Kuro have been developing rapidly, too. The distributors of P2P software claim that file-sharing falls within the private use exception to copyright, but the Supreme People's Court of China rejected this interpretation. Increasingly, copyright owners and right organizations are challenging file-sharing Web sites on copyright infringement claims.
3. The Beijing No 1 People's Court ruled in April 2004 that the Web site chinamp3.com violated the IP rights of Hong Kong-based entertainment companies Go East Entertainment and Sony Music Entertainment (Hong Kong), and ordered the site to pay US$19,000 in damages. The suit concerned the unauthorized distribution of MP3 music files. The defendant argued that he had merely provided links for download and not a direct

[94] http://resources.infosecinstitute.com/2013-impact-cybercrime/

download service, and therefore should not be held responsible for the IP rights violations. According to observers, the court's ruling may prove to be a significant development in the nascent field of Chinese copyright enforcement in the digital age.

18.4. Indian Cases related to Cyber Crimes-I:

PARLIAMENT ATTACK CASE: Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at

Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal.

The emblems (of the three lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

State of Tamil Nadu Vs Suhas Katti: The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced the

accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.
The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.
Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved. Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on 5-11-04 as follows:

" The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

18.5. **Indian Cases related to Cyber Crimes-II:**

Baazee.com case: CEO of Baazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi

Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

Pune Citibank MphasiS Call Center Fraud: US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has froze

the accounts where the money was transferred. There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.[95]

18.6. Top Cyber Crime Stories-I[96]:

[95] http://www.cyberlawclinic.org/casestudy.asp

[96] http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-2014

1. Business needs to take cyber crime seriously, says top EU cyber cop Trowels Orting

Business needs to take cyber crime very seriously, according to Trowels Orting, head of Europol's European Cybercrime Centre.

"At some time or other, all businesses are likely to be hit by cyber crime as the world becomes increasingly online," Orting told Computer Weekly. "Companies that do not think information security is important should reconsider; otherwise they could end up going out of business."

The threat of cyber crime is much greater than most people think, he said, because much of it still goes unreported.

"We know of a lot of cyber crimes that are very costly to business that are not reported to the police," said Orting. "We also see losses through fraud and other crimes of more than €9m in some months, but these are going unreported."

Orting believes businesses that invest in the right processes, procedures and technologies will be rewarded in the longer term – but failure to do so could have devastating consequences.

2. Service model driving cyber crime, says Europol report

The cyber crime support industry is becoming increasingly commercialised, according to a report published by Europol's European Cybercrime Centre in September.

Specialists in the virtual underground economy are developing products and services for use by other cyber criminals, the *Internet Organised Crime Threat Assessment* (IOCTA) report said.

The report's authors believe this crime-as-a-service business model drives innovation and sophistication, and provides access to a wide range of services that facilitate almost any type of cyber crime. As a result, the barriers to entry for cyber crime are being lowered to allow those lacking technical expertise – including traditional organised crime groups – to conduct cyber crime.

The report also highlighted the abuse of legitimate services and tools such as anonymisation, encryption and virtual currencies, as well as the abuse of "darkness" for illicit online trade in drugs, weapons, stolen goods, stolen personal and payment card data, forged identity documents and child abuse material.

3. UK-led cyber crime taskforce proving its worth, says top EU cyber cop

Just one month into a six-month pilot, a UK-led international cyber crime looked set to become permanent, Trowels Orting, head of Europol's European Cybercrime Centre (EC3) said in October.

EC3 is hosting the Joint Cybercrime Action Taskforce (J-Cat) set up in September 2014 to co-ordinate international investigations with partners, targeting key cyber crime threats and top targets.

Initiated by EC3, the EU Cybercrime Taskforce, the FBI and the National Crime Agency (NCA), the J-Cat is made up of cyber liaison officers from EU states, non-EU law enforcement partners and EC3.

Oerting said the unit, which is led by deputy director of the UK's National Cyber Crime Unit (NCCU) Andy Archibald, is due for its first evaluation at the end of February 2015.

"There are already indications it will be extended for at least another six months, but I think it is likely to become permanent as it keeps acquiring cases and we are trying to get European Union (EU) funding for it," he said.

4. UK operation nets 17 suspected Blackshades cyber attackers

In May, the first-ever UK-wide cyber crime operation netted 17 suspected users of Blackshades malware, which is designed to take over control of computers and steal information.

Co-ordinate by the new National Crime Agency, the week-long operation in May involved nearly every UK regional organised crime unit as well as Police Scotland and the Metropolitan Police.

The UK investigation was part of global activity targeting developers and prolific users of Blackshades, a set of malware tools sold online for less than £100.

In an operation initiated by the FBI and co-ordinated in Europe through Eurojust and the European Cybercrime Centre at Europol, police forces internationally apprehended dozens of suspected users.

Arrests took place in the UK, the Netherlands, Belgium, Finland, Austria, Estonia, Denmark, Canada, Chile, Croatia and Italy, taking the total number of arrests in connection with Blackshades to 97. The most common Blackshades product is a remote access tool (Rat), which enables cyber criminals to remotely take over and control the operations of an infected computer.

5. Dark markets downed in international anti-cyber crime operation

International law enforcers took down several dark markets operating on hidden Tor networks and arrested 17 cyber crime suspects in early November.

Operation Ominous involved law enforcement officers from 16 European states and the US in one of the biggest anti-cyber crime operations to date.

The operation was aimed at halting the sale, distribution and promotion of illegal and harmful items, including weapons and drugs through dark marketplaces online.

Operation Onymous was co-ordinated from Europol's European Cybercrime Centre in The Hague and supported by the UK-led Joint Cybercrime Action Taskforce (J-Cat). Operation Onymous was J-Cat's second big success in just over a month of a six-month pilot, and came just weeks after Operation Imperium, which resulted in 31 arrests and 42 house searches.

18.7. Top Cyber Crime Stories-II[97]:

6. UK police make four arrests in international cyber crime crackdown

UK police made four arrests in late November as part of an international crackdown on cyber criminals who use malware tools to hijack computers and steal data. The UK raids were led by the NCA, and involved officers from a number of police Regional Organized Crime Units (ROCUs).

The international operation was co-ordinate through Europol, and focused on the threat posed by tools known as remote access Trojans.

Police in Estonia, France, Romania, Latvia, Italy and Norway made 11 further arrests. In the UK, two 33-year-old men and a 30-year-old woman were arrested in Leeds, and a 20-year-old man was arrested in Kent. Police executed a search warrant on a 19-year-old man from Liverpool, who had been brought in for voluntary questioning.

The NCA said that, in addition to arresting people believed to be using remote access trojans, police use a variety of approaches to warn individuals that any movement into cyber criminality will result in further action.

7. More than a hundred cyber criminals arrested in global operation

[97] http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-2014

Law enforcement agencies around the world arrested 118 suspects, including around 40 in the UK, in the third international cyber-crime operation of its kind in late November.

The operation was led by Europol's European Cybercrime Centre in The Hague and co-ordinate with the help of Interpol in Singapore and Ameripol in Bogota. The operation was aimed at tackling online fraud and was conducted in collaboration with the airline, travel and credit card industries.

More than 60 airlines and 45 countries were involved in the activity, which took place at more than 80 airports across the world. The co-ordinate action targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data. In many cases it was revealed how the credit card fraud has links to or is facilitating other forms of serious crime, such as drug trafficking.

8. UK National Cyber Crime Unit open to business

The UK's National Cyber Crime Unit (NCCU) is open to working with business and other organizations in the private sector, according to deputy director Andy Archibald.

"Business is welcome to contact us directly about dynamic, fast-moving cyber crime in action, and we will work with them to ensure they get the most appropriate response," he told Computer Weekly.

The NCCU sees a deeper, more defined and developed relationship with private sector businesses as crucial, not only to identify crimes and patterns of criminal activity, but also to tap into specialist skills.

"We need to be able to go to organizations in the private sector and ask to work with people with the skills we need in some of our investigations," said Archibald. "Industry can bring things to the table that we may not be aware of, and we will work with the private sector within the law if the solution to an operation is something the private sector can take the lead on."

9. UK police face steep learning curve on cyber crime

UK police face a steep learning curve in getting to grips with cyber crime, but several initiatives underway are geared to growing capability and capacity, the London Assembly's Police and Crime Committee's Online Crime Working Group heard in November.

The working group is gathering evidence on the response of the Metropolitan Police Service to cyber-enabled crimes. Asked whether policing is behind the

curve when it comes to tacking cyber-enabled crime, College of Policing CEO Alex Marshall said it is clear there is an inconsistent response to this threat.

"There is much catching up to be done," he said, with experienced officers increasingly having to deal with complex, online and cyber issues, which they were never originally trained for.

Marshall said the 18-month-old College of Policing plans to publish new national standards for online investigation and intelligence in 2015 to replace outdated standards published in 2010. The college has also developed a huge range of online training courses for police in England and Wales, as well as specific courses for different skill areas in cyber or online crime.

10. Cyber criminals set to become information dealers, says Web sense

Cyber criminals are set to become information dealers in the coming year, according to the top 10 cyber security predictions for 2015 by Web sense Security Labs.

Web sense principal security analyst Carl Leonard said criminals will use the sale of credit card numbers to fund the collection of a broader range of data about victims.

"The underground market is flooded with stolen credit card data, but that will help fund the collection of fuller, richer personal information sets about individuals," he told Computer Weekly.

These data sets will be far more lucrative than credit card details on the underground market and will include details of multiple credit cards, as well as regional, geographic, behavioral and personal data. Web sense expects this emerging trade in data sets on individuals will enable a new level of identity theft to enable fraud.

18.8. Indian Case Laws-I:

First conviction in India: A complaint was filed in by Sony India Private Ltd which runs a website called sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002,someone logged onto the website under the identity of Barbara Campa

and ordered a Sony Colour Television set and a cordless head phone.A lady gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit car agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless head phone.

The accused admitted his guilt and the court of Shri Gulshan Kumar Metropolitan Magistrate, New Delhi, convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cyber crime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.98

18.9 Indian Case Laws-II:

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail

98 http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Case_1_First_conviction_in_Ind

account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Edmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked. The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant her self to implicate the accused as accused alleged to have turned down the request of the complainant to marry her. Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court based on the expert witness of Naavi an other evidence produced including the witness of the Cyber Cafe owners came to the conclusion that the crime was conclusively proved.

The court has also held that because of the meticulous investigation carried on by the IO, the origination of the obscene message was traced out and the real culprit has been brought before the court of law. In this case Sri S. Kothandaraman, Special Public Prosecutor appointed by the Government conducted the case.

Honorable Sri.Arulraj, Additional Chief Metropolitan Magistrate, Egmore, delivered the judgment on 5-11-04 as follows:

"The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay

fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently."99

18.10 Indian Case Laws-III

The Additional District and Sessions Court here has upheld a lower court's verdict in the first cyber case filed in the State sentencing a Pentecostal Church priest and his son to rigorous imprisonment in 2006.

Disposing of the appeal filed by the priest T.S. Balan and his son, Aneesh Balan, against the order of the Chief Judicial Magistrate, on Wednesday, Additional District Judge T.U. Mathewkutty said it was time the government took effective measures to check the growing trend of cyber crimes in the State.The court upheld the magistrate's order sentencing the two to three-year rigorous imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the information technology (IT) Act; awarding six months rigorous imprisonment under Section 120(B) of the Indian Penal Code; and ordering one year rigorous imprisonment and imposing a fine of Rs. 10,000 under Section 469 of the code. The court revoked the sentence under Section 66 of the IT Act.

The cyber case dates back to January-February 2002 and the priest and his son became the first to be convicted of committing a cyber crime.

The two were found guilty of morphing, web-hosting and e-mailing nude picturof Pastor Abraham and his family.

Balan had worked with the pastor until he fell out with him and was shown the door by the latter. Balan joined the Sharo Pentecostal Churchlater.

The prosecution said the duo had morphed photographs of Abraham, his son, Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs with captions.

The morphed pictures were put on the web and the accused, who edited a local magazine called The Defender, wrote about these photos in his publication. Valsan received the pictures on the Internet and asked his father to file a complaint to the police. A police party raided the house of Balan and his son at Perumbavoor and collected evidences.

---

99 http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Case_1_First_conviction_in_Ind

The magistrate's verdict came after a four-year trial, for which the court had to procure a computer with Internet connection and accessories. The police had to secure the services of a computer analyst too to piece together the evidences. Twenty-nine witnesses, including the Internet service provider and Bharat Sanchar Nigam Ltd., had to depose before the court.100

18.11 Summary:

The issue of cyber crime can be understandable through case studies easily rather focus more on theoretical aspects. The issues related to cyber crime discussed through case studies of cyber crime in UK, selected Asia-Pacific cases, Indian cases related to cyber crime and top cyber crime stories and Indian case law are discussed for better understanding through proper illustration and examples.

18.12 Some Useful Books:

- Black Ice: The Invisible Threat of Cyber Terrorism by Dan Verton (Mc Graw Hill Professionals Publication)
- Cyber Crime and Cyber Terrorism by R.K. Pradhan (Mangalam Publication)
- Cyber Crime and Cyber Terrorism by Vinod Kumar Jayaswal (Neha Publishers and Distributors)
- Cyber Terrorism by S. Venkatesh (Authorpress)
- Crypto and Network Security by Khate (Mc Graw Hill Education (India) Pvt. Ltd.)
- Information Technology Act, 2000: A Conceptual Paradigm Shift in Law by Divya Chansoria and Rajeshwar Ashok Srivastava (Vista International Publishing House)
- Cyber Crime and Information Technology by Vikram Singh Jaswal (Regal Publication)

100 http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Case_1_First_conviction_in_Ind

- Guide to Cyber Laws (Information Technology Act, 2000. E-Commerce, Data Protection and the Internet) by Rodney D Ryder (Lexis Nexis-India)
- Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)
- Cyber Laws and IT Protection by Harsh Cander (PHI Publication)
- Introduction to Cyber Laws by Dr. J.P. Mishra (Central Law Publication)
- Cyber War and Terrorism by Mithilesh K. Singh (Prashant Publishing House)
- Cyber Terrorism: Political and Economic implications by Andrew M. Colarik (Idea Group Publishing)
- Cyber Terrorism and Law by S. Kaur, Anand Pawar & G. Kaur (Lambert Academic Publishing)
- The Fallacy of Net Neutrality by Thomas W. Hazlett (Encounters Books)
- Access to Broadband Networks: The Net Neutrality Debate (Create space Publication)
- Cyber Space and Cyber Security by Progressive Management (Progressive Management Publications)
- Computers, Privacy and Data Protection: An Element of Choice (Springer)
- All Relevant Website quoted at appropriate place in the study material for ready reference. The author is not claiming any right with reference to that quoted material.

18.13 Check your Progress:

A. Which of the following statements are true or false:

a) Stopping cyber crime can positively impact world economies.

b) The most important cost of cyber crime comes from its damage to company performance and to national economies.

c) Technologies such as mobile and social networking are increasingly threatened by cyber criminals.

d) The US industry estimates the value of counterfeit goods in China at US $ 19 billion to US $ 24 billion.
e) Law enforcement agencies around the world arrested 118 suspects, including around 40 in the UK, in the third international cyber-crime operation of its kind.

B. Fill in the Blanks:

I. In ……., the UK government documented in an official report that the overall cost of cyber crime economy was …….
II. Reportedly, China has become a …….of counterfeit and pirated goods in the world.
III. ……..was arrested in December, 2004 because a CD with objectionable material was being sold on the website.
IV. The cyber crime support industry is becoming increasingly ……...
V. ……., for example, actual hacking losses totaled $ 875 million but the recovery, or clean up costs reached $ 8.5 billion.

18.14 Answer to Check your Progress:

A.

1. True
2. True
3. True
4. True
5. True

B.

1. 2011; $ 27 billion a year
2. Leading Exporter
3. CEO of Bazze.com
4. Commercialized
5. In Italy

18.15 Terminal Questions

1. Discuss in detail cyber crime in UK.
2. Discuss selected Asia-Pacific cases.
3. Discuss Indian cases related to cyber crime-I.
4. Discuss Indian cases related to cyber crime-II.
5. Discuss top cyber crime stories.