CHAPTER 9

Cyber Security and Role of Social Media

9.1 What is Cyber Security?

Cyber security can be defined as the protection of systems, networks and data in cyber space. It refers to the preventative methods used to protect information from being stolen, compromised or attacked.

Cyber security is a complex issue that cuts across multiple domains and calls for multi-dimensional, multi-layered initiatives and responses. It has proved to be a challenge for governments because it involves various ministries and departments. It is more difficult primarily due to the diffused and varied nature of the threats and the inability to frame an adequate response in the absence of tangible perpetrators.

Cyberspace has expanded dramatically in its brief existence due to rapid development of information technology (IT) and commercial applications associated with it. Advances in information and communications technologies have revolutionised the scientific, educational and commercial infrastructures developed by the government. The IT infrastructure has become an integral part of the critical infrastructure which supports national capabilities such as energy, power grids, telecommunications, emergency communication systems, financial systems, defence systems, space, transport, land records, public essential services and utilities, law enforcement and security and air traffic control networks, to name a few. All these infrastructures increasingly depend on relay data for communication and commercial transactions. The operational stability and security of critical information infrastructure is vital for the economic security of the country.

The evolving nature of the telecommunications infrastructure poses further challenges. The expanding wireless connectivity to individual computers and networks is making determination of physical and logical boundaries of networks increasingly difficult. The increasing inter connectivity and accessibility to computer based systems that are critical to the country's economy are adding to the risk.

9.2 Cyber Threats

Cyber threats vary from simple hacking of an email to waging a war against a state. Cyber threats can be classified broadly into two categories:

1. Cyber crime: against individuals, corporates, etc.
2. Cyber warfare: against a state

9.2.1 Cyber Crime

Use of cyber space, i.e. computer, internet, cellphone, other technical devices, etc., to commit a crime by an individual or organised group is called cyber crime. Cyber attackers use numerous vulnerabilities in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. *DoS* attacks are used to overwhelm the targeted websites. *Hacking* is a common way of piercing the defences of protected computer systems and interfering with their functioning. *Identity theft* is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.

Cyber crimes may be divided into two categories:

1. Crimes that Target Computers Directly

They include:

- Spreading computer viruses
- Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. It temporarily or indefinitely interrupts or suspends services of a host connected to the internet.
- Malware (malicious code) is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software, for example Trojan Horses, rootkits, worms, adware, etc.

2. Crimes Facilitated by Computer Networks or Devices, the Primary Target of which is Independent of the Computer Network or Device

This can take many forms as listed below:

- Economic frauds to destabilise the economy of a country, attack on banking transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft and intellectual theft of property
- Impairing the operations of a website or service through data alteration, data destruction
- Spreading pornography
- Copyright infringement
- Cyber stalking, outraging modesty of women, obscene content to humiliate girls and harm their reputation
- Threatening e-mail
- Assuming fake identity, virtual impersonation
- Breach of right to privacy
- Misuse of social media in fanning intolerance, instigating communal tensions and inciting riots. Posting inflammatory material that tends to incite hate-crimes (Even Prime Minister Manmohan Singh expressed deep concern on misuse of social media in sparking off communal sentiments in September)
- Information warfare
- Phishing scams

➤ 9.2.2 Key Terms of Cyber Attack

- **Phishing**: Phishing is the act of attempting to acquire information, such as usernames, passwords and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social websites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging.
- **Vishing (Voice Phishing)**: The term is a combination of 'voice' and 'phishing'. When phishing is done with the help of telephonic system, it is called vishing.
- **Tabnabbing:** Tabnabbing is one of the latest phishing technologies. It takes advantage of tabbed browsing(which uses multiple open tabs) that a user uses and silently redirects the user to the affected site. This technique operates in reverse to most phishing techniques as it does not directly take the user to the fraudulent site, but, instead, phishers load their fake page in one of the open tabs.
- **Whaling**: Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

- **Spoofing:** A spoofing attack is a situation in which one person or programme successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. A spoofing attack involves one programme, system or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another programme. The purpose of this is usually to fool programmes, systems or users into revealing confidential information, such as user names and passwords, to the attacker.
- **Zombies:** A zombie is a computer connected to the internet that has been compromised by a hacker, computer virus or trojan horse. It can be used to perform malicious tasks under remote direction. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.
- **Botnets:** A botnet is a collection of internetconnected programmes communicating with other similar programmes in order to perform tasks.

  Botnets sometimes compromise computers whose security defences have been breached and control conceded to a third party. Each such compromised device, known as a 'bot', is created when a computer is penetrated by software from a malware (malicious software) distribution.
- **Pharming:** It is an attack to redirect a website's traffic to a different, fake website, where the individual's information is then compromised.
- **Drive-by:** These are opportunistic attacks against specific weaknesses within a system.
- **MITM:** 'Man in the middle attack' is an attack where a middleman impersonates each endpoint and is thus able to manipulate both victims.
- **Spam:** The unsolicited sending of bulk email for commercial purposes, is unlawful in some jurisdictions. While anti-spam laws are relatively new, limits on unsolicited electronic communications have existed for some time.

➤ 9.2.3 Cyber Warfare and Cyber Terror

It is said that future wars will not be like traditional wars which are fought on land, water or air. Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century.

While there is no agreed definition of cyber warfare but 'when any state initiates the use of internet based invisible force as an instrument of state policy to sabotage and espionage against another nation, it is called cyber war'. Attacking the information systems of other countries for espionage and for disrupting their critical infrastructure may be referred as cyber warfare. It includes hacking of vital information, important webpages, strategic controls and intelligence.

The attacks on the websites of Estonia in 2007 and of Georgia in 2008 have been widely reported. Although there is no clinching evidence of the involvement of a state in these attacks, it is widely held that in these attacks, non-state actors (for example, hackers) may have been used by state actors. Since these cyber attacks, the issue of cyber warfare has assumed urgency in the global media.

When an organisation, working independently of a nation state, operates terrorist activities through the medium of cyber space, it is generally called cyber terror.

Special Features of Cyber War Compared to Traditional War

1. **Independent theatre of war:** The development of the internet and low-cost wireless communication is the contemporary equivalent of what airplanes were a hundred years ago. Their use in economic, social and political transactions has increased at a rate that far exceeds the growth in airplane use over the last century. These technologies already play an important part in military operations in the traditional spheres of land, sea, air and the newer one of space. There are signs that they have been used for aggressive purposes by some states. There is also ample evidence of their use by criminals and terrorist groups. It is only a matter of time, like air power a hundred years ago, before cyberspace becomes an independent theatre of war.

   There is one important nuance in the treatment of cyberspace as a fifth potential theatre of war, along with land, sea, air and space. The use of cyberspace depends on physical facilities like undersea cables, microwave and optical fibre networks, telecom exchanges, routers, data servers, and so on. Protecting or attacking these is in the domain of the traditional arms of the military. Cyberspace, as an independent theatre of war, is about attacks that compromise the capability to use these facilities—they cannot be prevented by the security services in isolation.
2. **An undefined space (no specific areas):**The defence of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest. It is not possible for a country to ignore what is happening in any part of this space if it is to protect the functionality of the cyberspace relevant for its own nationals. Moreover, a key part of this space, the global internet system, is still under the control of one country. Hence, national defence and international cooperation are inevitably intermeshed. This means that a country's government must ensure coherence between its security policy and the diplomatic stance taken by it in multilateral and bilateral discussions on matters like internet and telecom governance, human rights related to information freedoms, trade negotiations on infotech services, and so on.
3. **Disguised attackers:** There is another feature of cyberspace that complicates the design of security structures and policies compared to the other theatres of conflict. In cyberspace, it is very easy for an attacker to cover his tracks and even mislead the target into believing that the attack has

come from somewhere else. This difficulty in identifying the perpetrator makes it difficult to rely on the capacity to retaliate as a deterrent.

4. **No Contact war:** The evolution of technology impacts the nature of conflict and war. Amongst the recent aspects of conflict is 'no contact war' wherein there is no 'physical' or 'kinetic' action across borders.

Future world war will most likely be cyber war. Future war will not be like traditional wars which were fought on territorial borders or in air space.

9.3 Snowden Revelations

Edward Joseph Snowden is an American computer professional, former employee of the Central Intelligence Agency (CIA) and former contractor for the National Security Agency (NSA).

He hogged international limelight when he disclosed to several media outlets thousands of classified documents. Snowden's release of classified material has been described as the most significant leak in US history. The US Department of Justice charged Snowden with espionage.

Snowden's leaked documents uncovered the existence of numerous global surveillance programmes; many of them run by the NSA with the cooperation of telecommunication companies and European governments. The massive extent of NSA's spying, both foreign and domestic, was revealed to the public in a series of detailed disclosures of internal NSA documents. In 2013, the existence of the 'Boundless Informant' was revealed, along with the PRISM electronic data mining programme, the XKeyscore analytical tool, the Tempora interception project, the MUSCULAR access point and the massive FASCIA database, which contains trillions of device-location records. In the following year, Britain's Joint Threat Research Intelligence Group was revealed, along with the Dishfire database, Squeaky Dolphin's real-time monitoring of social media networks and the bulk collection of private webcam images via the Optic Nerve programme.

The disclosures have fuelled debates over mass surveillance, government secrecy and the balance between national security and information privacy.

Modus Operandi of Widespread Cyber Snooping by National Security Agency (NSA)

Basically, three major players were used by the NSA:

- Different nations
- Domestic/foreign agencies
- Private players within and outside the USA

Data was collected through:

- Telecom operators from Global Optic Fibre Network
- Servers of US based internet giants like Google and Microsoft

- Hardware manufacturers like Cisco and Juniper
- Large scale Malware operations and Firewall
- Off the Air components, including Wi-Fi, GSM, CDMA and Satellite signals in alliance with Australia, New Zealand and South Africa
- Taps placed on undersea cables in South America, North of Africa and the Indian Ocean
- Monitoring international payments, banking transactions
- iPhones, Blackberry and Android operating system

Vulnerability of Indian Cyber Space

Documents leaked by NSA whistle-blower Edward Snowden indicate that much of the NSA surveillance was focused on India's domestic politics and its strategic and commercial interests, exposing India's vulnerability to cyber snooping in all sectors. India was fifth among targeted countries. The US has had a major influence on the development of cyberspace by virtue of the fact that much of the initial infrastructure and use was centred in that country and it continues to be a major force in its development and use. The US has thus been in a position to fend off periodic attempts to challenge its supremacy, and those times when it could not, it has been forced to shed some of its control.

➤ 9.3.1 Impact of Snowden Revelations

1. It will pave way for the 'Internet Governance Era'. Microsoft recently allowed foreign customers to have their personal data stored on servers outside America. Hence, the consequence of Edward Snowden's NSA leaks is that countries and companies would erect borders of sorts in cyberspace.
2. Following the shocking revelations about governments' widespread monitoring of global communications, it is clear that all facets of the cybersecurity world have been indelibly changed, from ordinary people having their eyes opened to what is really going on, to governments becoming ever-more distrustful of each other.
3. Some experts believe the technical details contained in documents leaked by Snowden had weakened the security situation in western countries, decreasing the level of security in the US and UK in particular. They feel the leaks were a 'gift' to allow terrorists to 'evade us and strike at will'. It is being said that as fallout of the revelations, Al-Qaeda has changed the way it communicates.
4. One of the biggest impacts Snowden has had on the world is that his leaks have led to an acceleration of cyber arms race around the world.

There is a greater awareness among the masses about the right to privacy. People have become conscious. Even Barack Obama, President of USA, conceded that those leaks triggered a passionate and welcome debate about American snooping.

9.4 Threat to India's Cyber Space

As is clear from Snowden's revelations, India's cyber space is almost unprotected. Till now, we only have very basic security features. We have started considering advanced features only after the Snowden revelations. All our vital institutions, installations and critical infrastructure need to be protected from cyber attacks.

The future war will target crucial areas like:

- Defence installations
- Sensitive documents related to both internal and external security
- Communication networks, including satellites
- ATC management
- Railway traffic control
- Financial services
- Premier institutions of science, technology and research

9.4.1 Critical Infrastructure (CI) and Critical Information Infrastructure (CII)

In general, critical infrastructure (CI) can be defined as:

'Those facilities, systems, or functions, whose incapacity or destruction would cause a debilitating impact on national security, governance, economy and social well-being of a nation.'

It broadly includes the following sectors:

- Energy
- Transportation (air, surface, rail and water)
- Banking and finance
- Telecommunication
- Defence
- Space
- Law enforcement, security and intelligence
- Sensitive government organisations
- Public health
- Water supply
- Critical manufacturing
- E-governance

Across the world, critical information infrastructure (CII) is broadly defined as including 'those networks which are interrelated, interconnected and interdependent'. In India, the guidelines would initially include information and communications, transportation, energy, finance, technology, law enforcement, security and law enforcement, government, space and sensitive organisations.

Critical Information Infrastructure (CII) are those ICT infrastructure upon which the core functionality of critical infrastructure is dependent.

India's new guidelines are an extension of the legislative recognition under the IT Act 2000. Section 70 of the Act defines critical information infrastructure (CII) as:

'Those computer resource and incapacitation or description of which, shall have debilitating impact on national security, economy, public health or safety.'

CII is highly complex, distributed, interconnected and interdependent.

Threats to CII

Threats to CII are classified as:

- *Internal threat*: It is defined as 'one or more individuals with the access and/or inside knowledge of a company, organisation or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products or facilities with the intent to cause harm'.

  Insider betrayals cause losses due to IT sabotage, fraud and theft of confidential or proprietary information. This may be intentional or due to ignorance.
- *External threat*: This threat arises from outside of the organisation, by individuals, hackers, organisations, terrorists, foreign government agents, non-state actors, and pose risk, like crippling CII, espionage, cyber/electronic warfare, cyber terrorism, etc.

Threat may be caused by individuals, including disgruntled or former employees, rivals (industrial espionage), hackers, script kiddies, crackers, cyber criminals (organised as well as unorganised), cyber mercenaries, terrorist groups (cyberjehadis), non-state actors and hostile states.

Effects of cyber attacks on CII:

- Damage or destruction of CII
- Disruption or degradation of services
- Loss of sensitive and strategic information
- Widespread damage in short time
- Cascading effects on several CII

9.5 Steps Taken by the Government of India

The following steps have been taken by the Government of India:

- The government has identified a list of critical computer infrastructure which need special protection against cyber attacks. Included in this list are networks related to national security, defence, banks, stock markets, power grids, railways and airlines, weather and many others.
- A national policy on cyber security was framed in 2013.
- A National Critical Information Infrastructure Protection Centre (NCIIPC) is in the process of being set up to create a fool-proof firewall around these networks.

- The creation of NCIIPC is just one of the many ideas being implemented as part of the Framework for Cyber Security that was recently approved by the Cabinet Committee on Security.
- A multi-agency National Cyber Coordination Centre to make assessment of cyber threats and share information with stakeholders is also being set up.
- A Centre of Excellence in Cryptology, the science of encrypting data, is being established at the Indian Institute of Statistics in Kolkata.
- Attacks on Indian networks have come mainly from computers based in 20 countries, including the US, UK, Germany, France, Brazil, Poland and the Netherlands. One such attempt tried to jeopardise the Delhi Commonwealth Games in 2010. Hackers had tried to get into the computer systems to tamper with the timers and scoring machines.
- The government had come up with a 'roadmap on cyber security', that has laid stress on collaboration between the government and private sector in this area.
- As a follow-up to that, the government has set up three cyber-forensic laboratories in Bangalore, Pune and Kolkata in association with the software industry group NASSCOM. Nine more such laboratories are planned in partnership with state governments.
- A cyber crisis management plan has already been put in place, with state governments as an integral part.
- CERT-In, or Computer Emergency Response Team (India), the nodal agency to deal with such crisis is being replicated on a smaller scale for specific sectors.
- The defence establishment has already set up a sectoral CERT for itself. Railways and the power sector are also planning to have a CERT of their own.

➤ 9.5.1 National Cyber Security Policy 2013

Department of Electronics and Information Technology (DeitY) under the Ministry of Communication and Information Technology, Government of India released the National Cyber Security Policy 2013 to build a secure and resilient cyber space for citizens, businesses and government.

The mission of this policy is to (1) protect information and information infrastructure in cyberspace, (2) build capabilities to prevent and respond to cyber threat, (3) reduce vulnerabilities and (4) minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

The objectives of this policy are defined below.

Objectives

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy

2. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology and people)
3. To strengthen the regulatory framework for ensuring a secure cyberspace ecosystem
4. To enhance and create national and sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions
5. To enhance the protection and resilience of nation's critical information infrastructure by operating a 24x7 **National Critical Information Infrastructure Protection Centre** (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources
6. To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing national security requirements
7. To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing and validation of security of such products
8. To create a workforce of 5,00,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training
9. To provide fiscal benefits to businesses for adoption of standard security practices and processes
10. To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft
11. To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention
12. To create a culture of cyber security and privacy enabling responsible user behaviour and actions through an effective communication and promotion strategy
13. To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace
14. To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace
15. To encourage all organisations, private and public, to designate a member of senior management as **Chief Information Security Officer** (CISO), responsible for cyber security efforts and initiatives

16. To encourage all organisations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage and transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure
17. To ensure that all organisations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents
18. To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security
19. To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions
20. To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts
21. To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

Main Features

The main features of the National Cyber Security Policy 2013 include:

1. To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture
2. To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices
3. To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement
4. To foster education and training programmes both in formal and informal sectors to support the nation's cyber security needs and build capacity
5. To establish cyber security training infrastructure across the country by way of public private partnership arrangements
6. To establish institutional mechanisms for capacity building for law enforcement agencies
7. To promote and launch a comprehensive national awareness programme on security of cyberspace
8. To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security
9. To create a think tank for cyber security policy inputs, discussion and deliberations

10. To develop bilateral and multi-lateral relationships in the area of cyber security with other countries
11. To enhance national and global cooperation among security agencies, CERTs, defence agencies and forces, law enforcement agencies and the judicial systems
12. To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems, including critical information infrastructure.

Assessment of National Cyber Security Policy (NCSP) 2013

- Security risks associated with Cloud Computing have not been addressed.
- There is also a need to incorporate cyber crime tracking, cyber forensic capacity building and creation of a platform for sharing and analysis of information between public and private sectors on continuous basis.

➤ 9.5.2 National Critical Information Infrastructure Protection Centre (NCIIPC)

The Government is setting up the National Critical Information Infrastructure Protection Centre (NCIIPC) which will function as a specialised unit under the National Technical Research Organisation (NTRO). Under Section 70A of the IT Act, NCIIPC, under NTRO, is being declared as the nodal agency for protection of critical information infrastructure of India.

NCIIPC, under its mandate from Section 70A(2) of IT Act, is responsible for all measures including research and development for protection of critical information infrastructure.

NCIIPC's vision is 'To facilitate safe, secure and resilient information Infrastructure for Critical Sectors of the Nation'.

NCIIPC mission is 'To take all necessary measures to facilitate protection of Critical Information Infrastructure from unauthorised access, modification, use, disclosure, disruption, incapacitation or destruction through coherent coordination, synergy and raising information security awareness among all stakeholders'.

Functions [C]

The functions of NCIIPC include:

1. Identification of critical sub-sectors
2. Study of information infrastructure of identified critical sub-sectors
3. Issue of daily/monthly cyber alerts/advisories
4. Malware analysis
5. Tracking zombies and Malware spreading IPs
6. Cyber forensics activities
7. Research and development for smart and secure environment
8. Facilitate CII owners in adoption of appropriate policies, standards, best practices for protection of CII

9. Annual CISO Conference for critical sectors
10. Awareness and training
11. 24X7 operation and helpdesk

NTRO has identified 17 sub-sectors initially and has started activities for 7 sub-sectors and organisations named below:

- Air traffic management (ATM), Civil aviation (Transportation)
- Power grid (Energy)
- MTNL
- NSEI
- BSNL
- Railways
- SBI

Each organisation/ministry in critical sector should nominate a Nodal Officer (CISO) for interaction with NCIIPC. CISO will be the point of contact for NCIIPC.

➤ Role and Responsibilities of Chief Information Security Officer (CISO)

CISO responsibilities include, but are not limited to:

- Build an Information security culture
- Assist senior management in the development, implementation and maintenance of an information security infrastructure
- Develop, communicate and ensure compliance with organisational information security policy, standards and guidelines
- Ensure regulatory and standards compliance
- Develop a security awareness and training programme
- Periodically conduct internal audit to check compliance with organisational security policy, standard and guidelines
- Risk management
- Incident management
- Business continuity management
- Assist senior management in acquisition of products, tools and services related to information and related technology

➤ 9.5.3 National Telecom Security Policy (NTSP)

NTSP has been formulated with a view to build-in the security features in the systems, services, technologies, equipment, devices and software rather than being an add-on feature. It is a structured policy to deal with issues related to the requirement of the security agencies and to secure the telecom network in the country. It deals with the four broad issues of communication assistance to security agencies, security of communication, information and data, security of telecom network and disaster management. NTSP puts emphasis on indigenisation of sophisticated telecom equipment so that they could be produced and installed in secure environment with all checks and balances.

➤ 9.5.4 Electronic System and Design and Manufacturing (ESDM) Sector Policy

Background of Electronics Industry

At the current rate of growth, domestic production can cater to a demand of USD 100 billion in 2020 as against a demand of USD 400 billion and the rest would have to be met by imports. This aggregates to a demand supply gap of nearly USD 300 billion by 2020. Unless the situation is corrected, it is likely that by 2020, electronics import may far exceed oil imports. This fact goes unnoticed because electronics, as a 'meta resource' forms a significant part of all machines and equipment imported, which are classified in their final sectoral forms, for example, automobiles, aviation, health equipment, media and broadcasting, defence armaments, etc.

Our electronic age is characterised by high velocity of technological change. Consequently, the lifecycle of products is declining. As a result, the value of design and development in the product has increased quite significantly. Given India's growing strength in chip design and embedded software, the increasing importance of design in product development has potential to make India a favoured destination for Electronic System and Design and Manufacturing (ESDM).

There is an urgent need for domestic production and design of electronic equipment.

India is one of the fastest growing markets of electronics in the world. There is potential to develop the ESDM sector to meet our domestic demand as well as to use the capabilities so created to successfully export ESDM products from the country. The National Policy on Electronics aims to address the issue with the explicit goal of transforming India into a premier ESDM hub.

The strategies include setting up of a National Electronics Mission with industry participation and renaming the Department of Information Technology as Department of Electronics and Information Technology (Deity).

Security Implications of ESDM Policy

The policy is expected to create an indigenous manufacturing ecosystem for electronics in the country. It will foster the manufacturing of indigenously designed and manufactured chips creating a more cyber secure ecosystem in the country. It will enable India to tap the great economic potential that this knowledge sector offers. The increased development and manufacturing in the sector will lead to greater economic growth through more manufacturing and consequently greater employment in the sector.

ESDM is of strategic importance as well. Not only in internal security and defence, the pervasive deployment of electronics in civilian domains such as telecom, power, railways, civil aviation, etc. can have serious consequences of disruption of service. This renders tremendous strategic importance to the sector. The country, therefore, cannot be totally dependent on imported electronic components and products.

The policy proposes the following strategies:

(i) *Creating ecosystem for globally competitive ESDM sector*: The strategies include provision of fiscal incentives for investment, setting up of electronic manufacturing clusters, preferential market access to domestically manufactured electronic products, setting up of semiconductor wafer fabrication facilities, industry friendly and stable tax regime. Based on Cabinet approval, a high level empowered committee has been constituted to identify and shortlist technology and investors for setting up two semiconductor wafer manufacturing fabrication facilities. Based on another Cabinet approval a policy for providing preference to domestically manufactured electronic goods has been announced. Separate proposals have also been considered by the Cabinet for approval of Modified Special Incentive Package for the ESDM Sector and for setting up of Electronics Manufacturing Clusters (EMCs).

(ii) *Promotion of exports*: The strategies include aggressive marketing of India as an investment destination and providing incentives for export.

(iii) *Human resource development*: The strategies include involvement of private sector, universities and institutions of learning for scaling up of requisite capacities at all levels for the projected manpower demand. A specialised institute for semiconductor chip design is also proposed.

(iv) *Setting up standards*: Developing and mandating standards to curb inflow of sub-standard and unsafe electronic products by mandating technical and safety standards which conform to international standards.

(v) *Cyber security*: To create a complete secure cyber ecosystem in the country, through suitable design and development of indigenous appropriate products through frontier technology/product oriented research, testing and validation of security of products.

(vi) *Strategic electronics:* The strategies include creating long-term partnerships between domestic ESDM industry and strategic sectors for sourcing products domestically and providing Defence Offset obligations for electronic procurements through ESDM products.

(vii) *Research and development*: Creating ecosystem for vibrant innovation and R&D in the ESDM sector, including nanoelectronics. The strategy includes creation of an Electronic Development Fund.

(viii) *Electronics in other sectors:* The strategy includes supporting and developing expertise in electronics in the following sectors of economy: automotive, avionics, light emitting diodes (LEDs), industrial, medical, solar photovoltaic, information and broadcasting, telecommunications, railways, intelligent transport systems and games and toys.

(ix) *Handling e-waste*: The strategy includes various initiatives to facilitate environment friendly e-waste handling policies.

9.6 Legal Framework

9.6.1 Information Technology Act 2000 (Amended in 2008)

Information technology Act 2000 consists of 94 sections segregated into 13 chapters. The Act was amended in 2008 which has now 124 sections. Salient features of the IT Act are as follows:

1. The Act provides legal recognition to e-commerce, which facilitates commercial e-transactions.
2. It recognises records kept in electronic form like any other documentary record. In this way, it brings electronic transactions at par with paper transactions in documentary form.
3. The Act also provides legal recognition to digital signatures which need to be duly authenticated by the certifying authorities.
4. Cyber Law Appellate Tribunal has been set up to hear appeal against adjudicating authorities.
5. The provisions of the IT Act have no application to negotiable instruments, power of attorney, trust, will and any contract for sale or conveyance of immovable property.
6. The Act applies to any cyber offence or contravention committed outside India by a person irrespective of his/her nationality.
7. As provided under Section 90 of the Act, the State Government may, by notification in 'Official Gazette', make rules to carry out the provisions of the Act.
8. Consequent to the passing of this Act, the SEBI had announced that trading of securities on the internet will be valid in India, but initially there was no specific provision for protection of confidentiality and net trading. This lacuna has been removed by the IT (Amendment) Act, 2008.

9.6.2 Offences under the IT Act

Sec-65. Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys, or alters any computer source code used for a computer, computer program, computer system or computer network, when the source code is required to be kept or maintained by law, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Sec-66. Hacking with Computer System

1. Whoever with the intent of cause or knowing that is likely to cause, wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.
2. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Sec-66-A Sending Offensive Messages through Communication Service, etc. (Introduced Vide Amendment in 2008)

Any person who sends, by means of a computer resource or a communication device,

(a) Any information that is grossly offensive or has menacing character; or

(b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device, or

(c) Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

9.7 International Cooperation in Cyber Security

9.7.1 NETmundial Conference 2014

Sau Paulo in Brazil hosted a two-day conference in April 2014 on internet governance. It included representatives from nearly 180 countries. Its theme was 'Global Multi-stakeholder Meeting on the Future of Governance'.

A global discussion on Net governance tried to bring the vision of multiple stakeholders in line with democracy. India took this opportunity to highlight US dominance of the internet and press for equal rights and say for all nations on matters related to Internet governance and cyber security. India lamented the lack of truly representative and democratic nature of the existing systems of internet governance, including the management of critical internet resources, and called for cyber jurisprudence to ensure security of the cyberspace.

There are three major issues here.

1. Should internet governance be carried out through a multilateral model or multi-stakeholder model? The multilateral model involves primarily Governments. UN is operated by this model.

   On the other hand, multi-stakeholder model recognizes that civil society groups, internet users and corporates have a say as well. Russia, India and China were in favour of multilateral model. 'Civil society' and Western countries are more inclined towards a multi-stakeholder set-up. While a multi-stakeholder option seems like the more reasonable and politically correct choice, it begs the question: Who are these civil society groups, who do they claim to represent, and how do we know that they simply haven't been hijacked by corporate interests?
2. The second issue is the question of internet fragmentation or 'Balkanisation' of the internet. Western countries and civil society groups fear that as countries such as India and Russia reduce their reliance on American

infrastructure, they will shatter the global unity of the internet and impose barriers that will hinder connections between users in different countries. While this fear is real, it also shuts us off to looking at a different type of Balkanisation; one where we reduce dependence on surveillance-tinged, Silicon Valley-based services while promoting local and secure digital infrastructure. In India, these fault lines are already being drawn, for better or worse: The Election Commission recently aborted a potential partnership with Google, for voter facilitation services, on the grounds of 'national security'. Government officials are slowly starting to shun Hotmail and Gmail as well. Technology start-ups like Wonobo, a Google Street clone, are starting to receive Government backing.

3. Third issue is 'net neutrality' or the principle that telecom companies should treat all internet content equally as it flows through their cables and pipes. If net neutrality is abandoned, internet service providers would be allowed to prioritise certain types of traffic, leading to disastrous consequences.

On most of these issues, and a few others such as intellectual property, NETmundial has scored poorly, mostly because vested interests often take root when the global community has to strive for 'rough consensus'.The conference's outcome document takes soft stances on validating the multi-stakeholder model and condemning surveillance. Net neutrality, for instance, is relegated to a 'point of future discussion'.

The proposal for a decentralised internet assumes significance in the wake of Edward Snowden's Wikileaks revelations of mass surveillance in recent months.

The US has had a major influence on the development of cyberspace by virtue of the fact that much of the initial infrastructure and use was centred in that country and it continues to be a major force in its development and use. The US has thus been in a position to fend off periodic attempts to challenge its supremacy, and those times when it has been forced to shed some of its control.

Bowing to the demands of Brazil and other nations following revelations last year of its massive electronic surveillance of internet users, the United States has agreed to relinquish oversight of the Internet Corporation for Assigned of Names and Numbers (ICANN), a non-profit group based in California that assigns internet domain names or addresses. The revelations by former NSA analyst, Edward Snowden, brought worldwide calls for the United States to reduce its control of the internet, created 50 years ago to link the computers of American universities to the US defence industry.

9.8 Social Media

Social media refers to internet based communication among people who create, share and exchange their ideas, photos, videos and information on virtual cyber platform. Its reach and popularity among people has rapidly increased over the last few years, primarily due to a sharp rise in the number of internet users and cell phone users. It is claimed that people spent more than 20% of the time spent on internet on social media. Nearly 20 crore people use internet in India. It is likely that it will soon overtake US as far as number of internet users is concerned. People freely exercise their right to express on social media as well as they get access to faster information and knowledge. Knowledge is power. Information is power. Social media includes Facebook, Twitter, Youtube, blogs, new microblogging sites, etc.

➤ 9.8.1 How is Social Media different from Traditional Media?

Social Media is a new form of media. It is different from traditional media in the following ways:

1. It rapidly passes information to its users. It is distinct from traditional media because it provides real time communication of information. Information on social media is widely spread within a very short time so its impact is much far than traditional print and electronic media and also far than traditional modes for communication, like telephone, postal and face-to-face communication.
2. Traditional print media and electronic media are controlled by big media houses. Their control is limited to a selected few. So they exercise their monopoly by influencing the masses, elections and politics through modified distorted version of news items. But social media is in the hands of people. It cannot be controlled by any individual or any group. So, social media has broken the monopoly of big media houses. Social media has ensured a greater transparency in traditional media. In fact, electronic media and print media are also becoming available on social media now.
3. Traditional media provides one-way communication. It only provides information to users but people discuss and debate on current issues, important policies, etc. on the social media. So, social media has not only enhanced transparency and accountability of the government, it has also made our democracy more participatory. It has developed a culture of debate that is the most important requirement for strengthening any democracy.

➤ 9.8.2 Negative Usage of Social Media

The negative usage of social media includes:

- Riots
- Misinformation
- Terrorism, anti-national activities
- False opinion building
- Addiction
- Inciting communal violence

9.8.3 Positive Usage of Social Media

The positive usage of social media includes:

- Social awareness
- Cheapest and fastest form of communication
- Spread of social activism like movements against corruption and sexual harassment, etc.
- Promoting a culture of debate and discussion
- Breaking the monopoly of big media houses
- Participatory democracy

9.9 Key Issues

Since the last 2-3 years, a debate has been going on regarding use / misuse of social media. On the one hand are the issues of freedom of expression and right of privacy, while on the other, are the issues of hurting religious sentiments, promoting hatred, enmity between different classes & groups, causing annoyance, criminal defamation etc. We know that there has to be a fine balance between the two, while freedom of expression envisaged in the Constitution is the right of individual but we have to exercise it within the limits of law and we have to see that we don't hurt others feeling which creates law and order problems for the administration. We have to take care of the rights of others also.

Two instances that got highlighted in the recent past are given below:

1. The arrest of two women over a comment on Facebook sparked off widespread anger in India. One of the women, in her Facebook post, had criticized the shutdown of Mumbai after the death of politician Bal Thackeray, while the other had 'liked' the comment. The women accused of 'promoting enmity between classes' were later released on bail. It sparked a nationwide debate of Section 66-A of IT Act 2000. The chairman of the Press Council of India Markandey Katju, also criticized the arrests. Later, the charges against the girls were withdrawn by the Government.
2. Aseem Trivedi, a cartoonist, was arrested on the charge of putting seditious cartoons on Facebook. Although his cartoons were related to corruption and the failure of the Parliament to deal with corruption, he faced serious allegations of insulting the national emblem, the Parliament, the flag and the Constitution through his anti-corruption cartoons. In January 2012, a case of sedition (Section 124A of the Indian Penal Code) was filed against him in the Beed District Court, Maharashtra. Additional charges were brought against him by the Maharashtra Police in Mumbai for insulting India's national symbols, under the State Emblem of India (Prohibition of Improper Use) Act 2005. He was arrested in Mumbai on September 9, 2012 on charges of sedition, related to the content of his work. This also faced lot of criticism by media.

PROBABLE QUESTIONS BASED ON THIS CHAPTER

1. Explain the following terms:
   (a) Phishing
   (b) Tabnabbing
   (c) Whaling
   (d) Spoofing
   (e) Zombies
   (f) Botnets
2. What are the basic features of the National Cyber Security Policy 2013?
3. What are social networking sites and what security implications do these sites present?
4. What is CII and how is it important for cyber security of India?
5. What are the salient features of NCIIPC?
6. What are the implications of Snowden revelations on cyber security of India?
7. What is cyber war? How is it different from a traditional war?