General Studies – 3; Topic: *Basics of cyber security*

Cyber Security in India

1) Introduction

- The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike.
- Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole.
- Cyber security threats pose one of the most serious economic and national security challenges.

2) Current status of Cyber Security preparedness

- The initiatives taken by the Government have focused on threats to critical information infrastructure and national Security, adoption of relevant security technologies, Information Security awareness, training and research
- Due to the dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time.
- Information Technology (Amendment) Act 2008 has been enacted to cater to the needs of National Cyber Security
- Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response.
- Growth and application of digital signature certificates in a number of areas.
- National Crisis Management Plan for countering cyber attacks and cyber terrorism has been prepared and is being updated annually.
- Security Auditors have been empanelled for conducting security audits
- R&D activities have been supported through premier Academic and R&D Institutions
- Nation-wide Information Security Education and Awareness Programme have been in progress to create necessary cyber security awareness

3) Cyber Security in Banking Sector

- As banking sector plays a crucial role in a country like India, a strong cyber security framework is necessary
- Threats like Phishing, Denial of cards, Credit card Frauds causes thousands and lakhs of money every day which causes huge financial risks and effects Indian economy.
- RBI aim of cashless transactions will be delayed and this goal can't be reached if such attacks keep repeating.
- **solution**
  a) Banks should immediately put in place a cyber-security policy to reduce threats.
  b) Sharing of cyber knowledge between IT industries and banking sector about emerging risks and creating awareness among staff and top employees about malware.
  c) Strengthening CERT-IN and penalizing banks if not informed immediately after cyber attacks
  d) Increasing security by recruiting special Cyber Investigation cell at police stations Eg: Cyberdome, Kerala and strict punishments on hacking
  e) Creating awareness among public about phishing, spam mails, wrong call from unknown users and online transactions services

4) Concerns / Challenges

- Frequent data breaches will steadily erode the confidence of Internet users and deter them from using digital gateways
- If the country's digital assets are today vulnerable to espionage and disruptive attacks, there are institutional, economic and social factors fuelling their neglect.
- The National Informatics Centre (NIC), which hosts the government's mail servers, has been compromised several times in the past
- Appointment of National Cyber Security Coordinator in 2014 has not been supplemented by creating liaison officers in the States
- The Computer Emergency Response Team (CERT-In) is woefully understaffed.
- The private sector fails to report and respond to breaches in digital networks.
- Most Indian applications available on Android and iOS stores allow for automatic updates or patches, increasing the likelihood that an exploit or malware can be introduced without the user's knowledge.
- Most Indian companies that rely on Gmail for official communication also do not make two-factor authentication (2FA) mandatory for its employees.
- Post-demonetisation, the Centre has pushed the citizenry to go 'cashless', without building capacity and awareness on the security of devices or transactions.

5) Solution

- Seamless integration of agencies involved in the area of cyber security
- Creating Centres of Excellence for research in identified areas of advanced security
- Setting up a mechanism to certify IT products to provide security assurance
- Establishing Security Information Sharing and Analysis Centres (ISACs) across the regions and sectors for government-to-private and private-to-private information sharing.
- Establishing Sectoral CERTs.
- Strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange.
- Setting up Cyber Security Help Desks at regional levels for general users to provide first level of guidance and support.
- Establishing Cyber Security Training Labs/facilities across the country in collaboration with State Governments and Private Sector
- Setting up of think tanks in Public-Private mode to identify gaps in the existing policy and frameworks and take action to address them.
- Launching formal Security Education, Skill Building and Awareness Programmes.