Security Class 05

23rd April, 2024 at 9:00 AM

DISCUSSION ABOUT PRELIMS (09:01 AM)

CYBERSECURITY (09:07 AM)

- According to the IT Act, cybersecurity is defined as securing computer devices, networks, and information stored on them from unauthorized access, disclosure, disruption, modification, or destruction.

CYBER THREATS FACED BY INDIA (09:42 AM)

- **1) Cybercrimes**
- These are defined as those crimes which are carried out in the cyberspace. For instance, hacking, phishing, denial of service (DoS) attacks, cyberstalking, child pornography etc.
- *Cyberspace has led to the creation of **para-social** relationships. Social relationships require two things: a) An intelligible awareness of the other - physical presence is not necessary here; b) This awareness should also exert an influence over the other.*
- **2) Cyber Terrorism**
- It refers to the use of cyberspace by terror outfits to carry out unlawful attacks/threats of attacks against computer networks, devices, or information to intimidate or coerce a government or its people toward the furtherance of their social or political objectives.
- **3) Cybre Warfare -** It is commonly defined as the use of offensive action by a nation-state against others. For example - The Stuxnet attack, is alleged to have emanated from Israel-USA against Iran's nuclear programs.
- Example - Operation Cuckoo Bees - spearheaded by the Chinese state actor APD 41 has allegedly stolen intellectual property worth trillions of dollars from 30 MNCs in the USA.
- Example - **Wiper Malware -** In 2022 ~~2017~~, Russian military intelligence hackers released the Notpetya worm to attack Ukraine's military establishments (Operation Acid Rain).

INDIA'S VULNERABILITY TO CYBER THREATS (10:03 AM)

- India is among the top 5 targets for cyber attacks in the Asia Pacific Region, especially cyber espionage.
- The reasons range from:
- 1) Increasing Internet penetration in India - Internet penetration in India was 4% in 2007 but was 45% in 2021.
- 2) India has also embarked upon massive digitalization across various spheres. For example - e-governance initiatives.
- 3) India has the biggest citizen identity program (Aadhar).
- 4) Electronic transfer of money is increasingly replacing cash transactions.
- ~~5)~~ This puts a sizeable chunk of India's population at risk of cybercrime, especially with a huge digital divide between its users.
- **These attacks have had severe implications:**
- 1) Cybercrimes in India led to siphoning off of roughly Rs. 1.25 Lakh Crores in 2019.
- 2) Personal details of 81 81 Crore Indians were leaked and put up on sale on the dark web, as a result of the attack on ICMR databank.
- 3) There was an alleged Chinese cyberattack on 5 AIIMS servers, compromising the data of nearly 3 to 4 crore patients.
- 4) In 2017, Petya ransomware disrupted shipping facilities at the Jawaharlal Nehru Port Trust.
- 5) In 2020, Mumbai was hit by a massive power outage and it is alleged that a few terror organizations were behind this attack.
- 6) 68% of organizations in India have had at least one instance of ransomware attacks. According to NCRB, there has been roughly a 25% increase in registered cybercrime in India from 2021 to 2022.

Stages of Cyber Attack (10:16 AM)

- **1) Planning** - The attacker selects the target and the particular weapon to be used
- **2) Reconnaissance** - The weapon is then introduced into the cyber environment where it looks for other vulnerabilities.
- **3) Replicate** - The weapon, post vulnerability identification, starts to replicate itself while being stealthy.
- **4) Assault** - The weapon starts its attack on the target. It may or may not remain stealthy in the system.
- **5) Obfuscate** - The weapon may either self-destruct or stay hidden.
- **6) Withdraw** - If both parties agree (as in the case of warfare), the weapon may then be withdrawn.

INDIA'S CYBER SECURITY ARCHITECTURE (10:39 AM)

- **1) Legal Front -** The ~~Information~~ IT Act, 2000. This act was brought into force to formalize electronic contracts and regulate online transactions. Initially, its aim was not to prohibit or control activities like cyber terrorism, cyber offenses, etc.
- Amendments were made to the Act in 2008 that introduced relevant provisions concerning cyber security. For instance - Section 43A puts the responsibility of protecting the personal information of users on private companies. The now-repealed Section 66A prohibited the act of publishing annoying/menacing information.
- Similarly, Section 66C is against Identity theft, Section 67B is against child pornography, 66F defines cyber-terrorism, etc.

2. Policy Front:

- **National Cyber Security Policy 2013-**
- a) This policy mentioned a five-year target for training and inducting 5 lakh cyber security professionals.
- b) Setting up a nodal agency for protecting critical information infrastructure -
- c) Giving financial incentives to private companies to strengthen cyber security practices.
- d) Establishing a 24x7 cyber security technology to proactively deduct and respond to cyber threats
- e) It mandates the development of IT Infrastructure according to the guidelines under ISO 27001.
- f) Mandates both public and private companies to hire a chief information officer (CIO)
- g) Promotes collaboration between industry and research facilities.
- 3) **~~2)~~ Institutional Front -**
- **a) National Critical Information Infrastructure Protection Centre (NCIIPC) -** This is India's nodal agency to create a safe and secure critical information infrastructure environment.
- **b) CERT-IN -** It is India's nodal agency for providing emergency response in case of cyber security incidents. This body also analyses and disseminates information to the relevant stakeholders.
- **c) I4C - Indian cyber crimes coordination center -** whose task is to coordinate response to cyber attacks
- **d) CSK - Cyber Swacchta Kendra -** It is a BOTNET and malware analysis center. It detects malicious programs and provides free tools to the citizens to remove them.
- **e) NCRP - National Cybercrime Reporting Portal -** This portal caters to complaints pertaining to cyber crimes.
- **f) National Information Board - NIB -** This body is the main policy agency in the context of cyber security. It will be headed by the National Security Advisor (NSA) and will be responsible for inter-ministerial coordination.
- **g) National Cybersecurity Strategy 2020.**

CHALLENGES (11:15 AM)

- **1) On the Legal front -** India does not have a dedicated procedural law ~~concerning~~ w.r.t IT offenses. In the absence of a dedicated procedural law, agencies have to rely on the Indian Evidence Act which is not fit for effective trials of cyber offences.
- The Bureau of Indian Standards (BIS) has laid down comprehensive guidelines concerning the collection and analysis of evidence but it has so far not received any legal backing.
- The last set of amendments to the IT Act was made in 2008. Cyberspace has evolved manifold ever since. Several offences have not been defined in the law making it difficult for agencies to catch hold of cyber criminals.
- **2) On the institutional front -** A lack of coherence between various institutions affects the effective enforcement of cyber security mechanisms.
- **3) Infrastructure -** India imports roughly 70% of its telecom equipment which makes cyber security vulnerable to bugs being introduced at the manufacturing stage itself.
- Most state forensic labs lack the technology to carry out effective investigations of cyber crimes.
- There is an increased over-dependence on external servers for data storage. At present, most tech companies store their data in servers located outside India.
- India spends a minuscule proportion of its GDP on Research and Development (R&D).
- **4) Policy-Related Challenges -** The national cybersecurity policy is outdated and India lacks a comprehensive cybersecurity doctrine.
- **5) Human Resources -** Agencies lack trained staff for carrying out investigations. The policy aim of creating 5 Lakh cybersecurity professionals remains unfulfilled.
- Delayed enactment of the Personal Data Protection legislation meant that there was no deterrence for misuse of personal information by public or private agencies.

TOPIC FOR NEXT CLASS - NAXALISM