Be Mains Ready

Examine India’s vulnerability to cyber threats, especially to its critical infrastructure, along with steps taken by the government in this regard. (250 words)

24 Jul 2019 | GS Paper 3 | Internal Security

Approach / Explaination / Answer

Approach

- Mention latest facts related to cyber security in the country.
- List the different areas vulnerable to cyberthreat and state the reasons behind it.
- Explain the impact on infrastructure.
- List the steps taken by government.
- Conclude by listing more steps that should be taken in this direction.

Introduction

India is one of the key players in the digital and knowledge-based economy, holding more than a 50% share of the world’s outsourcing market. Moreover, pioneering and technology-inspired programmes such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net, Startup India, Skill India and Smart Cities are propelling India towards technological competence and transformation.

- India is already the third largest hub for technology-driven startups in the world and its Information and Communications Technology sector is estimated to reach the $225 billion landmark by 2020.

However, cyberspace is increasingly becoming a key domain besides air, sea and land warfare. This is evident from the results of a recent survey, according to which cybersecurity continues to be a major issue in India with 76% organizations hit by online attacks in 2018.

- Therefore, innovation in technology, enhanced connectivity, and increasing integration in commerce and governance make it very important to protect citizens’ data confidentiality, integrity and privacy, public safety, business and economic development and national security.

Body

India’s Vulnerabilities to Cyber Threats

- Internet of Things is adding a new dimension to the cyber security issue by cross-networking of personal data devices, electronic health records, medical devices and hospital networks - creating

new opportunities for data theft, source code manipulation, and undetected access to target networks.

- **Large population, internet literacy and the rapid economic growth make India one of the most important countries from a cybersecurity aspect.**
- State sponsored cyber terrorism, non-state terrorist groups, corporate and individual hackvists are engaged in different crimes, espionage, theft of patents, and other information assets.
    - Nations such as Russia, China, Iran, North Korea have in the past used cyber capabilities as an effective geostrategic tool for espionage, propaganda attacks, to target critical infrastructure systems, for intelligence gathering, and to support political and military objectives.
- Dependence on AI systems for civilian industries and national security - exposes them to breach of privacy, reliability, manipulation and misuse -which can damage critical infrastructure. Critical infrastructure are the assets that are crucial for the functioning of the economy and society.

Vulnerabilities to Critical Infrastructure

- Critical infrastructure under the cyber threats are:
    - Agriculture and Food
    - Public Health
    - Energy: Power Plants and Power Grids
    - Telecommunication
    - Chemical industry
    - Banking and Finance Sector
    - Water
    - Transportation: Postal and Shipping
    - Information and Technology Databases

Steps Taken by the Government

- **Information Technology Act, 2000:** Regulates use of computer systems, computer networks and also data and information in electronic format.
- Protection and resilience of critical information infrastructure with the **National Critical Information Infrastructure Protection Centre** (NCIIPC) operating as the nodal agency.
    - NCIIPC has been **created under Information Technology Act, 2000** to secure India's critical information infrastructure. It is based in New Delhi.
- **National Cyber Policy, 2013** that aims to
    - Create a secure cyber ecosystem.
    - Create mechanisms for security threats and responses to the same through national systems and processes.
    - Secure e-governance by implementing global best practices, and wider use of Public Key Infrastructure.
- **National Computer Emergency Response Team (CERT-in)** functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.
- **Cyber Surakshit Bharat Initiative** was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **National Cyber security Coordination Centre (NCCC)** was established in 2017. Its mandate is to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
- **Information Security Education and Awareness Project (ISEA)–** raises awareness and provides research, education and training in the field of Information Security.
- **Online Cybercrime Reporting Portal:** To enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content.
- **Indian Cyber Crime Coordination Centre (I4C):** To handle issues related to cybercrime in the

country in a comprehensive and coordinated manner.

Way Forward: Steps to be Taken

- **Cyber Security Policy of 2013 must be reviewed** in the light of emerging cyber threats propagated by state sponsored international cyber terrorism, military espionage, corporate espionage and financial frauds by individual hackers and groups. The policy is incapable of resolving these issues now.
- Cyber security strategy must be able to **protect multiple digital intrusions at all levels:** military and corporate espionage, electronic attacks disrupting critical infrastructure, ICT and IoT systems and data privacy, integrity and security of its citizens.
- Currently the country has a number of agencies dealing with the issue of cybersecurity however, India needs to **set up a single point national cyber security agency overcome the multiplicity** in order to develop appropriate policy, strategy and action plan, linking key ministries.
    - The existing National Information Board (NIB), headed by the National Security Adviser (NSA), duly empowered, can play the role of an apex body in India.
- **Dissemination of best security practices, intelligence sharing, intrusion reporting and effective coordination** and partnership between private, corporate, government and international level organisations like the UN, the European Union and India's allies is the need of the hour.
- Institutions such as the NCC, NTRO, CERT should be **equipped with skilled manpower.**
- **Adequate funding should be provided** for strategic research and development. India must enhance its technological and investigative capabilities.

Conclusion

India has ranked 47 out of 165 nations on the Global Cybersecurity Index 2018, released by the International Telecommunication Union. This shows India's commitment to cybersecurity. Given the huge number of online users and continued efforts on affordable access, India can overcome the vulnerabilities to cyber threats by integrating **cybersecurity in every aspect of policy and planning.**