Mains Practice Question

Q. How do you evaluate the preparation of India against potential cyber-attacks? Suggest a few measures that should be put in place to curb this menace.

27 Oct, 2021 GS Paper 3 Internal Security

Approach

- Explain the concept of cybersecurity
- Discuss the measures in place to counter cyber-attack
- Mention the associated challenges
- Suggest measures to effectively curb the menace of cyberthreats

Introduction

Cybersecurity or information technology security is the technique of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. The evolution of technology has changed the nature of conflict and war. Operations are conducted in a covert manner using resources such as agents in the information domain to weaken or strike at an adversary to achieve political objectives.

The country's core assets such as power grids and financial and transport networks are fast getting connected to the internet and more official data is getting stored online. In order to safeguard the digital infrastructure, various initiatives have been taken by the government such as:

- A specialized unit called the Indian Computer Emergency Response Team (CERT-In) has been operationalised as a national nodal agency for responding to cyber security incidents as and when they occur.
- Government of India has enacted the Information Technology (Amendment) Act 2008, to cater to the needs of the National Cyber Security regime.
- In 2013, a National Cyber Security Policy was put in place. It was launched to integrate all the initiatives in the area of Cyber Security and to tackle the fast-changing nature of cybercrimes.
- Initiatives such as setting-up the National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC), and creating sector-specific Computer Emergency Response Teams (CERT) under CERT-In etc. have been implemented under the National Cyber Security Policy.
- The Government of India has formulated a National Crisis Management Plan for tackling cyber-attacks and cyber-terrorism. This plan is re-evaluated yearly and updated to tackle the changing landscape of cyber threats.
- Security Auditors are also empanelled for conducting security audits by both government and private companies.

Cybersecurity is a complex issue that cuts across multiple domains and calls for multi-dimensional, multilayered initiatives and responses. It has proved a challenge for government because:

- Different domains are typically administered through siloed ministries and departments.
- Inchoate and diffuse nature of the threats and the inability to frame an adequate response in the

absence of tangible perpetrators make policy formulation a difficult task.

- Private companies and banks do not report regularly about the cyber attack to the government organizations.
- There is a lack of awareness among the common people about cybersecurity, hence they fall prey to the attempts of the hackers.
- Frequent cyberattacks erode the trust of customers on digital platforms and hamper India's dreams of becoming a cashless economy.
- Growth in online radicalization is another area of concern. Cyberspace has no physical boundaries for extremists and terrorists, unlike traditional warfare.

Certain measures that can address the menace of cyberattacks can be as follows:

- The Cyber Coordination Centre should be established at the operational level. This centre would serve as a clearing-house, assessing information arriving in real-time and assigning responsibilities to the agencies concerned, as and when required.
- The government should initiate a special drive of implementing best practices in the field of cybersecurity in the critical infrastructure sectors and provide necessary budgetary support for such implementation.
- The government should establish a mechanism for measuring the preparedness of critical sectors against potential cyberattacks such as a security index, which captures preparedness of the sector and assigns a value to it.
- Awareness with regard to the threat to Information and Communication Technology (ICT) infrastructure needs to be created and the necessary legal provisions to ensure cyber safety must be developed, regularly updated and effectively implemented.
- Cybersecurity should be regarded as an integral component of national security. Urgent attention should be given to the issues of cybercrime, cyberterrorism, cyber warfare etc.