National Cyber Security Strategy

written by iasexam.com | 17/12/2022

Topic- Internal Security [GS Paper-3]

Context- The National Security Council Secretariat (NSCS) formulated a draft National Cyber Security Strategy which looks at addressing the issue of security of national cyberspace.

National Cyber Security Strategy

- The strategy is headed by Lt General Rajesh Pant.
- The strategy proposes a separate legislative framework for cyberspace and the creation of an apex body to address threats, responses and complaints.
- It will focus on both threat assessment and response.

Need for the Policy

- The existing legal and regulatory frameworks have failed to address the evolving threat scenarios or processes to combat the cyber incidents.
- There is no specific body to look after cyber security at present and no one that you can hold accountable.
- Presently, the response to cyber security threats can be taken under the information technology act and the Indian Penal Code.

Other provisions:

- Its objective is to create a comprehensive system with both state-owned and private companies having to comply with cybersecurity standards.

- It also provides for a periodic cyber audit and recommends annual reviews by the apex body that will be created.
- A centre of excellence will be set up in Bangalore to further innovations in the area.

Some Important data on cyber security

- Till November 2022, a total 12,67,564 cyber security incidents were reported.
- In 2021, in total 14,02,809 such events were recorded as compared to 11,58,208 in 2020 and 3,94,499 in 2019.
- Ransomware attacks jumped 51% in 2022 and Maharashtra was the most targeted state in India facing 42% of all ransomware attacks.
- Cyber thieves exploited legitimate tools like “AnyDesk” used for remote administration.

Reasons for increasing Cyber Attacks

- **Adverse relations of the country with China**
    - China is often considered one of the world leaders in information technology.
    - Therefore, it is expected to possess capabilities to disable or partially interrupt the information technology services in another country.
    - Combined with the recent border standoff and violent incidents between the armies of the two countries, the adversity in relations is expected to result in attacking each other’s critical information infrastructure.
- **Asymmetric and covert warfare:**
    - Unlike conventional warfare with loss of lives, cyber warfare is covert warfare with the scope of plausible deniability, i.e., the governments can deny their involvement even when they are caught.
    - Even a small nation with advanced systems and skilled resources can launch an attack on a bigger power, without the fear of heavy losses.

- **Increasing dependency on technology:**
    - With the faster growth, more and more systems are being shifted to virtual space to promote access and ease of use.
    - However, the downside to this trend is the major vulnerability of such systems to cyber-attacks.

Issues with Cyber Security

- **Low digital awareness**:
    - While India is considered the world leader in the technology industry, the general level of awareness in India about the internet is very low.
- **Vulnerable points in the system**:
    - Sometimes the third-party apps have built-in back door entry or may have malware attached to their installation files and such issues can be addressed by effective user account control and careful monitoring of the system.
- **State-sponsored Cyber Attacks:**
    - The issue with such state-sponsored attacks is the unlimited funding received by

    - the hackers to break into the foreign systems.
- **Continuous process:**
    - Cyber-attacks, by their very nature, are innovative and creative and they continue to evolve, and the next attack is more advanced than its previous version.
- **Novel issues:**
    - Due to the ever-changing and fast evolving nature of technology, new issues keep creeping up in the IT sector.

Way Ahead

- The government aims at ensuring an open, safe, trusted and accountable Internet for its users.
- The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures to protect computers and networks on an ongoing basis.
- CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) in order to detect malicious programmes and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.
- Security tips have been published for users for the purpose of securing their desktops and mobile phones and to prevent phishing attacks.
- CERT-In and the Reserve Bank of India [RBI] together carry out a cyber security awareness campaign on ‘Beware and be aware of financial frauds’ through the Digital India Platform.
- The Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs (MHA) has been delegated as the nodal point in the fight against cybercrime.
- Pursuant to the United Nations General Assembly resolution 75/282 is an ad-hoc committee to elaborate a ‘Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes’ was established with all the member states.
- India being the member of the committee has proposed criminalisation of cyber terrorism under the Convention.
- The MHA has also issued National Information Security Policy and Guidelines to the Central Ministries as well as State governments and Union Territories with the aim of preventing information security breaches and cyber intrusions in the information and communication technology infrastructure.