AIR Spotlight: Cyber Security In India: Preparedness, Threats and Challenges

AIR Spotlight is an insightful program featured daily on the All India Radio Newsonair. In this program, many eminent panellists discuss issues of importance which can be quite helpful in IAS exam preparation.

This article is about the discussion on **"Cyber Security In India: Preparedness, Threats and Challenges".**

Participants:

1. Pavan Duggal, Cyber Security Expert
2. Ravi Kumar, AIR Correspondent

Context: Recently, several services at the All-India Institute of Medical Sciences (AIIMS) were crippled by a ransomware attack.

Introduction:

- On November 23, e-services at the All-India Institute of Medical Sciences (AIIMS) were crippled by ransomware attacks.
- Pending sanitisation of the entire network and its nodes, all hospital services are currently being executed manually.
- Cyberattacks on healthcare have grown across the world as more hospitals and healthcare services providers are moving their operations and databases online.
- According to cybersecurity firm CheckPoint Research, healthcare suffered the highest number of ransomware attacks globally during the September quarter of 2022.
- With one of the lowest data tariffs in the world, Internet users in India have more than doubled to 76.5 crore users over the past five years with a massive 6.5 times growth in 4G data traffic.
- Around 346 million Indians are engaged in online transactions including e-commerce, and digital payments, according to a report published by the Internet and Mobile Association of India (IAMAI).
- According to the National Crime Records Bureau (NCRB) data, India reported 52,974 cases of cybercrime in 2021, an increase of over 5 per cent from 2020 (50,035 cases) and over 15 per cent from 2019 (44,735 cases).

How serious are ransomware attacks?

- In recent times, there have been numerous reports of ransomware attacks in India that targeted critical and commercial infrastructure.
    - In May 2022, Spicejet faced such a threat, while Public Sector Undertaking Oil India was targeted in April 2022.
- In its third-quarter global report, the cybersecurity company Trellix identified 25 of the most prevalent ransomware.
- Ransomware ranked second after money laundering in the first-ever Interpol Global Crime Trend report, which was issued at its 90th General Assembly meeting in Delhi recently. Additionally, it is anticipated to rise the most (72%).

Cyber Security Preparedness of India:

- Cyber capabilities are now considered an essential element of national power. Increasing dependency on the digital ecosystem highlights the need for secure cyberspace in the country.
- India has been taking steps, such as creating agencies, developing doctrines and pursuing diplomatic collaborations with like-minded strategic partners, to ensure that deficiencies in the cyber security domain could be addressed.
- The initiatives taken by the government of India have focused on threats to critical information infrastructure and national security, adoption of relevant security technologies, information security awareness, training and research.
- The Information Technology (Amendment) Act 2008 has been enacted to address 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.
- National Crisis Management Plan for countering cyber attacks and cyber terrorism has been prepared and is annually updated.
- CERT-In, Reserve Bank of India (RBI) and Digital India jointly carry out a cyber security awareness campaign on ‘beware and be aware of financial frauds’ through the Digital India Platform.
- To strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Ministry of Home Affairs has provided financial assistance to all the States & UTs under Cyber Crime Prevention against Women & Children (CCPWC) scheme to support their efforts for setting up of cyber forensic-cum-training laboratories and training.
- The government is operating the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

India's cybersecurity threat:

- India is one of the fastest-growing markets for digital technologies fuelling the government's push towards actualising its Digital India mission.
  Whether creating broadband highways or rolling out services such as DigiLocker and e-governance schemes like the Jan Dhan Yojana, the government has pushed for as much digital adoption as possible over the past five years.
- From payments to e-shopping to WFH, the pandemic led to greater adoption of interconnected devices and hybrid work networks. Consequently, this vast and rapid expansion of digital assets has increased the surface area for cyber-attacks by malicious actors and adversaries.
- A number of electronic equipment in India are imported. It remains unknown whether these devices are tampered with or programmed for control processes. Hence, there is a need for much more rigorous testing of such equipment.
- The private sector in India fails to report and respond to security breaches in digital networks, even though it remains a prominent player.
- It is difficult for policymakers to navigate to draw up concrete policies as cybersecurity laws involve several different moving parts.

Way Forward:

- India needs a single nodal agency to enforce strict laws and penalise entities if they fail to step up their cybersecurity investments.
  - Currently, there are multiple government agencies, both at the state and national levels.
- A national cybercrime cell that can leverage resources to tackle threats and breaches is necessary.
- Business organisations and companies must also bear some of the responsibility of creating defences against acts of cybercrime. Organisations must bring on board cybercrime experts to put in place guidelines and SOPs in case of a cybersecurity threat.
- Government must integrate cybersecurity with its national agenda and weave it into broad initiatives, both strategic and socioeconomic.
- A robust cybersecurity strategy that safeguards government systems, citizens, and the business ecosystem will help protect citizens from cyber threats and also boost investor confidence in the economy.