Cyber Safety and National Security

For Prelims: Cyber Security, Indian Cyber Crime Coordination Centre, CERT-In

For Mains: Cyber Safety threat, Government Initiatives for Cyber Safety

Why in News?

Recently, the **National Conference on Cyber Safety and National Security** concluded in New Delhi.

- The conference is **part of the efforts to create mass awareness** for the prevention of cybercrimes in the country.
- It is also part of the **Azadi Ka Amrit Mahotsav** to celebrate India's progress and achievements in the 75th year of India's Independence.

What is Cyber Safety?

- **About:**
  - A set of activities and other measures intended to **protect cyberspace networks, related hardware and devices software, and the information they contain and communicate**, including software and data from all threats **including threats to national security.**
- **Relation with National Security:**
  - Since **Cyber-armies** have been formed to launch cyberattacks against India, **cyber security** is closely connected to national security.
    - A **cyber-army** is a **group of soldiers highly skilled in information technology** with cyber skills.

What's upping India's Cyber Safety threat?

- **Digital India Vision:**
  - 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 **Digi Locker** and **e-governance** schemes like the **Jan Dhan Yojana**, the government has pushed for as much digital adoption as possible.
    - Under **Pradhan Mantri Jan Dhan Yojana** 45 crore new accounts have been opened and 32 crore RuPay Debit Cards have been distributed in the last 8 years.
    - **BharatNet** is also developing very fast, 5.75 lakh km of fiber cable has been laid and work has been done to connect 1.80 lakhvillages in the last 8 years which was less than 10,000 8 years ago.
- **Increasing footprint of Digital activities:**
  - **India now has over 1.15 billion phones and more than 700 million internet users** and makes it a large pool of digitally vulnerable targets.
    - In January 2020, India had the **second largest Internet user base with over**

550 million Internet users.
- In 2021, **40% of the total global digital payments took place in India.**
- Digital Inclusion increases the potential of digital threats leading to cyber-attacks and crimes.

What distinguishes Cybercrime from Traditional Criminal Activity?

- **Cybercrime**, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and **intellectual property** stealing identities or violating privacy.
    - Most **cybercrime is an attack on information about individuals, corporations, or governments.**
    - Although the attacks **do not take place on a physical body as traditional criminal activity, they do take place on the personal or corporate virtual body,** which is the set of informational attributes that define people and institutions on the Internet.

What are the challenges behind Cyber Safety?

- **Service Providers:**
    - Rush towards digitisation in almost every sector has led to increased collaborations with application service providers. This is done **to provide customers with the best apps and services in the shortest possible time.**
    - Hardware and software being of foreign origin or the terabytes of data that is parked on servers outside India serve a potential threat to National Cyber space.
- **Wide Coverage:**
    - India has now more than 700 million internet users and makes it a large pool of digitally vulnerable targets. Considering our nation's size and scale, it serves as a challenge to monitor and suspect digital threats.

What are the Present Government Initiatives for Cyber Safety?

- **Cybercrime portal:**
    - It aims to enable citizens to report online content pertaining to **Child Pornography/ Child Sexual Abuse Material or sexually explicit content such as Rape/Gang Rape** (CP/RGR).
- **Indian Cyber Crime Coordination Centre (I4C):**
    - The prevention of cybercrimes is being handled through seven pillars under **I4C and CIS Division of Ministry of Home Affairs -**
    - **National Cyber Crime Threat Analytics Unit**
    - **National Cyber Crime Reporting Portal**
    - **National Cyber Crime Training Centre**
    - **National Cyber Crime Research and Innovation Centre**
    - **Joint Cyber Crime Coordination**
    - **National Cyber Crime Ecosystem Management Unit**
    - **National Cyber Crime Forensic Laboratory**
- **CERT-In:**
    - India's national agency for cybersecurity, **The Indian Computer Emergency Response Team** (CERT-In), has led to a reduction in cyber-attacks on government networks due to its advancements in tackling the nation's cybersecurity.
- **Cyber Surakshit Bharat:**
    - It is an initiative from the **Ministry of Electronics and Information Technology (MeitY)** that aims at creating a robust cybersecurity ecosystem in India. This aligns with the government's vision for a **'Digital India'. The National E-Government Division (NeGD) sponsored this program.**
- **Cyber Swachhta Kendra:**
    - It is an installation under the **Ministry of Electronics and Information Technology (MeitY)** aims to create secure cyberspace for Indian users by detecting botnet infections and enabling end-users to clean their systems and secure their systems thereafter to

prevent further infections.

- **Personal Data Protection Bill:**
    - Worldwide data breaches served a threat to personal security for Indian citizens, the PDP Bill was approved by the union government **to protect them from global breaches, focusing on localised data.**

Way Forward

- To achieve the goal of **cyber-secure nation**, India will require a robust **cybersecurity strategy** that safeguards government systems, citizens, and the business ecosystem. This will not only help protect citizens from cyber-threats, but also boost investor confidence in the economy.
    - The university and school curriculum must also emphasise **cybersecurity as a high-decibel awareness** subject.
    - Pressure also needs to be put on officials in the public domain to carry out **regular vulnerability assessments** and **create necessary awareness** of the growing cyber threat.
    - A dedicated industry forum for cyber security should be set up to develop trusted **indigenous solutions to check cyber-attacks.**

Source: PIB