NEXT IAS

DAILY EDITORIAL ANALYSIS

TOPIC

GROWING CYBERCRIME & NEED FOR AN INDIAN CYBERSECURITY FORCE

GROWING CYBERCRIME & NEED FOR AN INDIAN CYBERSECURITY FORCE

Context

- India's G-20 Sherpa and former NITI Aayog CEO recently unveiled a report highlighting that over 1,16,000 cybersecurity incidents were reported in 2023, a significant increase from previous years.
- The rising prevalence of cyber threats underscores the urgent need for robust cybersecurity measures.

About the Cyber Crime

- It is the **use of digital technologies** such as computers and the internet **to commit criminal activities.**
- It includes **financial fraud** *(credit card fraud, online transaction fraud),* **crime against women and children** with regard to **sexually explicit material, and deep fake content** etc.

Do You Know?

- Cyber Crime is **not defined in Information Technology Act 2000** nor in the I.T. Amendment Act 2008 **nor in any other legislation in India.**
- However, the IT Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber crime.
- It is interpreted as **any offence or crime** in which a **computer is used is a cyber crime.**

Types of Cyber Fraud

- **Phishing Attacks:** Fraudsters use deceptive emails and websites to steal sensitive information such as passwords and credit card details.
- **Identity Theft:** Criminals obtain personal information to impersonate individuals, leading to financial and reputational damage.
- **Online Scams:** These include lottery scams, job frauds, and fake online shopping websites that trick victims into parting with their money.

Trends: Rising Threat

- **Global**: About 5.5 billion malware attacks annually and 6.3 trillion attempted breaches — an average of 6.5 attacks every second.
  - By August 2024, nearly 60% of businesses globally had experienced a ransomware attack.
  - The demand for cybersecurity professionals has surged in the South Asian region and the ***'Five Eyes' countries*** *(Australia, Canada, New Zealand, the United Kingdom, and the United States)*, driven primarily by rapid digital transformation.
- **In India** alone, a company falls victim to cyberattacks **every 11 seconds.**
  - Ransomware poses a significant threat, with **eight out of ten enterprises** confirming that they have experienced such attacks.
  - Further, **almost 40% of large enterprises in India** have fallen victim to phishing **email-led attacks.**
- The Indian cybersecurity market is projected to grow at a **Compound Annual Growth Rate (CAGR)** of 18.33% from 2024 to 2029, reflecting increased investment in cybersecurity measures by financial institutions.

Key Factors Contributing to the Rise of Cybercrime

- **Increased Internet Penetration:** The widespread availability of affordable smartphones and low-cost data plans has significantly increased internet usage in India.
- **Rapid Digital Transformation:** The shift towards digital platforms for business, governance, and personal use has created more opportunities for cybercriminals.
- **Financial Incentives:** Cybercrime offers lucrative financial rewards, making it an attractive venture for criminals.
- **Lack of Cybersecurity Awareness:** Many individuals and organizations are still not fully aware of the best practices for cybersecurity, making them vulnerable to attacks.
- **Data Privacy Concerns:** The increasing amount of personal and sensitive data online has made data breaches more impactful and damaging.

Need for a Dedicated Cybersecurity Force

- **Shortage of Skilled Professionals:** There is a significant shortage of trained cybersecurity professionals in India. A dedicated force would help bridge this gap by providing specialized training and resources.
  - India is home to nearly one-third of the world's graduates in **science, technology, engineering, and mathematics (STEM)**.
  - However, 30% of the 40,000 job vacancies for cybersecurity professionals in 2024 remain unfilled due to talent shortages.
  - The current market for skilled talent offers a valuable opportunity for bolstering national security and enhancing economic growth.
- **Advanced Threat Detection and Response:** A specialized cybersecurity force would be equipped with the latest technology and methodologies to detect and respond to cyber threats more effectively.
- **Coordination and Collaboration:** A centralized force would facilitate better coordination between various government agencies, private sector entities, and international partners to combat cybercrime.
- **Public Awareness and Education:** This force could also focus on raising public awareness about cybersecurity best practices and the importance of data protection.

Key Legislative Measures Combating Cyber Fraud in India

- **Information Technology Act, 2000 (IT Act):** It provides legal recognition for electronic transactions and aims to facilitate e-commerce and addresses various cybercrimes, including hacking, identity theft, and cyber terrorism. Key sections relevant to cyber fraud include:
  - **Section 66C:** Punishment for identity theft.
  - **Section 66D:** Punishment for cheating by personation using computer resources.
  - **Section 43:** Penalty for damage to computer systems.
- **Indian Penal Code (IPC), 1860:** It includes provisions that address cyber fraud like:
  - Section 420: Cheating and dishonestly inducing delivery of property.
  - Section 468: Forgery for the purpose of cheating.
  - Section 471: Using as genuine a forged document.
- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:** These rules mandate intermediaries, such as social media platforms, to exercise due diligence and ensure the safety and security of users.
  - They require intermediaries to report cyber incidents to the **Indian Computer Emergency Response Team (CERT-In).**

Regulatory Bodies and Initiatives

- **Indian Cyber Crime Coordination Centre (I4C):** Established under the **Ministry of Home Affairs**, I4C aims to combat cybercrime in a coordinated manner.
  - It provides a platform for law enforcement agencies to collaborate and share information on cybercrime.
- **Cyber Swachhta Kendra:** This **initiative by CERT-In** focuses on creating awareness about cybersecurity and providing tools to detect and remove malicious software from devices.
- **National Cyber Security Policy, 2013:** It outlines strategies to protect the public and private infrastructure from cyber threats. It emphasises the need for a secure and resilient cyberspace.
- **National Cyber Crime Reporting Portal:** It allows citizens to report various types of cybercrimes, including financial fraud and crimes against women and children.
- **Cyber Crime Awareness Campaigns:** The government regularly conducts awareness campaigns to educate the public about safe online practices.

Related Global Efforts

- **Budapest Convention:** It is the 1st international treaty to address cybercrime.
  - **India is not a signatory to the treaty.**
- **Internet Corporation for Assigned Names and Numbers (ICANN):** It is a US-based not-for-profit organisation for coordinating & maintenance of several databases.
- **Internet Governance Forum:** It is the **United Nations forum** for multi-stakeholder policy dialogue on Internet governance issues.

Conclusion and Way Forward

- As cybercrime continues to evolve, the need for robust cybersecurity measures becomes imperative.
- Establishing an Indian cybersecurity force would not only enhance national security but also contribute to economic growth and the well-being of its citizens.
- It is time for India to take decisive action and build a resilient cybersecurity framework to safeguard its digital future.

Source: TH

Mains Practice Question

Discuss the escalating threat of cybercrime in India and analyze the urgent need for a dedicated and robust Indian cybersecurity force to effectively combat these challenges.