MAINS iMPACT 2026 **23-02-2026**

CYBER SECURITY

SYLLABUS:

GS 3 > Security > Cyber Security

REFERENCE NEWS:

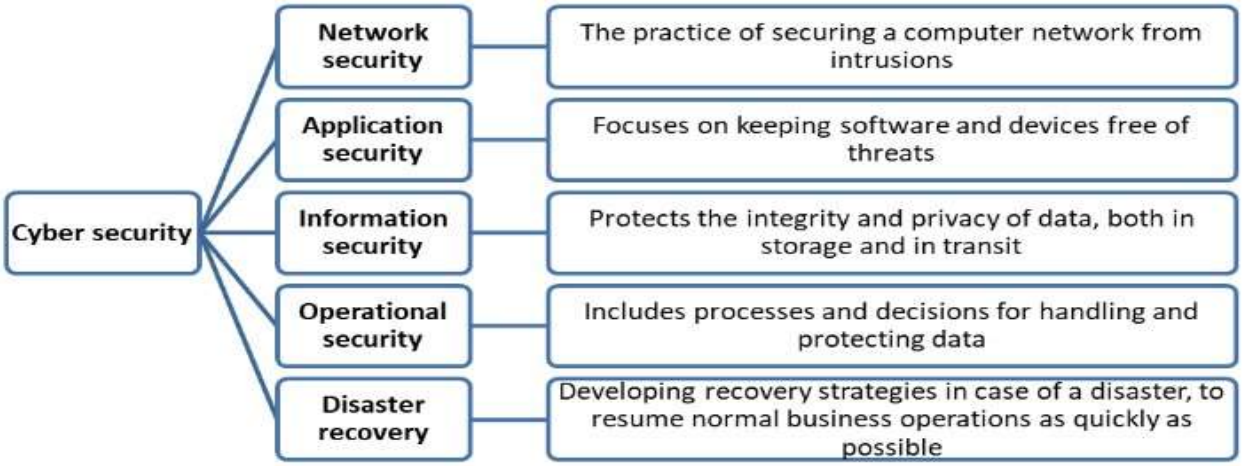
- **Investment scams** accounted for m**ore than 75 percent of the money Indians lost to cybercrimes in 2025**, even as overall financial losses saw a marginal decline from the previous year, data sourced from the Ministry of Home Affairs shows.

MORE ON NEWS:

- In 2025, Indians **lost ₹22,495 crore to cyber fraud**, slightly lower than ₹22,845 crore in 2024. However, reported cases rose sharply **from 22.68 lakh to 28.15 lakh**. FIRs declined, as quicker bank and police intervention helped block funds before formal cases were registered.
- **Investment scams dominated** the landscape, accounting for 76% of total financial losses. These included Ponzi schemes, fake stock trading platforms and cryptocurrency frauds. Though they formed about 35% of cases, they caused the highest monetary damage.
- **Digital arrest scams accounted for 9% of losses, while sextortion made up 19% of cases but a smaller share of total money lost.**
- The Centre has strengthened enforcement through the Indian Cyber Crime Coordination Centre (I4C), expanded **cybercrime police stations, and real-time reporting systems** that have helped block thousands of crores in fraudulent transactions.
- The trend shows that while cybercrime is expanding in scale and sophistication, financial containment mechanisms are also improving.

WHAT IS CYBER SECURITY?

- Cyber security **involves the techniques of protecting computers, networks, programs and data** from unauthorized access or attacks that are aimed for exploitation.
- The concept includes **guidelines, policies, safeguards, technologies, tools and training** to provide the best protection for the cyber environment and its users.



TYPES OF CYBER ATTACKS:

Cyber-attacks compromise the security of individuals, organizations, or nations in cyberspace. They can be categorized into:

- **Cyber Espionage**: Illicit access to confidential information through networks, often targeting governments or organizations (e.g., 2019 Kudankulam nuclear plant attack).
- **Cyber Crime**: Criminal activities using computers or networks, often for financial gain or to spread malware or illegal content.(e.g., The 2016 breach of over 3.2 million debit cards due to malware at Hitachi Payment Services affecting customers of banks like State Bank of India.)
- **Cyber Terrorism**: Attacks on computers or networks intended to intimidate or coerce governments or people, advancing political or social objectives.(e.g. Threats by extremist groups to target Indian critical infrastructure networks)
- **Cyber Warfare**: Actions by nation-states to damage or disrupt another nation's networks for espionage or conflict, seen as the fifth domain of warfare. (e.g. The 2020 Mumbai power outage, where investigations suggested possible Chinese state-linked cyber probing amid India-China border tensions)

RECENT EXAMPLES OF MAJOR CYBER-ATTACKS IN INDIA:

- **Digital Arrest Scam Surge (2024–25)**: A new wave of scams involving impersonation of police, CBI and ED officials through video calls led to significant financial losses across states.
- **Telecom Data Breach (2024)**: Data of 750 million Indian telecom users, including Aadhaar details, was compromised and sold online, prompting a DoT security audit.
- **AIIMS, 2023:** The systems at AIIMS and its centers were corrupted by the cyberattack, which wiped outpatient and research data from its primary and backup servers.
- **Attack on Air India (2021)**: Cyber attackers compromised data of 4.5 million customers, exposing sensitive information like passport and credit card details.
- **Kudankulam Nuclear Power Plant Malware Attack (2019)**: A malware attack targeted the administrative network, compromising its systems.
- **Aadhaar Data Leak (2019)**: Personal information of 6.7 million Aadhaar users was exposed in a massive data breach.
- **WannaCry & Petya Ransomware Attacks (2017)**: These global ransomware attacks locked down thousands of systems in India, affecting government utilities and organizations.

- **Scorpene Submarine Data Leak (2016)**: Confidential details of India's Scorpene-class submarines were leaked, raising serious national security concerns.

STATISTICS:

- India's digital ecosystem has grown rapidly under Digital India, **with over 86% of households connected to the internet.** With **1.2 billion mobile subscribers and 970 million internet users**, cyberspace now supports crores of daily transactions. (Source: PIB)
- However, this expansion has widened the attack surface. Cybersecurity incidents **increased from 10.29 lakh in 2022 to 22.68 lakh in 2024**, reflecting both rising threats and improved reporting mechanisms. (Source: PIB)
- Cyber frauds reported on the National Cyber Crime Reporting Portal (NCRP) resulted in **financial losses amounting to ₹36.45 lakh crore** (as per report data up to February 2025).
- In the **Global Cybersecurity Index (GCI) 2024** by the **International Telecommunication Union (ITU)**, India achieved **Tier 1 status**, ranking among 46 countries recognized for strong commitments in legal measures, technical advancements, capacity development, and cooperation.

SIGNIFICANCE OF CYBER SECURITY:

- **Increasing Internet Use in India**:
  - India's digital ecosystem has grown rapidly under Digital India, **with over 86% of households connected to the internet.** (Source: PIB)
  - **With 1.2 billion mobile subscribers and 970 million internet users,** cyberspace now supports crores of daily transactions**.** This substantial growth in digital activity amplifies the need for enhanced cyber security to safeguard against rising threats in cyberspace.
- **Increasing Digitization in India**:
  - Initiatives like **Digital India**, **Land records digitization**, **Aadhaar**, and the **cashless economy** increase the need for secure cyber architecture.
  - For instance, as per data from the **Union Home Ministry (2024)**, **46% of the world's digital transaction volume** now takes place in India.
  - UPI-based frauds and compromised mobile numbers have prompted the launch of the **Financial Fraud Risk Indicator (FRI)** by DoT to classify suspicious numbers.
- **Constitutional Obligations**:
  - After the **K.S. Puttaswamy v. Union of India (2017) verdict**, the state is obligated to protect citizens' **right to privacy**, making cyber security essential.
- **Economic Value of Data**:
  - The rise of **big data**, **AI**, and **social media marketing** makes data more valuable, heightening vulnerabilities in cyberspace.

- **AI-enabled deepfakes, spoofing and phishing** have amplified risks, turning personal data into a primary target for organised cybercrime networks.

- **Rise in Cyber-Crimes**:
  - Cyber-crimes like **WannaCry ransomware**, the **Stuxnet attack**, and the **Scorpene submarine leak** are on the rise.
  - For instance, an **Android device** experienced an average of **three cyberattacks per month** in India in 2023, the India Cyber Security Threat report published by the **Data Security Council of India (DSCI)** revealed.
  - **Over 9.42 lakh SIM cards and 2,63,348 IMEIs linked to cyber fraud have been blocked**, indicating the scale of telecom-enabled cybercrime.
- **Critical Infrastructure**:
  - Protection of critical infrastructure like **Aadhaar**, **NATGRID**, and **nuclear plants** depends on robust cyber security.
  - CERT-In conducted 109 mock drills involving 1,438 organisations (March 2025), while NCIIPC continues to monitor and protect critical sectors.

> **NCIIPC (National Critical Information Infrastructure Protection Centre)** is the national nodal agency under the National Technical Research Organisation (NTRO), designated under Section 70A of the IT Act, 2000, responsible for protecting India's critical information infrastructure from cyber threats.

- **Cost of Cyber-Attacks**:
  - The financial impact of cyber-attacks continues to rise globally and in India.
  - According to the **2023 IBM Cost of a Data Breach Report,** the average cost of a data breach in India reached **₹179 million (₹17.9 crore),** an all-time high and a 28% increase since 2020.
  - Cyber fraud losses in India stood at **₹22,495 crore in 2025**, despite improved real-time intervention and fund blocking mechanisms.

MEASURES TAKEN TO IMPROVE CYBER SECURITY:

Institutions:

- National Critical Information Infrastructure Protection Centre (NCIIPC)
- National Cyber Security Coordinator (NCSC)
- Computer Emergency Response Team (CERT-In)
- Defence Cyber Agency (DCA)
- Indian Cyber Crime Coordination Centre (I4C)
- Cyber Swachhta Kendra
- National Technical Research Organization (NTRO)
- National Cyber Coordination Centre (NCCC)

Policies:

- National Cyber Security Strategy 2020
- National Cyber Security Policy 2013
- Cyber Crisis Management Plan (CCMP)

Surveillance:

- Central Monitoring System (CMS)
- Network Traffic Analysis (NETRA)
- National Intelligence Grid (NATGRID)
- National Cyber Crime Reporting Portal (NCRP)

- 1930 Cybercrime Helpline
- Financial Fraud Risk Indicator (FRI) by DoT

Legal Framework:

- Information Technology Act, 2000
- Indian Telegraph Act, 1885
- Personal Data Protection Bill replaced by DPDP Act, 2023
- Section 70A IT Act – statutory basis for NCIIPC protection of Critical Information Infrastructure
- Promotion and Regulation of Online Gaming Act, 2025

Global Cooperation:

- Convention on Cybercrime (Budapest Convention)
- Paris Call for Trust and Security in Cyberspace
- Global Centre for Cybersecurity (WEF)

CONCERNS IN CYBER SECURITY:

- **Lack of Awareness**: According to cybersecurity experts, **80% of cybercrime frauds** occur due to a lack of cyber hygiene and awareness. Rise in AI-based deepfakes and digital arrest scams shows citizens are vulnerable **not just technically, but psychologically.**
- **Digital Growth and Vulnerability**: The rapid expansion of the digital space due to the pandemic has exposed vulnerabilities. **During COVID-19**, overuse of social media and online financial activity led to an increase in cybercrimes. **Investment scams accounted for 76% of financial cyber losses in 2025**, reflecting high-value targeting of new digital investors.
- **Weak Digital Security**: India's outdated infrastructure and weak cybersecurity measures, as seen in the **Aadhaar data leakage** and **Scorpene submarine leak**, highlight the lack of robust protections. Despite the Digital Personal Data Protection Act, 2023, enforcement capacity and data auditing mechanisms are still evolving.
- **Institutional Issues**: With **36 central bodies** handling cyber issues, there is a lack of clear institutional boundaries and accountability, which limits coordination. Absence of a fully operational **National Cyber Security Strategy** (draft pending formal release) adds policy ambiguity.
- **Private and Public Sector Collaboration**: The private sector has not been sufficiently engaged in cybersecurity initiatives, despite being a major stakeholder. **Growing dependence on UPI, fintech and telecom networks** requires deeper regulatory–industry coordination, especially after large-scale SIM and mule account misuse.
- **Lack of a Cyber Security Doctrine**: India lacks a comprehensive cyber deterrence strategy, which leaves it vulnerable to low-scale cyber operations by state and non-state actors.
- **Service Hub Vulnerability**: India's large IT and service sectors, along with initiatives like **Digital India**, attract both investment and cybercriminals.
- **Cryptocurrency Risks**: The rise in cryptocurrency use, especially Bitcoin, has fueled the growth of the ransomware industry.
- **Resource Shortage**: India faces a shortage of trained cybersecurity professionals and lacks the hardware and software capabilities for robust cyber defense. In 2020, India had a shortfall of **1.5 million cybersecurity professionals**.
- **Anonymity of Cybercriminals**: The anonymity of cybercriminals and offshore servers hinder law enforcement efforts.
- **Regulatory Shortcomings**: The **IT Act, 2000**, is outdated and struggles to address modern cyber threats. The tussle between the government and tech companies like Twitter on intermediary

guidelines also hampers effective cybercrime management. Though DPDP Act 2023 strengthens data protection, sector-specific cyber regulation remains fragmented.

- **External Attacks**: Examples like **Shadow Network** (China), **Suckfly** (China), **Dtrack** (targeting Indian banks and Kudankulam nuclear plant), and spying concerns with **Huawei** and **ZTE** highlight external threats.
- **Obsolete Systems**: India's reliance on cheap electronic imports with inadequate security features and rampant use of unlicensed software makes the country vulnerable to attacks.
- **Jurisdictional Uncertainty**: The transnational nature of cybercrimes complicates the application of domestic laws, leading to enforcement challenges.
- **Reliance on Chinese Equipment**: Telecom sectors rely heavily on Chinese equipment, with companies like **Bharti Airtel** and **Vodafone Idea** having significant portions of their networks composed of Chinese components. Blocking of over 9.42 lakh SIM cards and 2.63 lakh IMEIs linked to fraud highlights telecom-layer exploitation.

WAY FORWARD:

- **Cyber-Security Doctrine**: India needs a clear cyber-security doctrine to enhance stability and transparency in cyber defense.
- **National Cyber Security Commission (NCSC)**: Establish an NCSC to coordinate with ministries on critical infrastructure and cyber warfare.
- **Human Resource Development**: Cybersecurity jobs are expected to rise, creating opportunities for **1 million jobs by 2025**. Investment in skill development is key.
- **Digital Education**: Incorporate cybersecurity awareness into school curriculums and expand the **Digital India** campaign to enhance public knowledge. Include awareness on **deepfake threats** and misuse of AI tools like FraudGPT and WormGPT in social engineering.
- **Atmanirbhar in Cyber Systems**: Boost indigenous electronics manufacturing and tighten monitoring of imports to ensure security.
- **Private Sector Collaboration**: Improve coordination between the private sector and government agencies to enhance cyber defense.
- **Zero-Trust Security**: Organizations should adopt a **zero-trust** approach, requiring strict identity verification for all users.
- **Cutting-Edge Technologies**: Encourage research in **AI** to enhance threat detection and response automation.
- **Cyber Deterrence**: Strengthen India's cyber warfare capabilities to confront threats from adversarial nations and non-state actors.
- **Cyber Safety for Children**: Develop child-safe digital spaces to ensure safe online education and digital awareness.
- **Upgrade Cyber Cells**: Establish dark web and social media monitoring cells to improve the capabilities of existing cyber cells.
- **Address Gender Gap**: Promote gender diversity in the cybersecurity workforce to address the projected shortage of **3.5 million professionals** by 2025.

Case Study: Kerala's Cyberdome Project

- Cyberdome is Kerala Police's cybersecurity initiative aimed at preventing cybercrime. It brings together ethical hackers, law enforcers, and volunteers to enhance cyber safety.

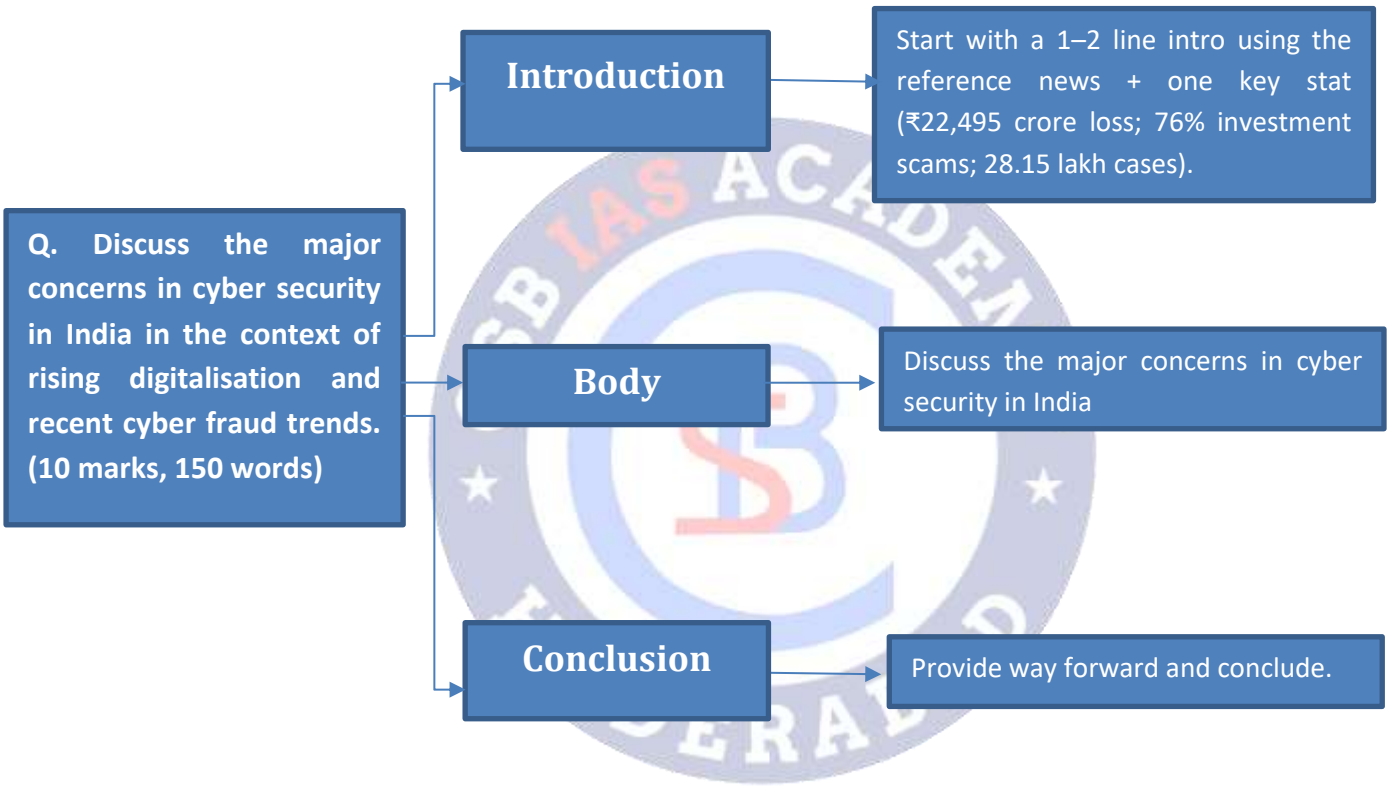
CONCLUSION:

- Cyber security is now central to India's national security and digital economy. While enforcement capacity and legal frameworks have strengthened, rising AI-enabled frauds, investment scams and critical infrastructure risks demand stronger coordination, cyber literacy, skilled manpower and indigenous technological capability to secure Digital India.

PRACTICE QUESTION:

Q. Discuss the major concerns in cyber security in India in the context of rising digitalisation and recent cyber fraud trends. (10 marks, 150 words)

APPROACH:



MODEL ANSWER:

India's expanding digital ecosystem has significantly increased cyber vulnerabilities. In 2025, Indians lost **₹22,495 crore to cyber fraud**, with **investment scams accounting** for **76% of total losses**, even as reported cases rose to 28.15 lakh (MHA data). This highlights the growing scale and sophistication of cyber threats amid rapid digitalisation.

Major Concerns:

1. Surge in Financial Cyber Frauds: High-value investment scams, digital arrest frauds and sextortion indicate organised and psychologically targeted crimes.

2. Expanding Digital Attack Surface: With 86% of households online and India handling 46% of global digital transactions, exposure to cyber risks has multiplied.

3. AI-Enabled Threats: Deepfakes, spoofing and phishing increase manipulation risks and erode trust in digital platforms.

4. Institutional Fragmentation: Multiple agencies and absence of a fully operational National Cyber Security Strategy create coordination gaps.

5. Regulatory and Legal Gaps: The IT Act, 2000 is outdated, and sector-specific cyber regulation remains fragmented despite the DPDP Act, 2023.

6. Skill and Infrastructure Deficit: Shortage of cybersecurity professionals and dependence on foreign telecom equipment increase systemic vulnerabilities.

7. Critical Infrastructure Risks: Threats to banking, telecom, Aadhaar and nuclear facilities elevate cyber security to a national security issue.

Way Forward

- Operationalise a clear and time-bound National Cyber Security Strategy with defined institutional roles
- Establish stronger inter-agency coordination through a unified cyber command framework.
- Modernise the IT Act, 2000 to address ransomware, AI-enabled fraud and deepfakes; ensure effective DPDP Act enforcement.
- Strengthen public–private collaboration in banking, fintech and telecom with mandatory breach reporting and threat sharing.
- Build indigenous cyber capabilities in telecom hardware, encryption and secure digital infrastructure.
- Bridge skill gaps through a national cybersecurity workforce mission and specialised training.
- Protect critical infrastructure through regular audits, zero-trust architecture and red-team exercises.

While initiatives like **I4C, CERT-In drills, NCRP portal and the 1930 helpline** have improved real-time response, sustained institutional clarity, skilled manpower and technological self-reliance are essential to secure India's digital future.