Building a Resilient Cybersecurity Framework for India

For Prelims: Digital threats, Artificial Intelligence, Deep fakes, WannaCry ransomware attack, Phishing, Internet of Things, National Cyber Security Policy, Indian Cyber Crime Coordination Centre, Computer Emergency Response Team - India , Cyber Swachhta Kendra , Digital Personal Data Protection Act 2023.

For Mains: Current Major Cyber Threats that India is Facing, Key Government Initiatives Related to Cybersecurity in India.

Source: ET

Why in News?

The **Parliamentary Standing Committee on Home Affair**s underscored the escalating **cyber threats** in India, calling for **greater public awareness,** enhanced **cyber safety**, and stronger **digital security** as internet penetration and online transactions rapidly expand.

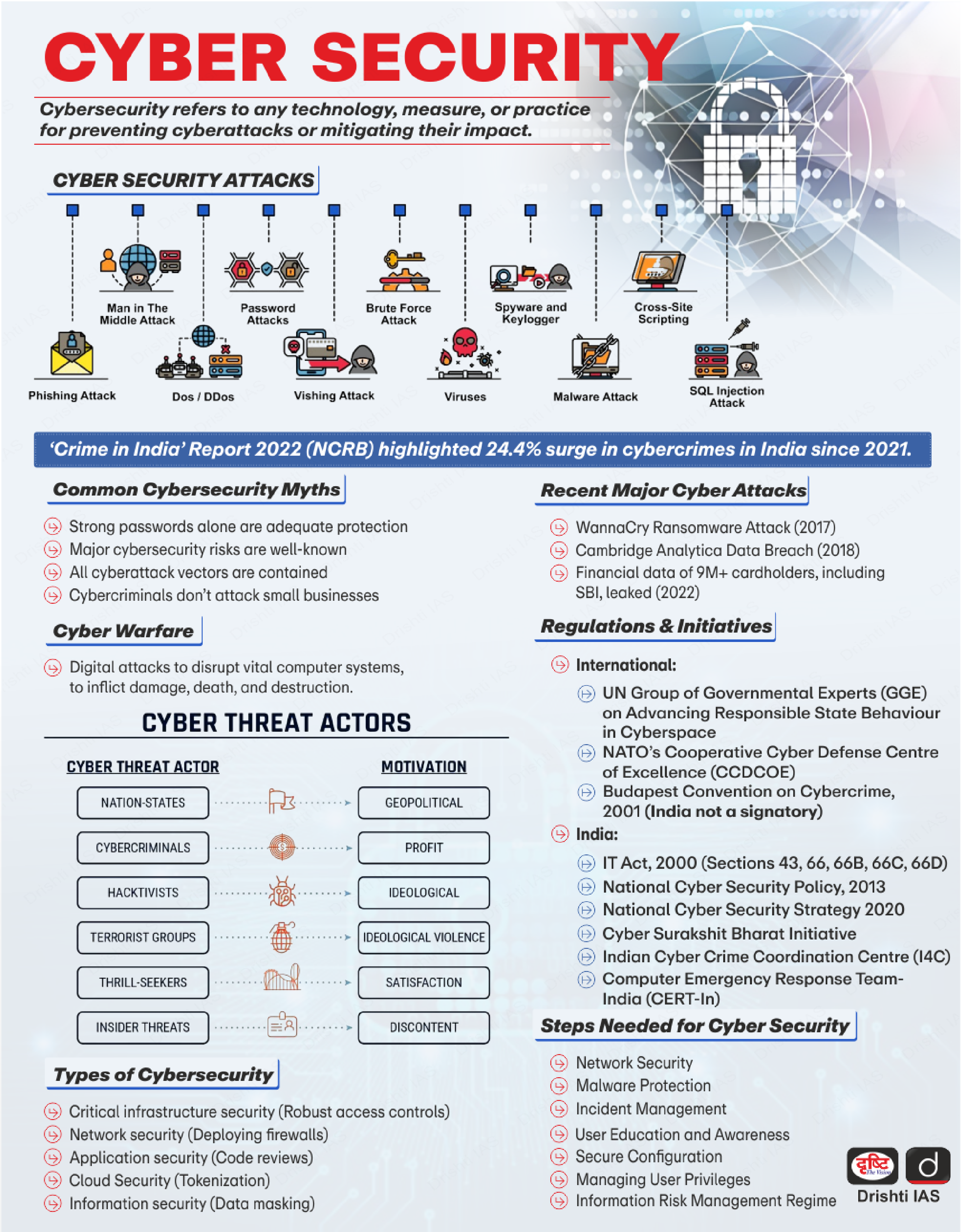
What are the Key Cyberthreats India is Facing?

- **Cyber-enabled Financial Frauds:** India is witnessing a surge in **phishing, ransomware, identity theft, UPI and online banking frauds**.
    - In 2024, the nation recorded **1.91 million cybercrime complaints**, reflecting the scale of digital financial vulnerability.
- **Ransomware & Malware Attacks: Hospitals, government databases, and critical private enterprises** are prime targets of ransomware and malware.
    - The **AIIMS Delhi cyberattack (2022)** exposed the fragility of health and public service systems.
- **Critical Infrastructure Vulnerability:** Strategic assets such as **power grids, telecom networks, nuclear facilities, and ports** face persistent cyber sabotage threats.
    - The **Kudankulam Nuclear Power Plant attack (2019)** underscored risks to **national security**.
- **Data Breaches & Privacy Risks:** Frequent cyber intrusions into **government and private sector databases** have led to large-scale **personal data leaks**.
    - The **Air India breach (2021)** compromised information of nearly **4.5 million passengers**.
- **Deepfa kes & Misinformation:** AI-driven **deepfake content and fake news campaigns** threaten **social cohesion, democratic institutions, and electoral integrity**.
    - The **2024 election campaign** saw deepfake videos of political leaders circulating widely.
- **Dark Web & Cyber Terrorism:** The **dark web** is increasingly exploited for **radicalization, illegal arms/narcotics trade, and terror financing via cryptocurrencies**. Such covert networks intensify **organized crime and cyber terrorism** in India.

What Factors are Undermining the Effectiveness of India’s

Cybersecurity Framework?

- **Inadequate Legal and Regulatory Framework:** Existing laws like the **IT Act, 2000**, and the **Digital Personal Data Protection Act, 2023,** lack specific provisions for emerging threats such as **AI-enabled attacks and deepfakes.**
- **Shortage of Skilled Cybersecurity Professionals:** India faces a **massive gap in trained cybersecurity experts** to monitor and respond to threats in real-time.
    - A report by **NASSCOM** states thatIndia needs **at least one million cybersecurity professionals,** but currently has **less than half that number.**
- **Rapid Digitalization and Low Cyber Awareness: As India’s digital ecosystem expands rapidly, the scale and sophistication of cyber threats have also risen in tandem**
    - Also, India faces weak cyber hygiene among citizens, with many users failing to identify **phishing attacks**, **fraudulent websites**, and **scam calls**, while limited **digital literacy programs** in rural areas further increase vulnerability to cyber fraud.
- **Weak Protection of Critical Infrastructure:** Power grids, telecom networks, and nuclear plants remain vulnerable due to outdated security protocols.
    - At the same time, **SMEs and critical sectors in India lack robust defenses**, and reliance on **imported IT/telecom equipment increases risks of embedded vulnerabilities.**
- **Fragmented Coordination Among Agencies:** Multiple agencies like **CERT-In, National Critical Information Infrastructure Protection Centre**, and private stakeholders operate with **limited coordinatio**n, causing **delays in threat detection and response.**



CYBER SECURITY

Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.

CYBER SECURITY ATTACKS

'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.

Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

Steps Needed for Cyber Security

- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

What are the Key Initiatives Related to Enhance Cybersecurity?

- **Legislative Measures:**
  - [Information Technology Act, 2000 (IT Act)]
  - [Digital Personal Data Protection Act, 2023]
- **Institutional Framework:**
  - Indian Computer Emergency Response Team **(CERT-In)**
  - National Critical Information Infrastructure Protection Centre **(NCIIPC)**
  - Indian Cyber Crime Coordination Centre **(I4C)**
  - Cyber Swachhta Kendra
  - Citizen Financial Cyber Fraud Reporting and Management System
- **Strategic Initiatives:**
  - Bharat National Cybersecurity Exercise 2024
  - National Cyber Security Policy, 2013
  - Chakshu, & Digital Intelligence Platform
  - Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024

What Measures Should be Adopted to Strengthen Cybersecurity Framework in India?

- **Strengthen Legal & Regulatory Framework**: The **IT Act, 2000 needs urgent updates** to cover **AI, deepfakes, and ransomware threats**. Strong enforcement of the **Digital Personal Data Protection Act, 2023** with clear accountability is essential.
- **Institutional & Audit Reforms:** Mandate **cybersecurity audits** and **stress tests** in **critical sectors** like banking, healthcare, and utilities.
  - Establish **district-level cybersecurity units** for localized threat management and strengthen coordination with **CERT-In**.
- **Strengthen Critical Infrastructure:** Enforce **two-factor authentication (2FA)**, **data encryption**, and **real-time monitoring systems** in **critical sectors like banks.**
  - India should promote **Zero-Trust Architecture** in **critical sectors (continuous verification instead of perimeter-only defense).**
- **Promote Indigenous Cybersecurity Solutions:** India should push for **Make in India cybersecurity tools** to reduce foreign dependence. Startups developing **AI-based threat detection** must be supported through **funding and incubation.**
- **Improve Cyber Hygiene & Awareness:** Launch **nationwide cyber literacy campaigns** in **regional languages**, targeting **rural communities, youth, and senior citizens**.
  - Integrate **cybersecurity education** in schools and universities, supported by **secure infrastructure and staff training**, to build digital resilience from an early stage.

Conclusion

Cyberthreats in India have moved beyond mere financial frauds to encompass **national security, privacy, and democratic integrity**. With the rapid digitization of governance and economy, India's vulnerability to **ransomware, data breaches, deepfakes, and critical infrastructure sabotage** has increased manifold. A multi-pronged approach involving **robust cyber laws, institutional capacity, public awareness, and global cooperation** is essential to secure India's cyberspace and safeguard its developmental trajectory.

Drishti Mains Question:

With India's growing digital footprint, cybersecurity threats have emerged as a major challenge to national security, economy, and governance. Examine the nature of these threats and suggest a comprehensive strategy to strengthen India's cybersecurity framework.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one’s computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (2022)

PDF Refernece URL: https://www.drishtiias.com/printpdf/building-a-resilient-cybersecurity-framework-for-india