Emerging Cyber Threats and Their Implications

This editorial is based on "Cyber cons go from digital arrests to wedding scams" which was published in Livemint on 29/11/2024. The article brings into picture the growing sophistication of cybercrime, from fake wedding invitation scams to 'digital arrests,' highlighting the urgent need for stronger digital awareness and robust cybersecurity measures.

For Prelims: Cybercrime, Digital arrest, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, Indian Computer Emergency Response Team, National Critical Information Infrastructure Protection Centre , Cyber Swachhta Kendra, Bharat National Cybersecurity Exercise 2024, Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024, Ransomware attack, Budapest Convention on Cybercrime.

For Mains: Current Framework for Cyber Security in India, Key Emerging Cyber Threats Affecting India's Digital Landscape.

In the ever-evolving landscape of **cybercrime**, fraudsters are pioneering increasingly sophisticated methods that prey on digital vulnerabilities, from the **invented concept of 'digital arrest'** to manipulative scams like fake wedding invitations on WhatsApp. As Indians grapple with these emerging threats, the boundaries **between virtual and real-world fraud become increasingly blurred**, exposing deep systemic challenges in our digital infrastructure. The proliferation of these scams underscores a critical need for **comprehensive digital awareness and robust cybersecurity mechanisms** that can anticipate and neutralize evolving criminal strategies.

What is the Current Framework for Cyber Security in India?

- **Legislative Measures:**
  - **Information Technology Act, 2000 (IT Act):** This foundational legislation provides the **legal framework for electronic governance and addresses cybercrimes and electronic commerce.**
    - It has been amended to i**ncorporate provisions related to data protection and cybersecurity.**
  - **Digital Personal Data Protection Act, 2023:** Enacted t**o protect personal data,** this act outlines the **rights of individuals and the obligations of data fiduciaries** in processing personal data.
    - It emphasizes lawful processing, data minimization, and accountability.
- **Institutional Framework:**
  - **Indian Computer Emergency Response Team (CERT-In):** Operating under the **Ministry of Electronics and Information Technology,** CERT-In is the national nodal agency for responding to computer security incidents.
    - It issues advisories, conducts training, and facilitates coordination among

stakeholders.
    - **National Critical Information Infrastructure Protection Centre (NCIIPC):** NCIIPC focuses on protecting critical information infrastructure in sectors like power, banking, and telecom.
        - It develops strategies and policies to safeguard these assets.
    - **Indian Cyber Crime Coordination Centre (I4C):** Launched by the **Ministry of Home Affairs,** I4C addresses cybercrime through a coordinated approach, including a national cybercrime reporting portal and capacity-building initiatives.
    - **Cyber Swachhta Kendra:** Established in February 2017, the Cyber Swachhta Kendra aims to create a secure cyber ecosystem in India by **detecting and mitigating botnet infections and malware**, in line with the National Cyber Security Policy.
    - **Cyber Surakshit Bharat:** An initiative of the Ministry of Electronics and Information Technology (MeitY) was conceptualised with the mission to **spread awareness about cyber-crime** and **build capacities of Chief Information Security Officers (CISOs**) and frontline IT officials, across all government departments.
- **Strategic Initiatives:**
    - **National Cyber Security Policy, 2013:** This policy outlines the vision and strategies for securing cyberspace, promoting a secure computing environment, and enhancing the resilience of national critical information infrastructure.
    - **Bharat National Cybersecurity Exercise 2024:** The exercise includes **immersive training on cyber defense and incident response, live-fire simulations of cyberattacks** on IT and OT systems, and collaborative platforms for government and industry stakeholders.
- **Sector-Specific Regulations:**
    - **Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities:** Issued by the Securities and Exchange Board of India, this framework mandates regulated entities to establish robust cybersecurity and cyber resilience policies to protect securities markets.
    - **Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024:** Introduced in November 2024, it mandates telecom entities labeled as **Critical Telecommunication Infrastructure (CTI)** to provide government-authorized personnel access to i**nspect their hardware, software, and data.**

What are the Key Emerging Cyber Threats Affecting India's Digital Landscape?

- **Digital Arrest Scams:** Cybercriminals have devised a new method of fraud, **impersonating law enforcement officials to instill fear in unsuspecting victims.**
    - These fraudsters contact individuals, claiming they are under investigation for fabricated crimes, and coerce them into paying hefty fines to avoid fictitious arrests.
    - By exploiting the authority associated with law enforcement and the victim's lack of digital literacy, these scams have become alarmingly effective.
    - **In 2024, Indians collectively lost a staggering ₹120.30 crore to such “digital arrest” fraud**.
- **Ransomware Attacks:** Ransomware attacks have escalated, targeting **critical infrastructure and financial institutions**, leading to operational disruptions and financial losses.
    - In **August 2024,** a ransomware attack on **C-Edge Technologies** disrupted payment systems across nearly 300 small Indian banks, highlighting vulnerabilities in financial networks.
    - Also, **2023 ransomware attack on the All India Institute of Medical Sciences (AIIMS)** in Delhi exemplifies the vulnerabilities in healthcare infrastructure
- **Supply Chain Attacks:** Cybercriminals are increasingly exploiting vulnerabilities in supply chains to infiltrate larger networks.
    - For instance, in **December 2020**, a global cyberattack targeting SolarWinds, a US-based software company offering network management tools, impacted multiple Indian organizations, including the **National Informatics Centre (NIC), the Ministry of Electronics and Information Technology (MeitY)**, and **Bharat Heavy Electricals Limited (BHEL).**
    - India suffered cyber fraud losses amounting to **Rs 11,333 crore** in the first nine months of 2024, according to data from the Indian Cyber Crime Coordination Centre (I4C)

- **State-Sponsored Cyber Espionage:** Nation-state actors are intensifying cyber **espionage activitie**s, targeting sensitive government and corporate data.
    - A cyber-attack originating from China was identified as the cause behind the massive power outage in **Mumbai** in 2020, exposing vulnerabilities in the city's critical infrastructure.
- **Deepfake Technology Exploitation:** The misuse of AI-generated **deepfakes** poses significant threats, including misinformation and fraud.
    - A 2024 report identified deepfakes as an imminent threat in India, capable of undermining public trust and manipulating information.
    - A deep fake video depicting actress **Rashmika Mandanna** in explicit content surfaced online, causing widespread outrage.
- **Exploitation of Internet of Things (IoT) Devices:** The widespread adoption of **Internet of Things (IoT) devices** has **significantly increased the vulnerability of digital ecosystems,** creating new opportunities for cybercriminals.
    - These devices, often lacking robust security features, are easily exploited to breach networks or conduct malicious activities.
    - In 2024, **India witnessed a staggering 59% rise in IoT-related cyberattacks,** underscoring the scale of this emerging threat.
    - From smart homes to connected industrial systems, the risks associated with unsecured IoT devices have escalated.
- **Cryptocurrency and Blockchain-Based Cyber Fraud:** The explosive growth of cryptocurrency adoption in India has created a **new, largely unregulated landscape for sophisticated cyber fraud mechanisms.**
    - Blockchain-based platforms are increasingly becoming targets for complex **Ponzi schemes, pump-and-dump manipulations**, and advanced money laundering techniques that exploit regulatory gray areas.
    - A **Bengaluru-based Bitcoin scam** exposed a nexus between a **hacker, police officials, and a cyber expert**, involving the illegal transfer of cryptocurrency worth **₹850 crore,** tampering of evidence, and allegations of corruption
- **Dark Web-Enabled Cybercrime:** The dark web remains a hub for illegal trading of stolen data and malicious tools.
    - Hackers are selling customized malware and ransomware kits on the dark web, making sophisticated attacks accessible to less-skilled threat actors.
    - A recent security breach has **exposed the personal data of 750 million telecom users in India**, with the data being sold on the dark web.

What Measures can be Adopted to Enhance the Cybersecurity Landscape in India?

- **Nationwide Cyber Literacy Campaigns:** Digital literacy campaigns should be rolled out in **regional languages, targeting vulnerable populations like rural communities and senior citizens.**
    - These initiatives can teach users to verify identities, recognize scams, and use secure payment systems.
    - Partnerships with schools, colleges, and local governance bodies can amplify impact.
- **Mandatory Security Protocols for IoT Devices:** Introduce enforceable standards **requiring manufacturers to integrate security-by-design principles** in IoT devices.
    - This includes firmware updates, encrypted communication, and tamper-proof mechanisms.
    - Certification from a **regulatory authority can ensure only secure devices reach the market.** Public awareness about IoT risks will further enhance security at the consumer level.
- **AI-Driven Threat Intelligence and Response Systems**: Deploy AI-based tools in critical sectors to **analyze network traffic, identify anomalies, and respond to threats in real time.**
    - These systems can predict ransomware attacks and neutralize vulnerabilities before exploitation.
    - AI can also enhance forensic investigations, aiding faster response to incidents. Regular testing of AI systems ensures accuracy and reliability.

- **Strengthen CERT-In Capabilities:** Expand CERT-In's mandate to include **deeper collaboration with international CERTs** and the private sector, aligning efforts with international frameworks such as the **Budapest Convention on Cybercrime.**
    - Introduce **regional CERT hubs for faster response to localized incidents.** Equip CERT-In with cutting-edge tools for threat detection, and advanced forensics.
    - Proactively issue advisories and simulation exercises to improve institutional resilience.
- **National Deepfake Detection and Regulation Framework**: Develop **Ethical-AI tools** capable of identifying deepfake content in real time.
    - Establish **penalties for creating and disseminating harmful deep fake media** under updated IT laws.
    - Collaboration with **social media platforms to flag and remove such content can reduce its spread.** Public awareness campaigns should educate people on recognizing manipulated media.
- **District-Level Cybersecurity Response Units:** Establish dedicated cybersecurity cells in every district equipped with trained personnel and forensic tools.
    - These units can **handle smaller-scale scams like digital arrest fraud quickly** and coordinate with CERT-In for larger issues.
    - Community engagement programs can build trust and encourage timely reporting of incidents.
- **Supply Chain Cybersecurity Certification:** Introduce a certification system for supply chain partners to ensure they adhere to cybersecurity best practices.
    - This includes **regular audits, blockchain integration, secure software development practices,** and encrypted communication channels.
    - Large enterprises should demand these certifications from vendors. This minimizes risks of breaches infiltrating through smaller entities.
- **Cryptocurrency Regulations:** Establish clear regulations for **cryptocurrency transactions,** focusing on transparency and traceability.
    - **Mandatory KYC for crypto exchanges** and real-time monitoring systems can prevent illegal activities.
    - Specialized crypto forensic units should address fraud swiftly.
- **Mandatory National Cybersecurity Audits:** Regular, government-mandated audits can identify and fix vulnerabilities in critical infrastructure systems.
    - Incorporating **stress tests, penetration tests, and employee training ensures comprehensive readiness**.
    - These audits should be compulsory for sectors like healthcare, banking, and utilities. Results can be used to prioritize resource allocation for better protection.
- **Cyber Hygiene Awareness for Startups:** Introduce government-supported **cybersecurity training programs tailored for startups**.
    - Subsidized access to cybersecurity tools and services can enable small businesses to adopt best practices.
    - **Awareness campaigns about the risks of poor security hygiene** can motivate startups to prioritize investments in protection. Sector-specific guidance ensures relevance.
- **Proactive Dark Web Monitoring:** Invest in tools that actively monitor the dark web for **stolen data, illegal goods, and malware sales**.
    - **Intelligence gathered from dark web activity** can preempt attacks and guide law enforcement operations.
    - Public-private collaboration can expand monitoring capabilities. Dedicated task forces should act swiftly on identified threats.
- **Multi-Factor Authentication (MFA) Enforcement:** Mandate MFA across critical systems, government portals, and financial platforms to reduce reliance on passwords alone.
    - Businesses should adopt adaptive MFA systems to enhance user experience without compromising security. This minimizes unauthorized access risks.
- **Cybersecurity for Education Sector:** Introduce cybersecurity awareness and defense mechanisms in schools and universities. This includes **regular backups, secure networks, and training staff to handle threats.**
    - National programs can provide resources for smaller institutions to enhance their defenses. Involving students in awareness campaigns builds a culture of cybersecurity early.
- **Implementing Data Localization Norms:** Although the **Digital Personal Data Protection**

Act, 2023 includes provisions for data localization, these **should not remain mere formalities on paper** but must be implemented in both letter and spirit.
    - Mandating that **critical and sensitive data remain stored within national borders** can improve control and reduce security risks.
    - Clear compliance frameworks and penalties for violations should be enforced.

Conclusion

The evolving landscape of cybercrime necessitates a **comprehensive and proactive approach.** India needs to strengthen its cybersecurity infrastructure**, promote digital literacy, and foster international collaboration to combat these threats effectively.** By investing in robust security measures, building a skilled workforce, and staying ahead of emerging threats, India can safeguard its digital future and protect its citizens from the growing risks of cyberattacks.

Drishti Mains Question:

With the increasing reliance on digital technologies in India, the country faces growing risks from emerging cyber threats. What measures should be adopted to enhance India's resilience against such evolving cyber risks?

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)**