Strengthening India's Cyber Defence

This editorial is based on "Disinformation, AI and 'cyber chakravyuh'" which was published in The Hindu on 13/08/2024. The article highlights the rising threat of AI and cyberattacks in 2024, emphasizing the need for increased vigilance and coordinated global action to combat these emerging digital dangers, especially in democratic nations. It also underscores the importance of addressing AI-enabled disinformation and the growing risk of cyber fraud in daily life.

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.

The year **2024** has ushered in a new era of digital threats, with Artificial Intelligence **(AI)** and its various manifestations, including **Generative AI and Artificial General Intelligence (AGI),** at the forefront of security concerns. The potential for digital attacks, disinformation campaigns, and cyber threats remains high. The recent **global disruption caused by a Microsoft Windows software** update glitch serves as a stark reminder of the vulnerabilities in our interconnected digital infrastructure.

For India, as with the rest of the world, the threat landscape is evolving rapidly. From AI-enabled deep fakes **to sophisticated cyber attacks** targeting critical infrastructure, the challenges are multifaceted and growing in complexity. The rise in cyber fraud affecting ordinary citizens, including phishing attempts, identity theft, and financial scams, underscores the need for heightened awareness and robust cybersecurity measures. As we navigate this new digital reality, it is imperative for both the public and private sectors in India to **prioritize cybersecurity,** invest in advanced protective measures, and foster a culture of digital vigilance to safeguard national security and individual privacy.

What are the Current Major Cyber Threats that India is Facing?

- **The Ransomware Rampage**: India witnessed an increase in ransomware attacks recently with the healthcare sector being particularly vulnerable.
    - Security software maker Quick Heal stated it has detected over **48000 instances of the** WannaCry ransomware attack **in India.**
    - The attack on the **All India Institute of Medical Sciences (AIIMS) Delhi** in November 2022.
        - There were at least 6,000 attempts to hack the server of the Indian Council of Medical Research (ICMR).
- **Phishing Paradox:** India recorded over 79 million phishing attacks in 2023. The finance sector bore the brunt, accounting for the majority of all phishing attacks.

    - Examples include the **Phishing Campaigns** targeting State Bank of India users , where fraudsters sent fake SMS messages to millions of customers, attempting to steal their banking credentials.
    - This trend underscores the importance of user education and advanced email security solutions.
- **The Cloud Conundrum:** As India rapidly adopts cloud technologies, with the overall **Indian Public Cloud Services (PCS)** market expected to reach **USD 24.2 billion by 2028**, cloud security threats have become a major concern.
    - In 2023, a significant data breach at Air India exposed the **personal data of 4.5 million passengers,** attributed to a compromise in its cloud service provider's systems.
    - This incident highlights the need for robust cloud security strategies, including proper configuration, access management, and continuous monitoring.
- **The IoT Invasion:** With India's IoT market projected to reach **USD 9.28 billion by 2025,** the **security of** Internet of Things (IoT) devices has become a critical issue.
    - Researchers discovered a vulnerability in **millions of** smart meters deployed across India, potentially allowing hackers to manipulate power consumption data.
    - This discovery emphasizes the need for stringent security standards and regular updates for IoT devices in both consumer and industrial settings.
- **The Supply Chain Siege:** India's digital supply chains faced unprecedented attacks in 2023, with a rampant increase in software supply chain vulnerabilities.
    - The **SolarWinds-like attack** on the IT services giant in 2023 is a prominent example.
    - This incident exposed the **cascading effect of supply chain attacks and highlighted the need for rigorous vendor risk management** and software integrity verification processes across Indian industries.
- **The Crypto Crimes Wave**: According to a report published by 'Broadband India Forum' Cryptocurrency theft grew with roughly $3.2 billion worth stolen in 2021, a 516% increase compared to 2020.
    - The infamous **WazirX Crypto Heist** which compromised **45% of WazirX's crypto assets,** has highlighted significant vulnerabilities highlighted the vulnerabilities in digital asset platforms.
    - This trend calls for stronger regulations, enhanced cybersecurity measures for crypto exchanges, and increased user awareness about safe crypto practices.
- **The Deepfake Dilemma:** India witnessed a **230% increase in** deepfake videos **in 2023**, with political misinformation campaigns leading the charge.
    - The viral deep fake video of a prominent Indian politician making inflammatory statements during the **2024 election campaign** caused significant social unrest.
    - This incident highlights the urgent need for deepfake detection technologies, stricter content moderation policies, and public awareness campaigns about digital media literacy.
- **Lack of Cybersecurity Professionals:** India faces a severe shortage of skilled cybersecurity professionals, **leaving organizations vulnerable to cyber threats.**
    - India has a shortage of 8 lakh cybersecurity professionals. This shortage is particularly acute in emerging technologies like AI and cloud security.
    - The lack of expertise hampers the implementation of robust cybersecurity measures and incident response capabilities, making it a critical threat to India's overall cybersecurity posture.
- **The Honey Trap Hazard: Honey trapping** has emerged as a significant cyber threat in India, particularly targeting government officials, military personnel, and high-profile individuals.
    - This method involves creating fake social media profiles, usually of attractive individuals, to lure targets into compromising situations or divulging sensitive information.
    - In 2023, the Indian Army reported a dramatic increase in honey trapping attempts on its personnel compared to the previous year.
    - Another **DRDO senior technical officer was detained in 2023** on suspicion of giving information about **India's missile testing to a Pakistani intelligence operative.**

What are the Key Government Initiatives Related to Cybersecurity in India?

- National Cyber Security Policy: The policy outlines objectives and strategies to protect **cyberspace information and infrastructure, develop capabilities to prevent and respond to cyber attacks**, and minimize damages through coordinated efforts across institutional structures,

people, processes, and technology.

- Indian Cyber Crime Coordination Centre (**I4C):** To provide a comprehensive and coordinated framework for law enforcement agencies to tackle cyber crimes.
    - **Components:**
        - **National Cyber Crime Threat Analytics Unit**
        - **National Cyber Crime Reporting Portal**
        - **National Cyber Crime Training Centre**
        - **Cyber Crime Ecosystem Management Unit**
        - **National Cyber Crime Research and Innovation Centre**
        - **National Cyber Crime Forensic Laboratory Ecosystem**
        - **Platform for Joint Cyber Crime Investigation Team**
- Computer Emergency Response Team - India (CERT-In): An organization under the Ministry of Electronics and Information Technology (MeitY) responsible for collecting, analyzing, and disseminating information on cyber incidents, as well as issuing alerts on cybersecurity threats.
- **Cyber Surakshit Bharat Initiative:** To raise awareness about cyber crimes and implement safety measures for **Chief Information Security Officers (CISOs)** and frontline IT staff across all government departments.
- Cyber Swachhta Kendra (**Botnet Cleaning and Malware Analysis Centre**): Launched in 2017, this **center aims to create a secure cyberspace by detecting botnet infections** in India and notifying users to enable the cleaning and securing of their systems to prevent further infections.
- National Critical Information Infrastructure Protection Centre (**NCIIPC)**: Established to protect **Critical Information Infrastructure (CII)** in sectors such as power, banking, telecom, transport, government, and strategic enterprises.
    - CII is defined as a computer resource whose destruction would have a debilitating impact on national security, economy, public health, or safety.
- **Defence Cyber Agency (DCyA**)A tri-service command of the Indian Armed Forces responsible for handling cybersecurity threats.
    - The DCyA has the capability to conduct cyber operations, including hacking, surveillance, data recovery, encryption, and countermeasures against various cyber threat actors.
- Digital Personal Data Protection Act 2023: This landmark legislation aims to protect the digital personal data of individuals in India and regulate the collection, storage, processing, and sharing of such data.
    - **Key features:**
        - Establishes a Data Protection Board of India to enforce compliance
        - Requires explicit consent for data collection and processing
        - Mandates data fiduciaries to implement reasonable security safeguards

What Measures can India Adopt to Bolster its Cybersecurity?

- **Cyber Fusion Centers:** Establish regional **Cyber Fusion Centers** to facilitate real-time threat intelligence sharing between public and private sectors.
    - Implement **advanced AI and machine learning systems** for predictive threat analysis.
    - Create a **centralized incident response team** capable of rapid deployment to address major cyber incidents.
    - Conduct **regular joint cyber exercises** involving multiple stakeholders to test and improve coordination.
- **Digital Literacy Crusade**: Launch a nationwide **digital literacy campaign targeting all demographics,** with a focus on cybersecurity awareness.
    - Integrate cybersecurity education into school curricula from secondary to higher education levels.
    - Develop a mobile app providing real-time cybersecurity tips and threat alerts to citizens.
    - Conduct **regular cyber hygiene workshops** in rural areas using local languages and relatable scenarios.
    - Partner with **popular social media influencers** to spread cybersecurity awareness among youth.
- **Strengthening Current Data Protection Framework:** India should strengthen the existing Digital Personal Data Protection Act 2023 by incorporating provisions for **regulating AI powered breaches of personal data, imposing stricter penalties for breaches,** and enforcing **rigorous implementation and scrutiny.**

    - Enhancing the current act will address emerging threats without duplicating legislative efforts.
- **Secure-by-Design Initiative:** Promote a 'Secure-by-Design' approach in software and hardware development across industries.
    - Establish a **national cybersecurity product certification program** to ensure adherence to security standards.
    - Offer **grants and funding for startups** focusing on developing innovative cybersecurity solutions.
    - Create a **dedicated R&D fund for quantum-resistant cryptography** to prepare for future threats.
- **AI-Powered Cyber Defense:** Invest in developing AI-powered cybersecurity solutions tailored to India's unique threat landscape.
    - Implement machine learning algorithms for **anomaly detection in network traffic and user behavior.**
    - Develop AI-driven threat hunting capabilities to proactively identify and neutralize emerging cyber threats.
- **Supply Chain Fortification:** Implement a comprehensive supply chain risk management framework for **both hardware and software procurement.**
    - Conduct regular **security assessments of third-party vendors and service providers.**
    - Develop a national database of trusted suppliers and mandate its use in government and critical sector procurements.
    - Implement **blockchain technology for enhanced traceability** and integrity in digital supply chains.
- **Cloud Citadel-Securing India's Digital Sky:** Establish a national cloud security framework with stringent compliance requirements for all cloud service providers.
    - Implement **mandatory encryption for all data stored in the cloud,** addressing vulnerabilities like those in the Air India breach.
    - Create a **Cloud Security Operations Center** to monitor and respond to threats across public cloud services.
- **Deepfake Defense:** Implement strict content verification protocols for all major social media platforms operating in India.
    - Create a **rapid response team** to address viral deepfakes during critical periods like elections.
    - Launch a public awareness campaign on identifying and reporting deepfakes.
- **The Cyber Warrior Initiative:** India should launch a comprehensive "**Cyber Warrior Initiative**" to address the critical shortage of cybersecurity professionals.
    - This program would involve partnering with universities to develop specialized cybersecurity curricula, establishing a **national cybersecurity scholarship program, and creating a cyber reserve force.**
    - Implementing a national certification program and offering tax incentives to companies investing in employee cybersecurity training would further strengthen the workforce.

Drishti Mains Question:

Discuss the key challenges in India's cybersecurity landscape and evaluate the effectiveness of current measures in addressing these threats. Suggest strategies for strengthening India's cybersecurity framework to counter emerging digital threats.

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)**