Mains Marathon 2024

Day 35: Assess the potential threats posed by cyber-attacks in India. Examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy to mitigate these threats. (250 words)

16 Aug 2024 | GS Paper 3 | Internal Security

Approach / Explaination / Answer

Approach

- Briefly introduce the concept of cyber-attacks.
- Assess the potential threats posed by cyber-attacks in India.
- Provide an overview of India's National Cyber Security Strategy.
- Suggest Further Steps to Enhance Cyber Security.
- Conclude Suitably.

Introduction

Cyber-attacks refer to malicious activities conducted through digital means, targeting computer systems, networks, or digital devices to disrupt operations, steal sensitive information, or gain unauthorized access. These attacks can range from simple phishing attempts to sophisticated operations like ransomware, hacking, and state-sponsored cyber espionage. As digitalization increases globally, the frequency and complexity of cyber-attacks have escalated, posing significant risks to national security, economic stability, and individual privacy

Body

Potential Threats Posed by Cyber-attacks in India:

- **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.
- **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.

- **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.
- **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.
- **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.
- **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.
- **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.
- **The Honey Trap Hazard:** This method involves creating fake social media profiles, usually of attractive individuals, to lure targets into compromising situations or divulging sensitive information.
    - In 2023, DRDO senior technical officer was detained in 2023 on suspicion of giving information about India's missile testing to a Pakistani intelligence operative.

India’s National Cyber Security Strategy:

- In 2020, the National Cyber Security Strategy was conceptualized by the Data Security Council of India (DSCI) headed by Lt General Rajesh Pant. The report focused on 21 areas to ensure a safe, secure, trusted, resilient, and vibrant cyberspace for India.
- **Key Components :**
    - **Large-Scale Digitisation of Public Services:**
        - Focus on security in the early stages of design in all digitization initiatives.
        - Developing institutional capability for assessment, evaluation, certification, and rating of the core devices
        - Timely reporting of vulnerabilities and incidents.
- **Supply Chain Security:**
    - Monitoring and mapping of the supply chain of the Integrated Circuits (ICT) and electronics products.
    - Leveraging the country’s semiconductor design capabilities globally at strategic, tactical and technical levels.
- **Critical Information Infrastructure Protection:**
    - Integrating Supervisory Control And Data Acquisition (SCADA) security
    - Maintaining a repository of vulnerabilities.
    - Preparing an aggregate level security baseline of the sector and tracking its controls.
    - Devising audit parameters for threat preparedness and developing cyber-insurance products.
- **Digital Payments:**
    - Mapping and modeling of devices and platforms deployed, supply chain, transacting entities, payment flows, interfaces and data exchange.
- **State-Level Cyber Security:**
    - Developing state-level cybersecurity policies,
    - Allocation of dedicated funds,
    - Critical scrutiny of digitization plans,
    - Guidelines for security architecture, operations, and governance.
- **Security of Small And Medium Businesses:**

- Policy intervention in cybersecurity granting incentives for a higher level of cybersecurity preparedness.
- Developing security standards, frameworks, and architectures for the adoption of the Internet of Things (IoT) and industrialization.

Further Steps to Enhance Cyber Security :

- **Strengthening Existing Legal Framework**: India's primary legislation governing cyber crimes is the Information Technology (IT) Act of 2000, which has been amended several times to address new challenges and threats.
  - India needs to enact comprehensive and updated laws that cover all aspects of cyber security, such as cyber terrorism, cyber warfare, cyber espionage, and cyber fraud.
  - In the year 2022, the Indian government proposed the enactment of the Digital India Act (DIA) that would give a global and coeval legal framework for India's evolving digital ecosystem.
- **Enhancing Cyber Security Capabilities:** India has several initiatives and policies to improve its cyber security, such as the National Cyber Security Policy, the Cyber Cells and Cybercrime Investigation Units, the Cyber Crime Reporting Platforms, and the Capacity Building and Training programs.
  - However, these efforts are still inadequate and fragmented, as India faces a shortage of technical staff, cyber forensics facilities, cyber security standards, and coordination among various stakeholders.
- **Establish a Cyber Security Board:** India must establish a cyber security board with government and private sector participants that has the authority to convene, following a significant cyber incident, to analyse what happened and make concrete recommendations for improving cybersecurity.
  - Adopt a zero-trust architecture, and mandate a standardised playbook for responding to cybersecurity vulnerabilities and incidents. Urgently execute a plan for defending and modernising state networks and updating its incident response policy.
- **Expanding International Cooperation:** India is not alone in facing the challenges of cyber security, as cyber attacks transcend national boundaries and affect the global community.
  - India needs to engage more with other countries and international organisations, such as the United Nations, the International Telecommunication Union, the Interpol, and the Global Forum on Cyber Expertise, to exchange best practices, share threat intelligence, harmonise cyber laws and norms, and cooperate in cyber investigations and prosecutions.
  - India also needs to participate more actively in regional and bilateral dialogues and initiatives, such as the ASEAN Regional Forum, the BRICS, and bilateral forums it has like Indo-US Cyber Security Forum, to build trust and confidence, and to address common cyber security issues and interests.

Conclusion

As India advances towards becoming a global digital leader, addressing cyber threats with a proactive and resilient approach will be key to safeguarding national security and fostering economic growth.The effective implementation of India's National Cyber Security Strategy is essential for safeguarding the nation's digital infrastructure against the growing threats of cyber-attacks.This strategy must be underpinned by a robust cybersecurity infrastructure, continuous technological innovation, and the development of a skilled cybersecurity workforce..