India's Cybersecurity Challenge: Threats and Strategies

This editorial is based on **"We want a Digital India. Just not the one we are living in"** which was published in The Indian Express on 26/12/2023. The article discusses the challenges and opportunities for India in the domain of cyber security, and argues that India needs a new approach that is based on self-reliance, innovation, and collaboration.

For Prelims: SWIFT system, National Informatics Centre (NIC), Cyber Surakshit Bharat Initiative, Cyber Swachhta Kendra, Indian Cyber Crime Coordination Centre (I4C), National Critical Information Infrastructure Protection Centre (NCIIPC), Defence Cyber Agency (DCyA),

For Mains: India's vulnerability to cyber attacks, Challenges posed by cyber attacks, Government Initiatives and Way Forward

As the world is advancing in the realm of digitalisation, the threat of cyber attacks has also grown and India is no exception to it. In October, 2023, Resecurity, a US company, informed the world about the availability of Indians' personal data on the dark web. It would have been easy to ignore this amid the deluge of bad news filling our news feeds but for the size and sensitivity of data. The seller of the data set was providing verifiable, sensitive information of 55% of the Indian population — roughly around 815 million (81.5 crore) citizens.

This included personally identifiable information like name, phone number, Aadhaar number, passport number and address. All for a paltry sum of USD80,000. On December 18, Delhi police had arrested four individuals in this matter.

How Vulnerable is India to Cyber Attacks?

- India has a large and growing population of internet users, with **more than 52% of the population or 759 million people** accessing the internet at least once a month in 2022
    - India is the **second largest online market** in the world, behind China.
    - By 2025, the number is **expected to grow to 900 million.**
- India has a rapidly expanding digital economy, with sectors such as healthcare, education, finance, retail, and agriculture relying on online platforms and services.
    - However, India's outdated or inadequate cyber security infrastructure, policies, and awareness, making it easy for hackers to exploit the gaps and weaknesses in the system that's why India faces sophisticated and persistent cyber threats from state-sponsored and non-state actors, who target India's strategic, economic, and national interests.

What are the Challenges Posed by Cyber Attacks on India?

- **Critical Infrastructure Vulnerability:** India's critical infrastructure, such as power grids,

transportation systems, and communication networks, is vulnerable to cyber attacks that can **disrupt essential services** and endanger public safety and national security.
    - For example, in October 2019, there was an attempted cyber-attack on the **Kudankulam Nuclear power plant.**
- **Financial Sector Threats:** The financial sector in India faces a high risk of cyberattacks from cybercriminals who seek to profit from stealing or extorting money. Attacks on banks, financial institutions, and online payment systems can cause financial losses, identity theft, and a loss of trust in the financial system.
    - For instance, in March 2020, a malware attack on the City Union Bank's **SWIFT system** led to unauthorised transactions worth USD 2 million.
- **Data Breaches and Privacy Concerns:** As India moves towards a digital economy, the amount of personal and government data stored online increases. This also increases the risk of data breaches, where hackers access and leak sensitive information. Data breaches can have serious consequences for the privacy and security of individuals and organisations.
    - For example, in May 2021, the personally identifiable information (PII) and test results of 190,000 candidates for the 2020 Common Admission Test (CAT), used to select applicants to the IIMs, were leaked and put up for sale on a cybercrime forum.
- **Cyber Espionage:** Cyber espionage is the use of cyber attacks to spy on or sabotage the interests of other countries or entities. India, like other countries, is a target for cyber espionage activities that aim to steal confidential information and gain a strategic edge. Cyber espionage can affect India's national security, foreign policy, and economic development.
    - For example, in 2020, a cyber espionage campaign called Operation SideCopy (a Pakistani threat actor) was uncovered, which targeted Indian military and diplomatic personnel with malware and phishing emails.
- **Advanced Persistent Threats (APTs):** APTs are complex and prolonged cyber attacks, usually carried out by well-resourced and skilled groups. These attacks are designed to infiltrate and remain hidden in the target's network for a long time, allowing them to steal or manipulate data, or cause damage.
    - APTs are difficult to detect and counter, as they use advanced techniques and tools to evade security measures.
    - For example, in February 2021, a cyber security firm called RedEcho revealed that a China-linked APT group had targeted 10 entities in India's power sector, with malware that could potentially cause power outages.
- **Supply Chain Vulnerabilities:** Supply chain vulnerabilities refer to the weaknesses in the software or hardware components that are used by government and businesses for their operations. Cyber attackers can exploit these vulnerabilities to compromise the systems and services that depend on these components, and cause widespread damage.
    - For example, in December 2020, a global cyberattack on SolarWinds, a US-based software company that provides network management tools, affected several Indian organisations, including the **National Informatics Centre (NIC),** the Ministry of Electronics and Information Technology (MeitY), and Bharat Heavy Electricals Limited (BHEL).

What are the Initiatives Regarding Cyber Security?

- **National Cyber Security Policy:** This policy aims to build a secure and resilient cyberspace for citizens, businesses, and the government. It outlines various objectives and strategies to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.
- **Cyber Surakshit Bharat Initiative:** This initiative was launched to raise awareness about cyber crimes and create safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **Indian Cyber Crime Coordination Centre (I4C):** This centre was established to provide a framework and eco-system for law enforcement agencies to deal with cyber crimes in a comprehensive and coordinated manner. It has seven components, namely:
    - 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.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):** This centre was launched in 2017 to create a secure cyberspace by detecting botnet infections in India and notifying, enabling cleaning and securing systems of end users to prevent further infections.
- **Computer Emergency Response Team - India (CERT-In):** It is an organisation of the MeitY which collects, analyses and disseminates information on cyber incidents, and also issues alerts on cybersecurity incidents.
- **Critical information infrastructure (CII):** It is defined as a computer resource, the destruction of which, shall have debilitating impact on national security, economy, public health or safety.
    - The government has established the **National Critical Information Infrastructure Protection Centre (NCIIPC)** to protect the CII of various sectors, such as power, banking, telecom, transport, government, and strategic enterprises.
- **Defence Cyber Agency (DCyA)**: The **DCyA** is a tri-service command of the Indian Armed Forces that is responsible for handling cyber security threats. It has the capability to conduct cyber operations, such as hacking, surveillance, data recovery, encryption, and countermeasures, against various cyber threat actors.

What Should India Do Further to Save Itself from Cyber attacks?

- **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.
    - However, the IT Act still has some gaps and limitations, such as the lack of clear definitions, procedures, and penalties for various cyber offences, and the low conviction rate of cyber criminals.
    - 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.
- **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.
    - India needs to invest more in developing its human and technological resources, establishing cyber security centers of excellence, adopting best practices and standards, and fostering collaboration and information sharing among different agencies and sectors.
- **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.

Drishti Mains Question:

Highlight the key challenges posed by Cyber Attacks on india. How can the government formulate effective strategies to mitigate the risks posed by cyber attacks?

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)**