Rethinking India’s Cyber Defence

This editorial is based on **“The AIIMS attack shows the importance of a robust cybersecurity framework”** which was published in Hindustan Times on 04/12/2022. It talks about Ransomware Attack on AIIMS server and related challenges to India’s cyberspace.

For Prelims: Cyber security, WannaCry, Ransomware, Trojan Horses, Clickjacking, Denial of Service (DOS) Attack, Man in Middle Attack, Zero Day Vulnerability, Artificial intelligence (AI) ,Indian Cyber Crime Coordination Centre (I4C), Indian Computer Emergency Response Team (CERT-In), Cyber Surakshit Bharat, Cyber Swachhta Kendra, National Cyber security Coordination Centre (NCCC).

For Mains: Recent Instances of Cyber Attacks in India, Major Types of Cyber Threats, Challenges Related to India’s CyberSpace.

The Internet **has become one of the integral parts of our daily life.** They are impacting most aspects of our day-to-day life. Cyberspace **connects** us virtually with crores of online users across the globe.

As India's internet base continues to grow, with over 900 internet users expected by 2025, a **parallel rise in cyber threats has become increasingly concerning.** The sophistication of cybercrimes is also increasing with the advancement of **digital technology.**

It is therefore imperative that **India closely examines the loopholes in its cyberspace and addresses them holistically through a more comprehensive** Cyber-Security Policy.

What is Cyber Security?

- Cyber security **or information technology security** are the techniques of **protecting computers, networks, programs and data** from unauthorised access or attacks that are aimed for exploitation of **cyber-physical systems** and **critical information infrastructure.**
    - **Critical Information Infrastructure(CII):** According to **Section 70(1) of the** Information Technology Act, CII is defined as a **“computer resource, the incapacitation or destruction of which**, shall have **debilitating impact on national security, economy, public health or safety”.**

What are the Recent Instances of Cyber Attacks in India?

- In **2020,** approximately **82% of Indian companies suffered ransomware attacks.**
    - In **May 2017**, top five cities in India (Kolkata, Delhi, Bhubaneswar, Pune and Mumbai) got

impacted due to WannaCry **ransomware attack.**
    - A **ransomware attack recently hit AIIMS Delhi.** The personal data of millions of patients in the top premier medical institute is at risk after a ransomware attack on its **servers.**
- In **2021**, A high-profile India-based payment company, **Juspay**, suffered a data breach impacting 35 million customers.
    - This breach is very noteworthy because **Juspay handles payments for online marketplaces, including Amazon** and other big players.
- In **February 2022,** Air India experienced a major cyberattack that compromised approximately **4.5 million customer records.** Passport, ticket, and some credit card information was compromised.

What are the Major Types of Cyber Threats?

- **Ransomware:** This type of **malware hijacks computer data** and then **demands payment (usually in bitcoins) in order to restore it.**
- **Trojan Horses:** A Trojan horse attack uses a **malicious program that is hidden inside a seemingly legitimate one.**
    - When the user executes the presumably innocent program, the **malware inside the Trojan can be used to open a backdoor** into the system through which hackers can penetrate the computer or network.
- **Clickjacking:** Act of tempting **internet users to click links containing malicious software** or unknowingly share private information on social media sites.
- **Denial of Service (DOS) Attack:** The deliberate act of **overloading a particular service** like website from multiple computers and routes with the aim of disrupting that service.
- **Man in Middle Attack**: In this kind of attack, the **messages between two parties are intercepted during transit.**
- **Cryptojacking:** The term **Cryptojacking is closely related to cryptocurrency.** Cryptojacking takes place when **attackers access someone else's computer for mining cryptocurrency.**
- **Zero Day Vulnerability:** A **zero-day vulnerability** is a flaw in the machine/network's operating system or application software which has not been fixed by the developer and can be exploited by a hacker who is aware of it.

What are the Challenges Related to India's CyberSpace?

- **Multiplying Capacity, Adding Vulnerability:** India's digital economy **has flourished because of citizens' digital integration, but it has also created a vulnerability to data theft.**
    - The government expected to remove all impediments to "data flows" across various sectors. This narrative resulted in **tech-industries paying only lip service to data protection.**
- **Parking Data Abroad:** In almost every sector, the **rush towards digitisation has led to collaborations with** application service providers **outside India,** so that customers can access the best apps and services as quickly as possible.
    - Having **foreign-sourced hardware and software**, or having **terabytes of data parked on servers outside India,** pose a threat to our national cyberspace.
- **Proxy Cyber Attacks:** Artificial intelligence (AI) is capable of producing autonomous lethal weapon systems that can kill and destroy lives and targets **without the involvement of humans.**
    - National security is also compromised by the vulnerability to illegal activities such as **fake digital currency and** intellectual property thefts through use of the latest **cyber technologies.**
- **China's Quantum Lead:** China's quantum advances expand the **spectre of quantum cyberattacks against India's digital infrastructure,** which already faces a barrage of attacks from Chinese state-sponsored hackers.
    - India's dependence on foreign, **particularly Chinese hardware, is an additional vulnerability.**

What are the Present Government Initiatives Related to Cyber Security?

- **Indian Cyber Crime Coordination Centre (I4C)**
- **Indian Computer Emergency Response Team (CERT-In)**
- **Cyber Surakshit Bharat**
- **Cyber Swachhta Kendra**
- **National Cyber security Coordination Centre (NCCC)**

What Should be the Way Forward?

- **Cyber-Awareness: Education** is one of the important sectors for **dissemination of information on prevention of cyber-crimes** and reiterated that the young population can act as a **force multiplier to be aware of their engagement in cyberspace and create an ecosystem for cyber security** and to **prevent cyber-crimes.**
- **Tech-Diplomacy for Secure Global CyberSpace:** To tackle **emerging cross-border cyber threats** and move towards a secure global cyberspace, **India should strengthen its diplomatic partnerships with advanced economies and techno-democracies.**
- **Cooperative Federalism and Cybersecurity**: **Police and public order** are included on State Lists, so states must ensure that law enforcement is well-equipped to deal with cybercrime.
    - The **IT Act and major laws** are enacted centrally, so the central government can develop **uniform statutory procedures for law enforcement.**
    - Also, the **centre and states must commit adequate funds** to develop much-needed **cyber infrastructure.**
- **Mandatory Data Protection Norms:** All government and private agencies dealing with **personal data** should be required to **adhere to mandatory data protection norms.**
    - To ensure compliance with norms, **relevant authorities should conduct regular data protection audits.**

Drishti Mains Question

As modern Cyber Technology multiplies India's capacity in different sectors, it also adds to its vulnerabilities. Comment.

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)**