Securing India’s Cyberspace

This editorial is based on **“Securing India’s cyberspace from quantum techniques”** which was published in The Indian Express on 17/10/2022. It talks about the issues related to India’s cyberspace and rising quantum technology.

For Prelims: WannaCry, Cloud computing, 5G, E-Commerce, Quantum technology, Man in Middle Attack, Denial of Service (DOS) Attack, CRISPR, National Cyber Security Policy, 2013, Indian Computer Emergency Response Team (Cert-In).

For Mains: Major Terminologies Related to Cyber Threats, Challenges Related to India’s Cyber-Space, National Mission on Quantum Technologies and Applications.

Unprecedented growth in technology has blurred boundaries by connecting people and transforming governance. The **Digital India Programme** launched by the Government of India, which aims to provide **government services digitally and promote** digital literacy**,** is driving this transformation by building world-class digital infrastructure for the country.

However, there exist gaps **which can be exploited by the adversaries and deprive us of the benefits of digital technologies**. Cyber adversaries are becoming more sophisticated and resourceful. Among more than 100 countries that were hit by WannaCry **(an advanced** ransomware attack**), India was the third worst affected.**

With **technology protocols still being developed** and evolving at a gradual pace, **it is very difficult to avoid such cyber-attacks** and considering the fact that India is moving towards a digitised life where the existence will highly depend on elements like **cloud computing**, **5G in telecom**, **e-Commerce** **and** **quantum technology** etc. it is **imperative to keep a check on loose ends.**

What are the Major Terminologies Related to Cyber Threats?

- **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.**
- **Ransomware:** It is a form of malware which first **hijacks a computer’s data and thereafter posts a message demanding money** (usually in the form of bitcoins) to restore it.
- **Spyware:** Malware that **secretly monitors a user’s computer** activity.
- **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 Cyber-Space?

- **Internet Polarisation:** Currently there are **no common rules and norms that govern the internet;** therefore, it enables the **illegitimate prioritisation of some websites over others** through **ad-based technology,** forcing viewers to browse and **deteriorating internet democracy.**
- **Multiplying Capacity, Adding Vulnerability: Artificial Intelligence (AI)** along with advances in new generation provide us with immense power to redefine and restructure lives.
    - **AI is capable of producing autonomous lethal weapon system**s that can kill and destroy lives and targets without any human interference.
    - Vulnerability to illegal activities ranging from **selling drugs, fake currency and** intellectual property thefts also **posing major concern to national security.**
- **Global Threat of Cyber Warfare and Internet Battlefields: Data has become a new "oil" for the world, which can be used to ignite** cyberwarfare **at any time.** All the major power centres in the world are converting their cyberspace into a warfare-ready domain.
    - The **Internet** is at high risk of potentially being used as an **intelligence gathering platform.**
- **Inter-Dependent Cyberspace:** The supply chains are increasingly **interconnected.** Increasingly, **personal data-based platforms are taking centre stage.** This makes a **company's security wall thin,** and **data breaches are becoming more common.**
- **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.
- **No Legal Backing for Internet of Things(IoT):** With the **Internet of Things** now becoming the backbone of modern ventures, organisations and even basic ways of living, it is worrying that **India has no dedicated law for IoT.**
- **Rising Fake News Concern:** Increasing **access to free information online,** either through news-based apps and services or messages forwarded via **social media** platforms, also known as **internet intermediaries**, has resulted in the rise of fake news with often grave consequences in the real world.
    - **Lack of awareness and digital illiteracy** makes them even more vulnerable.

What are the Recent Government Initiatives for Cyber Security?

- **National Cyber Security Policy, 2013**
- **National Cyber Security Coordination Centre (NCCC)**
- **Cyber Swachhta Kendra**
- **Indian Computer Emergency Response Team (Cert-In)**

What Should be the Way Forward?

- **Quantum-Resistant system:** With traditional internet models at risk and considering the **increasing potential of military applications of quantum technology**, the deployment of **“quantum-resistant” systems in India** is the **need of the hour.**
    - The **Union Budget 2020-21** had proposed to spend Rs 8,000 crore on the newly launched **National Mission on Quantum Technologies and Applications is a welcome step in this direction.**
- **Towards Techno-Diplomacy:** India needs to strengthen its diplomatic **partnerships with other “techno-democracies'' countries** and advanced economies **to pool in the ideas and resources** for tackling emerging **cross border cyber threats and move towards secured global cyberspace.**
- **Linking Cooperative Federalism with Cybersecurity:** State Lists include police and public order, and therefore, states must ensure that police are well equipped to deal with cybercrime.
    - In addition, **since the** IT Act **and major laws are centrally enacted, the central**

government can look forward to developing uniform statutory procedures for law enforcement agencies.
    - Also, the centre and states must commit adequate funds to develop much-needed cyber infrastructure.
- **Enhancing Cyber Forensic Laboratories:** In order to keep pace with new technologies, cyber forensic laboratories need to be upgraded.
    - The **National Cyber Forensic Laboratory and the Cyber Prevention, Awareness and Detection Centre (CyPAD)** initiative of the Delhi Police are good examples.
- **Blending Ethical Values with Cybersecurity:** Technology has reached a stage where we need **global understanding and commonality of** ethics and morality**,** for more judicious use of cyber resources for individual and global good.
- **Filling the Infrastructural Gaps:** There is need to **expand India's cyberspace by filling the physical infrastructural gaps a**nd move towards **cyber-inclusion amalgamated with cyber-security measures.**
- **Cyber-Awareness Campaign:** In a world of **e-governance, where government is becoming e-government, citizens are being e-citizens,** there is need to make strides to promote **cyber-awareness among citizens**, including **safe online transactions and not sharing personal information with unauthentic websites.**

Drishti Mains Question

Unprecedented growth in technology has blurred the boundaries of cyberspace across the world. Highlight major challenges related to India's cyber-space.

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)**

//
