India’s Cyber Ecosystem

This editorial is based on “India’s cyber infrastructure needs more than patches” which was published in The Hindu on 03/09/2022. It talks about India's Cyber Ecosystem and gaps existing in its cyber infrastructure.

For Prelims: Cyber- Wars, Cyber-Terrorism, Information Technology, Indian Cyber Crime Coordination Centre (I4C), Internet of Things (IoT), Computer Emergency Response Team (CERT-In), National Cyber Forensic Lab, IT Act, 2000.

For Mains: Challenges Related to Cyber Security in India, Existing Provisions for Cyber-Security in India.

If the ancestors of human beings were to wake up today after their long sleep of centuries, they would be amazed to see the **revolutionised and** digitalised world of contemporary times.

The advent of **digitalisation** has affected every sphere of human lives to a to a considerable extent. However, **information technology** use has been proving to be a **double-edged sword** as cyber crime **and threats** have increased dramatically.

As India is moving towards more and more digitalization in all spheres, cyberspace has become a serious concern of **National Security**. According to the **National Crime Records Bureau (NCRB)** data, **India reported 52,974 cases of cybercrime in 2021,** an increase of over **5 per cent from 2020** (50,035 cases) and over **15 per cent from 2019** (44,735 cases).

Though the Government of India has taken steps for ensuring **Cyber-Security** that include the setting up of the **Indian Cyber Crime Coordination Centre (I4C)** under the **Ministry of Home Affairs** to deal with all types of cybercrime, **much needs to be done to plug the infrastructural deficit**.

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**.
    - **Cyber-physical systems** integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.
        - **Examples:** Industrial control systems, water systems, robotics **systems**, smart grid etc.
    - **Critical Information Infrastructure:** The **Information Technology Act of 2000** defines **Critical Information Infrastructure** as a computer resource, the incapacitation or destruction of which shall have debilitating impact on **national security, economy, public health or safety**.

- **Cyber Threats:**
  - Malware**, Viruses,** Trojans**,** Spywares**, Backdoors,** which allow remote access.
  - **DDoS (Distributed Denial of Service)**, which **floods servers** and networks and makes them unusable.
  - **DNS (Domain Named System)** poisoning attacks which compromises the DNS and **redirect websites to malicious sites**.
- **Major Areas covered in Cyber Security are:**
  - **Application Security:** To **protect applications** from threats that can come through flaws in the application design
  - **Information Security:** To **protect information** from unauthorised access to avoid identity theft and to protect privacy.
  - **Disaster Recovery:** It is a process that includes **performing risk assessment**, establishing priorities, developing recovery strategies in case of a **cyber disaster**.
  - **Network Security:** includes activities to protect the **usability, reliability, integrity** and safety of the network.
    - Effective network security targets a variety of threats and **stops them from entering or spreading on the network**.

What is Cyber-Crime Vs Cyber-Terrorism Vs Cyber-War?

- **Cyber-Crimes:** Cyber crime is **unlawful acts wherein the computer is either a tool or a target or both**.
  - Cyber crimes can involve **criminal activities** that are traditional in nature, such as **theft, fraud, forgery, defamation and mischief etc**.
- **Cyberwars:** Cyberwar is an **organised effort by a nation state to conduct operations in cyberspace against foreign nations**.
  - Included in this category is the **Internet's use for intelligence** gathering purposes.
- **Cyber-Terrorism:** Cyberterrorism is the **convergence of cyberspace and** terrorism.
  - It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to **intimidate or coerce a government or its people** in furtherance of **political or social objectives**.

What are the Challenges Related to Cyber Security in India?

- **Profit-Friendly Infrastructure Mindset:** Post **liberalisation**, the **Information Technology (IT)**, electricity **and** telecom **sector** has witnessed large investments by the private sector. However, their inadequate focus on cyber attack preparedness and recovery in regulatory frameworks is a cause of concern.
  - All **operators are focused on profits,** and do not want to invest in infrastructure that will not generate profits.
- **Absence of Separate Procedural Code:** There is **no separate procedural code** for the investigation of cyber or computer-related offences.
- **Trans-National Nature of Cyber Attacks:** Most cyber crimes are trans-national in nature. The **collection of evidence from foreign territories** is not only a difficult but also a tardy process.
- **Expanding Digital Ecosystem:** In the last couple of years, India has traversed on the path of **digitalising its various economic factors** and has carved a niche for itself successfully.
  - Latest technologies like **5G** and the **Internet of Things (IoT)** will increase the coverage of the internet-connected ecosystem.
  - With the advent of digitalisation, **paramount consumer and citizen data** will be stored in digital format and transactions are likely to be carried out online which makes **India a breeding ground for potential hackers** and cyber-criminals.
- **Limited Expertise and Authority:** Offences related to **crypto-currency** remain **under-reported** as the capacity to solve such crimes remains limited.
  - Although most **State cyber labs** are capable of analysing hard disks and mobile phones, they are yet to be recognized as **'Examiners of Electronic Evidence'** (by the central government). Until then, **they cannot provide expert opinions on electronic data**.

What are the Current Provisions for Cyber-Security in India?

- Indian National Security Council**:** To shape the ecosystem related to cyber policy.
- National Cyber Security Strategy**:** To focus on security in the early stages of design in all digitisation initiatives.
- Computer Emergency Response Team (CERT-In)**:** For alerts regarding cybersecurity breaches and issues.
- Indian Cyber Crime Coordination Centre (I4C)**:** To handle several issues regarding cybercrime in a comprehensive and coordinated manner.
- Cyber Swachhta Kendra**:** To create a secure cyberspace by detecting botnet infections in India

What Should be the Modern Day Solutions For Modern Day Problems of Cyber-Threats?

- **Centre-State Nexus Towards Secure Cyberspace:** With **police and public order being in the** State List, the primary objective to check crime and create the necessary cyberinfrastructure lies with States.
    - At the same time, with the IT Act **and major laws being central legislations**, the central government should look forward to evolving **uniform statutory procedures for the law enforcement agencies**.
    - Centre and States must not only work in tandem and **frame statutory guidelines to facilitate investigation of cybercrime** but also need to commit sufficient funds to develop much-awaited and required **cyber infrastructure**.
- **Upgrading Cyber Labs:** Cyber forensic laboratories should be upgraded with the advent of new technologies.
    - **National Cyber Forensic Lab** and the **Cyber Prevention, Awareness and Detection Centre (CyPAD)** initiative of the Delhi Police, is a good step in this direction.
- **Capacity Building:** It is essential to build up sufficient capacity to deal with cybercrime. It could be done either by **setting up a separate cyberpolice station** in each district or range, or **having technically qualified staff in every police station**.
- **Reforming the Justice Delivery System:** As electronic evidence differs greatly from evidence of traditional crimes when it comes to breach of privacy, it is essential to **develop standard and uniform procedures to deal with electronic evidence** to ensure time-bound justice in order to maintain the safety of Indians as well as the infrastructure.
- **Developing Cyber-Defence Mechanism:** A holistic approach for dealing with cyber conflict is necessary, whether it's conducting **cyber search operations** or **extending the scope of countermeasures against cyber attacks**.
    - A **clear public posture on cyber defence** and warfare **boosts citizen confidence** thus enabling a more **engaging, stable and secure** cyber ecosystem.

Drishti Mains Question
As India moves towards Digitised Ecosystem, cyberspace has become a serious concern of National Security. Critically Analyse.

UPSC Civil Services Examination, Previous Year Question

Q.1 The terms 'WannaCry, Petya and EternalBlue' sometimes mentioned in the news recently are related to (2018)

(a) Exoplanets

(b) Cryptocurrency

(c) Cyber attacks

(d) Mini satellites

Ans: (c)

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)