Critical Information Infrastructure

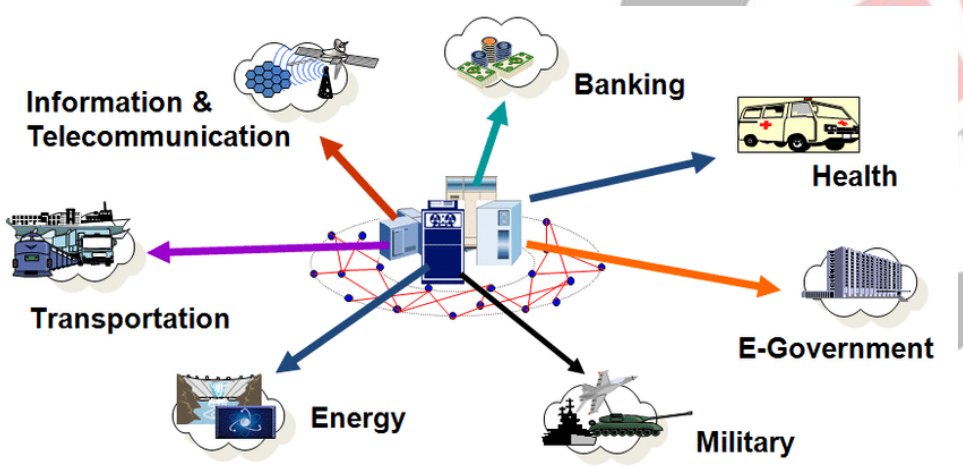
For Prelims: Critical Information Infrastructure, Cyber Attacks, NPCI, IT 2000

For Mains: Critical Information Infrastructure, Cyber Attacks, Cyber Security and Cyber Welfare

Why in News?

Recently, the Union Ministry of Electronics and IT (MeitY) has declared IT (Information Technology) resources of **ICICI Bank, HDFC Bank and** NPCI(National Payments Corporation of India) as **'critical information infrastructure'.**

//



What is 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.**
- The **government,** under **the IT Act of 2000**, has the **power to declare** any data, **database, IT network or communications infrastructure as CII** to protect that digital asset.
- Any person who secures access or attempts to **secure access to a protected system in violation of the law** can be punished with **a jail term of up to 10 years.**

Why is CII Classification and Protection Necessary?

- **Global Practice:** World over governments have been moving with alacrity to protect their critical information infrastructure.
- **Backbone of Countless Critical Operations:** IT resources form the backbone of countless critical operations in a country's infrastructure, and given their interconnectedness, disruptions can have a cascading effect across sectors.

- **IT Failure leads to Crippling other Sectors:** An information technology failure at a power grid can lead to prolonged outages crippling other sectors **like healthcare, banking services etc.**
    - **Example: Wave of Denial-of-Service Attacks in Estonia:** In 2007, a wave of denial-of-service attacks, allegedly from Russian IP addresses, hit major Estonian banks, government bodies – ministries and parliament, and media outlets. It was cyber aggression of the kind that the world had not seen before. The attacks played havoc in one of the most networked countries in the world for almost three weeks.
    - **A Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
- **Case of India:**
    - In October, 2020 as India battled the **pandemic, the electric grid supply to Mumbai suddenly snapped** hitting the mega city's hospitals, trains and businesses.
    - Later, a study by a US firm claimed that this power outage could have been a **cyber-attack**, **allegedly from a China-linked group**, aimed at **critical infrastructure**. The government, however, was quick to deny any **cyber-attack** in Mumbai.
    - But the incident underlined the possibility of hostile state and non-state actors **probing internet-dependent critical systems** in other countries, and the necessity **to fortify such assets.**

How are CIIs protected in India?

- **NCIIPC as Nodal Agency:**
    - Created in January 2014, the **National Critical Information Infrastructure Protection Centre (NCIIPC)** is the nodal agency for taking all measures to protect the nation's critical information infrastructure.
- **Mandate of NCIIPC:**
    - It is mandated to **guard CIIs from unauthorized access**, modification, use, disclosure, disruption, incapacitation or distraction.
    - It will **monitor and forecast national-level threats to CII** for policy guidance, expertise sharing and situational awareness for early warning or alerts.
    - In the event of **any threat to critical information infrastructure the NCIIPC may call for information and give directions to the critical sectors** or persons serving or having a critical impact on Critical Information Infrastructure.
- **Basic Responsibility:**
    - The basic responsibility for protecting the CII system **shall lie with the agency running that CII.**

UPSC Civil Services Examination, Previous Year Questions

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centers
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)

Exp:

- According to section 70B of the Information Technology Act, 2000 (IT Act), the Union Government

by notification should appoint an agency named Indian Computer Emergency Response Team (CERTIn) to serve as the national agency for incident response.

- The Union Government under section 70B of the IT Act, 2000 established and notified rules of CERT-In in 2014. According to Rule 12(1)(a), it is mandatory for service providers, intermediaries, data centers and corporate bodies to report cyber security incidences to CERT-In within a reasonable time of occurrence of the incident. Hence, 1, 2 and 3 are correct.
- **Therefore, option (d) is the correct answer.**

Source: IE