Why India needs an updated cybersecurity strategy

Context:

- In mid-June Australia had to ward off its biggest cyber threat with the attack targeting everything from public utilities to education and health infrastructure.

What is the need for cyber security?

- while each person had 1.7 networked devices in 2014, this is up to seven today. This requires an updated cyber security apparatus
- Increased Digital usage in Post-COVID world: Financial services, payments, health services, etc are all connected to digital mediums and this is expected to increase in post-COVID times
- Increased frequency of cyber-attack: In 2018, Pune-based Cosmos Bank lost Rs 94 crore in a malware attack. In 2019, the Kudankulam plant was attacked using malware.
- Securing Data: Data is referred to as the currency of the 21st century and due to its bulk creation owing to India's population, several international companies (Google, Amazon etc.) are trying to have access to it.
- Increasing Complexity: With growing usage of artificial intelligence (AI), machine learning (ML), cloud computing and Internet of Things (IoT), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature.

- National Security Imperative: With countries resorting to digital warfare and hackers targeting business organisations and government processes, India needs comprehensive cybersecurity guidelines and standards.

What are the challenges in India's cyber security approach?

Lack of Coordinated Cyber approach:

- Although India was one of the few countries to launch a cybersecurity policy in 2013, not much has transpired in terms of a coordinated cyber approach
- Countries like US, Singapore, and the UK where there is a single umbrella organisation dealing in cybersecurity,
- However, India has 36 different central bodies—most ministries have their own—that deal with cyber issues, and each has a different reporting structure;
- Each state government has its own CERT (Computer Emergency Response Team).

National Cyber Security Strategy 2020 yet to be announced:

- This was needed to devise a cyber-readiness roadmap for organisations and the government for cyber-readiness
- India doesn't have the 'active cyber defence' like the EU's General Data Protection Regulation or USA's Clarifying Lawful Overseas Use of Data (CLOUD) Act.

Lack of pro-activeness:

- While CERT-IN has responded to cyber threats, it has been late in conducting security checks, and often has released advisories once an attack has taken place.
- In the case of WhatsApp and Pegasus, CERT-IN only came in after others had warned of the possibility of individuals being compromised.

Inadequate modernisation of Computer systems:

- The government itself uses legacy systems which are vulnerable to cyberattacks.
- Countries like China and Singapore, in the meanwhile, have progressed towards creating cyber defence networks.

Dependency on Foreign Players for Cyber Security Tools:

- India lacks indigenisation in hardware as well as software cybersecurity tools
- This makes India's cyberspace vulnerable to cyberattacks motivated by state and non-state actors.

Way ahead?

- **Integrated Approach**: Given increasing dominance of mobile and telecommunication, both National cyber security policy and National Telecom Policy will have to effectively coalesce to make a comprehensive policy for 2030.
- Cyber Security in Training & Education: Educational institutions, government bodies and private industries must incorporate courses on cybersecurity.
- Modernising Cyber Infrastructure: India should not wait for an attack to upgrade its infrastructure.