# Chinese Cyber-Espionage threat Against India

**Why in the news? On 6 April 2022, American cybersecurity firm, Recorded Future revealed that Chinese state-sponsored hackers had targeted India's power grids in Ladakh. India is not alone. Several countries, including the Netherlands, United Kingdom, Australia, and the United States, and businesses like Vodafone and Microsoft have revealed China's unabated campaign to steal trade and other sensitive data.**

## How China Affects the Critical Infrastructure?

- China has even utilized overseas business contracts and activities to pursue its cyber-espionage campaign.
- China uses cyber espionage to fulfill several objectives. According to the latest US intelligence community assessment, these cyber-espionage operations often target those sectors which provide potentially rich "follow-on opportunities for intelligence collection, attack, or influence operations." China uses information ferreted from these sources:
    1. to boost its domestic manufacturing capabilities
    2. to produce lower-cost imitations of popular western brands/products and, thereby, attain a competitive advantage.
- While India has so far not proved such an attractive target for China's commercial cyber espionage, things may be changing. In March 2021, a Singapore-based company, CyFirma, revealed that a Chinese state-backed hackers' group had targeted the information technology systems of two Indian vaccine makers—Bharat Biotech and the Serum Institute of India (SII).
- The targeting of the power grids in Ladakh in the middle of the prolonged border stand-off is clearly aimed at sending a political message and signaling that Beijing can open other non-military fronts in the bilateral security competition. Pertinently, this is the second such attack on India's power sector by Chinese hackers.
- Moreover, the extent of Chinese persistence in targeting India is shown by the Advanced Persistent Threat 30 (APT30) vector. This threat actor's espionage operation ran for a decade before its discovery in 2015.
- In responding to this widening Chinese cyber-espionage activity, India is hardening its cyber defenses and undertaking its own offensive cyber operations. But it needs to do more. For one, it needs to start outlining technical evidence to attribute these attacks to Chinese state-sponsored

hackers—something which the national security establishment has resisted, even as the technical community in India and abroad has presented that evidence.

## India's Responsive System

- New Delhi also needs a dedicated mechanism to monitor these offensive operations. While respective intelligence and security agencies do trace foreign spying campaigns against India, this kind of cyber activity is often treated as a cyber breach or incident, focusing on the target and activity, but without linking it to the broader Chinese cyber-espionage campaign, the involvement of state-sponsored hacking groups and the trends in their targeting of Indian computer networks.
- Defense Cyber Agency can take the initiative to collaborate with the civilian technical community to track these operations. This will send a definite message that Beijing's mischief is not going unnoticed and is being systematically tracked as part of India's comprehensive cyber posture.

**Sources:**
https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/



Q1. Consider the following sectors:
1. Telecom
2. Power
3. Traffic Signals
4. IT

Which of the above are considered as critical infrastructure?
A. 1, 2 and 3 only
B. 2, 3 and 4 only
C. 1, 2 and 4 only
D. 1, 2 , 3 and 4

Answer - A
**Critical infrastructure is that infrastructure or essential service which is required to be functional at all times, 24×7. This includes telecom networks, air traffic control, traffic signals, nuclear reactors, power plants, pipelines.**