Twitter Thread by ✍■



✍■
@Aamani_03

Part 2: Cyber Warfare

If you think we might only see wars happening on land, air or water then you're wrong, wars aren't limited to these now.

There's Cyber Space too, this is generally termed as ‘The 5th Generation Warfare’

> You ever thought about what's cyber fraud, theft, warfare, terr0rism?
>
> And how good or bad is India in tackling these crimes?
>
> First let's first see what makes India vulnerable to cyber threats.
>
> — \u270d\ufe0f (@Aamani_03) June 25, 2021

India has already seen a sample of it recently during the Galwan Valley issue

Chinese govt backed hacker group called ‘Red Echo’ had done massive cyber attacks on India's critical infrastructure.

Due to the alertness of our ‘Cyber Response Team’ they couldn't cause much damage.

Wondering what happened?

A grid failure on 12 Oct '20 resulted in a major power outage in #Mumbai & its surrounding areas, affecting electricity supply, local trains etc.

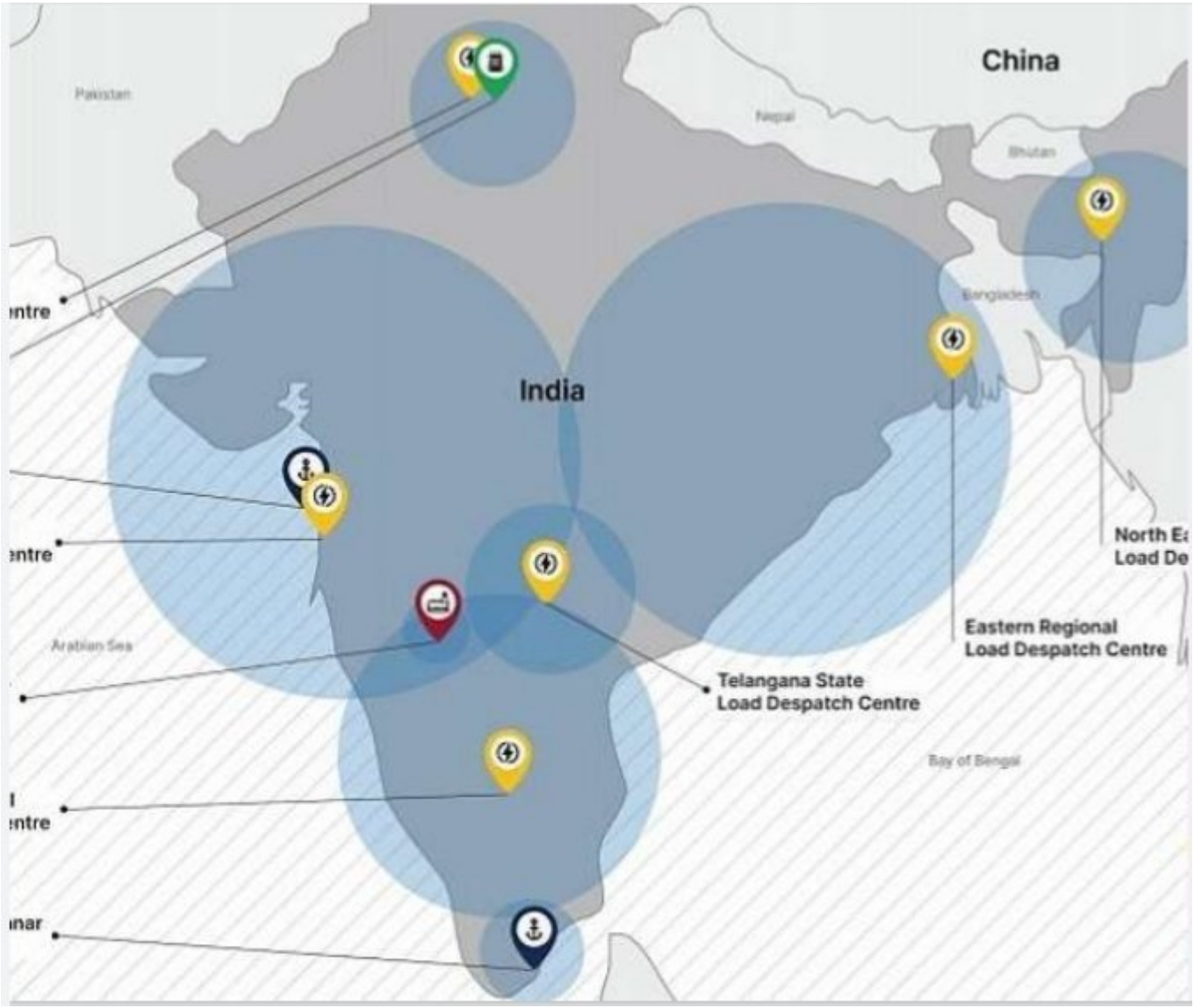
It took hours for power supply to be gradually restored in a phase-wise manner.

https://t.co/VS2swghLXo

US based cyber security firm ‘Recorded Future’ released a report titled, ‘China-linked Group #RedEcho targets Indian Power Sector Amid Heightened Border Tensions’ that points to inflow of Chinese malware into India's critical infrastructure systems that manage electricity supply.

The report identifies RedEcho — a China based advanced persistent threat(APT) group — as the entity behind attempts to infiltrate India's power grids.

Recorded Future also stated that ‘Red Echo’ had targeted 10 vital nodes in India’s power distribution system & 2 seaports.



What were Red Echo’s targets?

Recorded Future lists these as suspected targets:

• Power System Operation Corporation Limited
• NTPC Limited
• NTPC Kudgi STPP
• Western Regional Load Despatch Centre
• Southern Regional Load Despatch Centre

• North Eastern Regional Load Despatch Centre
• Eastern Regional Load Despatch Centre
• Telangana State Load Despatch Centre
• Delhi State Load Despatch Centre
• DTL Tikri Kalan (Mundka)

• Delhi Transco Ltd (substation)
• V. O. Chidambaranar Port
• Mumbai Port Trust

China's #RedEcho used server #AXIOMATICASYMPTOTE to introduce #ShadowPad a backdoor Trojan malware into India's critical Infrastructure.

Security firm Kaspersky says ShadowPad is built to target supply-chain infrastructure in sectors like transportation, telecom, energy & more.

Recorded Future says the kind of infrastructure sought to be accessed by RedEcho, such as Regional Load Despatch Centres, has minimal espionage possibilities.

So why did they choose it??

RedEcho introduced #ShadowPad into India's critical Infrastructure but didn't activate, their plan was just to introduce it and activate all at the same time when needed causing a massive damage to India.

But due to alertness of our Cyber Response Team their plan was failed on time without causing much damage.

Now can you imagine the damage of hacked servers? Of China controlling our electricity?

Not China alone, it can be any other country, any other org!