Chinese cyber-attack foiled: Power Ministry

The Union Power Ministry said that the State-sponsored Chinese hacker groups targeted various Indian power centres.

- It was stated that the Chinese state-sponsored threat actor group known as Red Echo is targeting the Indian Power sector's Regional Load Dispatch Centres (RLDCs).
- These groups have been blocked after government cyber agencies warned them about their activities.
- It also confirmed that no data breach/data loss has been detected due to these incidents.

Officials said they had been warned about the threat from a malware called "ShadowPad" in November 2020 by the -

- (MeitY's-CERT-in) &
- by the NTRO's National Critical Information Infrastructure Protection Centre (NCIIPC) in February 2021, of the threats, weeks before the Recorded Future report was released.

Patching the gaps in India's cybersecurity

Recently, the Union Power Ministry said that State-sponsored Chinese hacker groups targeted various Indian power centres.

- United States-based cybersecurity firm raised the possibility that the power outage in Mumbai could have been the result of an attack by a Chinese state-sponsored group.

Institutional security:

- In the last two decades, significant efforts have been made by India to craft institutional machinery focusing on cyber resilience spanning several government entities.
- The National Security Council, usually chaired by the National Security Adviser (NSA), plays a key role in shaping India's cyber policy ecosystem.
- The NSA also chairs the National Information Board, which is meant to be the apex body for cross-ministry coordination on cybersecurity policymaking.
- The National Critical Information Infrastructure Protection Centre established under the National

Technical Research Organisation in January 2014 was mandated to facilitate the protection of critical information infrastructure.

•In 2015, the Prime Minister established the office of the National Cyber Security Coordinator who advises the Prime Minister on strategic cybersecurity issues.

•India's Computer Emergency Response Team (CERT-In), which is the nodal entity responding to various cybersecurity threats to non-critical infrastructure comes under the (MEITY).

•The MoD has recently upgraded the Defence Information Assurance and Research Agency to establish the Defence Cyber Agency, a tri-service command of the Indian armed forces to coordinate and control joint cyber operations, and craft India's cyber doctrine.

•The MHA oversees multiple coordination centres that focus on law enforcement efforts to address cybercrime, espionage and terrorism.

•The MEA coordinates India's cyber diplomacy push, both bilaterally with other countries, and at international fora like the United Nations.

Problems in Institutional Framework:

- The institutional framework, while seeking to create an 'all of government' approach to countering and mitigating cybersecurity threats at the national level, has also resulted in concerns around:
  - Effective coordination
  - Overlapping responsibilities
  - Lack of clear institutional boundaries and accountability.

India has been a target earlier:

- India has been attacked by suspected Chinese state-sponsored groups multiple times in the past.
- In 2009, a suspected cyber espionage network dubbed GhostNet was found to be targeting the Tibetan government in exile in India, and many Indian embassies.
- The vast cyber-espionage operation extensively targeted Indian entities, including military establishments, news publications, and even the National Security Council Secretariat itself.

- There were a number of subsequent attacks that targeted India. Such as:
  - Stuxnet which had also taken down nuclear reactors in Iran.
  - Suckfly, which targeted not just government but also private entities including a firm that provided tech support to the National Stock Exchange.
  - Dtrack which first targeted Indian banks, and later the Kudankulam nuclear power plant (Tamil Nadu) in 2019.

Reports not made public:

- Neither the report from the Shadow Network investigation, nor any other, has ever been tabled in Parliament, nor even an edited version made public.

China's help in deconstructing the attacks:

- While there is much evidence to show that Chinese state-sponsored groups were responsible for many of these attacks, Chinese cybersecurity agencies have also helped the security community

in dismantling the infrastructure behind some of these attacks.

False flag attacks:

- Documents released by WikiLeaks show that groups such as the Central Intelligence Agency's UMBRAGE project have advanced capabilities of misdirecting attribution to another nation-state ("false flag attacks").
- They leave behind false fingerprints for investigators to find.

Way Forward:

1. Making the reports public:

- Appraising lawmakers of the scale and depth of the damage wrought is critical to enabling meaningful public discussions and crafting a robust response.

2. Strengthening the Institutional Framework:

- Given that the question of attribution of a certain cyberattack is questionable, a robust institutional posture and political acumen in publicly dealing with these issues are necessary.

•There is a need for clarity about the institutional framework in India's National Cyber Security Strategy, which has been drafted by the NSC and is yet to be released.

•Ensuring coherence and coordination between these different actors should be its primary goal.

3.Doctrine on cyber conflicts:

•India is also yet to clearly articulate a doctrine that holistically captures its approach to cyber conflict. That is, for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber-attacks.

•Unlike India's approach to other global security regimes like the 'No First Use' nuclear posture, the rules of engagement for targeted cyber-attacks are unclear.

•While it might seem like secrecy and ambiguity would provide a tactical advantage when engaging in cyber operations, in an increasingly unstable geopolitical scenario, the absence of a credible cyber deterrence strategy is undesirable.

•In such a scenario, states and non-state actors alike remain incentivised to undertake low-

scale cyber operations for a variety of purposes – espionage, cyber-crime, and even the disruption of critical information infrastructure.

4. Define the red lines:

- India has been an active participant in processes within the First Committee of the UNGA dealing with issues of disarmament and international security.
- While the Indian delegation has made public some of their intervention, India's long-term strategic thinking on core issues of debate at these fora remains relatively unknown.
- India must involve itself in a precise articulation of how international law applies to cyberspace.
- This could mould the global governance debate to further India's strategic interests and capabilities.

'Red Echo' over India

United States-based cybersecurity firm Recorded Future had reported that a group linked to the Chinese government, which it called 'Red Echo', had targeted 10 vital nodes in India's power distribution system and two seaports.

- It has raised the possibility that the massive power outage in Mumbai in October 2020 could have been the result of an attack by this Chinese state-sponsored group.
- The Maharashtra Power Minister Nitin Raut has announced that a State Cyber Cell probe found 14 Trojan horses in the servers of the Maharashtra State Electricity Transmission Company, with the potential to disrupt power distribution.

Modus operandi:

- RedEcho was using the AXIOMATICASYMPTOTE server infrastructure to carry out its intrusions into the networks of Indian organisations,
- AXIOMATICASYMPTOTE servers act as command-and-control centres for a malware known as ShadowPad.

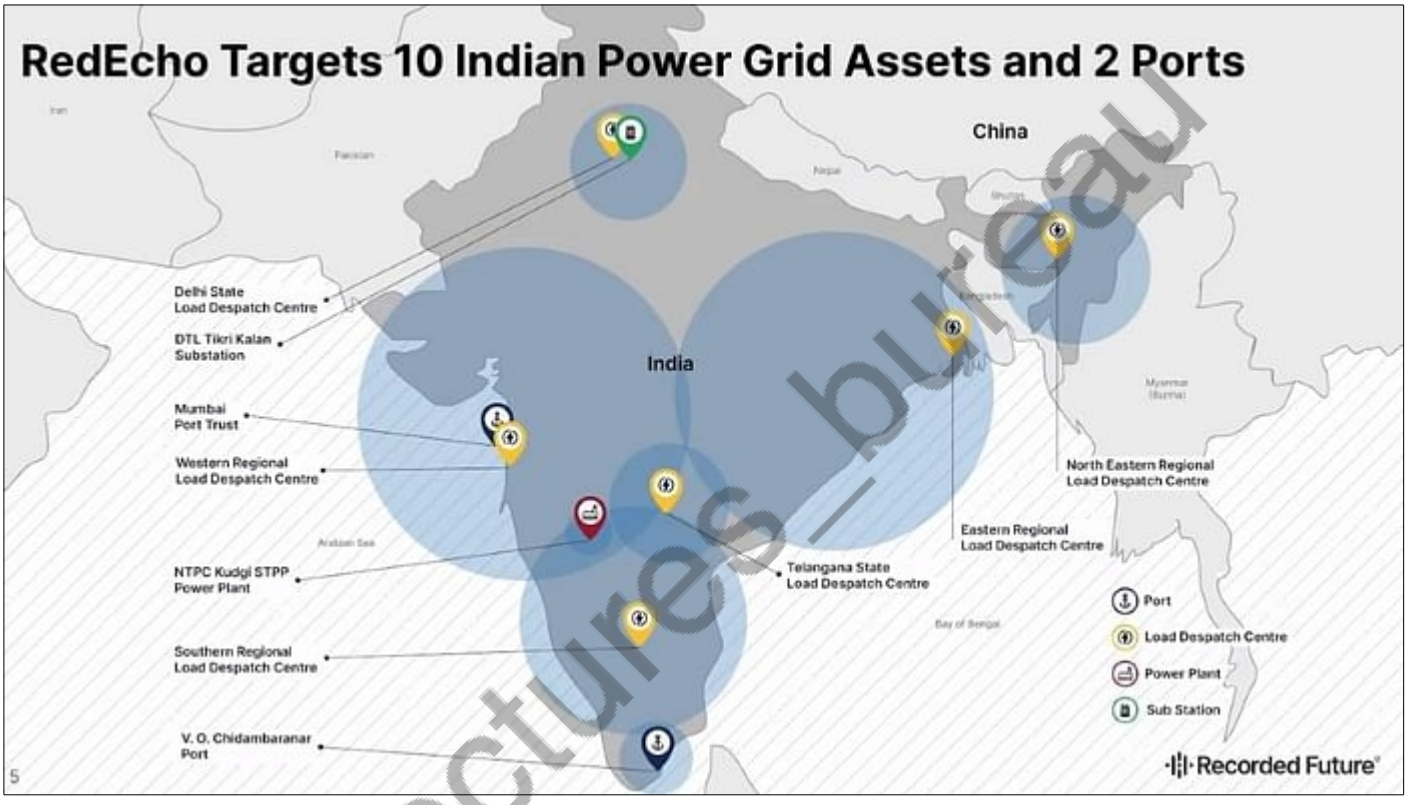
- ShadowPad is a backdoor Trojan malware, which means it opens a secret path from its target system to its command-and-control servers. Information can be extracted or more malicious code delivered via this path. ShadowPad is built to target supply-chain infrastructure in sectors like transportation, telecommunication, energy and more.
- Trojanised softwares, or softwares that have dangers hidden in them are the primary mode of delivery for ShadowPad.

The Chinese link:

- RedEcho group was Chinese state-sponsored.
- RedEcho has an overlapping modus operandi with several other known Chinese groups such as APT41, Winnti group and Barium.
- Many security firms have noted with high confidence that 'APT41' carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Targets:

- All the twelve targeted entities have been classified as critical infrastructure by the National Critical Information Infrastructure Protection Centre (NCIIPC).



Concerns:

- RedEcho's intrusions were part of a sustained strategic and targeted campaign against Indian organisations.
- Though the kind of infrastructure sought to be accessed by Red Echo, such as Regional Load Despatch Centres, has minimal espionage

* The world is hardly wired for cyber resilience

— Cyber attacks in the US

- 2020 — 'Solar Winds' cyberattack
  - believed to be Russian sponsored
  - Data breaches in several US Govt depts
- 2021 — Cyber attack by a Chinese group 'Hafnium'
  - exploited serious flaws in Microsoft's software ⇒ gained control over systems.
- 3 more attacks in 2021 in the US
  - ↳ Ransomware attack on Colonial Pipeline (main supplier of oil ↓ to US East Coast)
  - ↳ Phishing attack on 3000 e-mail accounts, targeting US-AID etc by another Russian backed group Nobellium.
  - ↳ Ransomware attack on a meat processing company (↓ paid millions in ransom)

— Cyber warfare ⇒ 5th domain of warfare

↳ earlier was limited to military & strategic targets

↳ but now even civilian targets.

- Zero day Vulnerabilities
  - ↳ cyber attacks capable of crippling an entire system & could lie undetected for a long time
  - ↳ Eg: Stuxnet → almost crippled Iran's Uranium enrichment programme.
  - ↳ Govts are busy erecting defences against such Zero day attacks.
  - ↳ While the civilian world is left to fend for itself.
    - Eg: Shamoon virus attack on Saudi Aramco
      - ↓
      - Wiped out memories of 30K computers

- Types of cyber attack in civilian domain -
  - Ransomware
    - ↳ A user or organization's critical data is encrypted so that they cannot access files, databases, or applications.
    - ↳ A ransom is then demanded to provide access.
    - ↳ Recovery costs in India has tripled.
    - ↳ Catastrophic situation for mid size companies
    - ↳ Banking & finance ⇒ most prone to attacks
    - ↳ Also oil, electricity grids & lately healthcare

- Phishing (incl. spear phishing)
  - ↳ Targets are contacted by email, phone or text messages by someone posing as a legitimate institution to lure individuals into providing sensitive data.
  - ↳ can result in identity theft & financial loss.
  - ↳ Spear phishing is targeted & personalised to a specific individual, group or institution

- Healthcare
  - ↳ Recent phenomena of cyber attacks in this sector
  - ↳ Health information being used by criminals as a commodity for trade.
  - ↳ Patients' data leaks creates risk for not just the individual but entire communities

- Motives behind cyber attacks -
  - Geopolitical transformation → nation-states
  - Profit seeking → (cyber criminals & terrorists)
  - Insider threats → discontentment with management

- Need for data protection -
  - Zero Trust based Environment
    - ↳ i.e. zero trust on end point devices,

identity & network to protect all sensitive data

- Software designed solutions
  ↳ perimeter security, secure gateways, cloud access security etc
- Threat intelligence platforms
- Using machine learning, AI & quantum computing
- Regular vulnerability assessments for public officials & company boards.

– Conclusion

↳ Value lies in the data and people are going to come after that data.

Disinformation is a cybersecurity threat

So far cybersecurity has mainly focused on protecting and defending computer systems, networks, and our digital lives from disruption.

The main focus of Cybersecurity has been to defend against cyberattacks executed using malware, viruses, trojans, botnets, and social engineering.

- There has been very little attention to the threat posed by disinformation attacks.
- Also, the industry has treated these attacks (cyberattacks and disinformation attack) independently and
- has separate teams working in silos to protect and defend against these attacks.
- The lack of coordination between teams leaves a huge gap that is exploited by malicious actors.

Disinformation:

- Disinformation attacks are the intentional dissemination of false information, with an end goal of misleading, confusing, or manipulating an audience.

- These attacks are commonly employed to reshape attitudes and beliefs, drive a particular agenda, or elicit certain actions out of a target audience.
- Nation-state actors, ideological believers, violent extremists, and economically motivated enterprises manipulate the information ecosystem to create social discord, increase polarisation, influence the outcome of an election, etc.
- Disinformation attacks can be employed through traditional media outlets such as TV channels or through social media.
- Disinformation attacks use manipulated, miscontextualised, misappropriated information, deep fakes, and cheap fakes.
- They pose the possibility of societal breakdown, business interruption, and violence in the streets.

Cognitive hacking:

- A cognitive hacking attack attempts to change the target audience's thoughts and actions, galvanise societies and disrupt harmony using disinformation.
- Disinformation is used for social engineering threats on a mass scale.

Examples of disinformation attacks and their impacts:

- QAnon spread false information about the U.S. 2020 presidential election. This led to rioting in the nation.
- Conspiracy theorists (in the United Kingdom, the Netherlands, Ireland, Cyprus and Belgium) burned down 5G towers because they believed it caused the novel coronavirus pandemic.
- COVID-19 disinformation campaigns have prevented people from wearing masks, using potentially dangerous alternative cures, and not getting vaccinated, making it even more challenging to contain the virus.

Factors aiding disinformation attacks:

- The advertisement-centric business modes and attention economy allow malicious actors to fill the information channels with disinformation with unprecedented speed and scale.
- Deep fakes add a whole new level of danger to disinformation campaigns.
- With the advent of social media, disinformation attacks have become increasingly widespread and

* Strategy meet discusses Chinese cyberattacks

- National Security Strategies Conference.

  - Chaired by Home Minister
  - Discussed the rising cyberattacks from China on critical installations.

- Concerns

  - Pakistani cyberattacks focused on stealing identity and personal data
  - Chinese hackers were more sophisticated.
  - Govt thwarted "state-sponsored" Chinese hacker groups targeting various Indian power centres in November 2020 and February 2021.
  - The U.S. cybersecurity firm Recorded Future discovered that Chinese may have deployed malware into Indian power grids and seaports .