

Cyber Attacks on Kudankulam Nuclear Unit

Why in news?

The Nuclear Power Corporation of India (NPCIL) admitted to a malware attack on one of the computers in Kudankulam nuclear power plant, Tamil Nadu.

What was the attack?

- The NPCIL admitted that computer systems at the Kudankulam nuclear power station had been infected with malware since early September 2019.
- The NPCIL infection is said to be caused by Dtrack.
- Dtrack is a Trojan virus that creates backdoors into computer networks.
- This was originally developed and commonly used by North Korean hackers with state backing.
- However, there are many variations of Dtrack, and the code may have been adapted by another group.

What were the other recent attacks?

- There have been multiple ransomware assaults on electric power billing systems across the world.
- Known cyberattacks on Indian power sector assets include the -
 - i. November 2017 malware attack on the Tehri Dam in Uttarakhand
 - ii. ransomware attack on West Bengal State Electricity Distribution Company in May 2017
 - iii. attack on Rajasthan's discom (February 2018)
 - iv. attack on Haryana's discoms (March 2018)
- Kudankulam is high on the list of such targets because it is both part of the nuclear programme, as well as the power grid.

What is the looming threat?

- Power grids are a tempting target for terrorists, in addition to being vulnerable in the case of hostilities with any other nation.
- Cyber-threat researchers estimate that a large number of assets on India's national power grid could be vulnerable to attacks.
- Cyber-attacks on nuclear installations and other power sector assets have become increasingly common.

- Some attacks have been carried out by state actors, while others are by cybercriminals to steal data, or extract ransom.
- The infamous Stuxnet attack on Iran's nuclear sector in 2010 is believed to have set back its nuclear programme by years.
- Evidently, an aggressive cyber-assault could cause a nationwide outage.

What are the challenges to ensuring security?

- The Indian Computer Emergency Response Team (CERT-In) claims to be aware of these vulnerabilities.
- It is also reported to have issued advisories in many instances.
- However, its scope is limited as it is the responsibility of the organisation owning the asset to protect it.
- It is also true that much of the equipment on the power grid is old.
- They are based on outdated chips with vulnerabilities that cannot be patched.
- The linking of all the regional grids to the national grid makes it easier to supply power to any region on demand.
- However, it also makes the entire infrastructure more vulnerable to contagion from cyber-attacks.

What are the measures in this regard?

- The government has been trying to set up a system for cyber-protection of infrastructure.
- The National Critical Information Infrastructure Protection Centre (NCIIPC) is proposed to be the coordinator.
- Dedicated sectoral CERTs, such as CERT-Thermal-NTPC and CERT-Transmission-POWERGRID would be responsible for guarding power assets.
- However, the government has to address the bureaucratic hassles in assigning the responsibility.

What is the way forward?

- Ramping up security across the power grid should be a strategic priority for the government.
- A holistic plan must be devised and implemented to prevent disastrous cyber attacks.

Source: Business Standard



SHANKAR
IAS PARLIAMENT
Information is Empowering