Context:

Minister of State for Atomic Energy and Space Jitendra Singh said that the cyber attack happened in the administrative block and not in the plant.

News:

Malware was detected at state-run Nuclear Power Corp. of India Ltd’s (NPCIL) Kudankulam Nuclear Power Plant (KKNPP) in September.

State-run NPCIL runs India’s fleet of 22 commercial nuclear power reactors with an installed capacity of 6,780 megawatts (MW).

A malware infection was identified in NPCIL KKNPP Internet connected system.

What is a malware?

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware.

Issues of cyberattacks in India:

- India’s power sector facing cyberattacks, with at least 30 events reported daily.
- A majority of the attacks originate from China, Singapore, Russia and the Commonwealth of Independent States countries.
- The cyberattacks assume importance given the increased state of hostilities in the Indian subcontinent and India’s ambitious nuclear plans that include constructing a dozen new nuclear power reactors across the country, with a total power-generation capacity of 9,000 MW.
- While nine reactors totaling 6,700 MW are under construction, the Indian government has also given in-principle approval for setting up nuclear power capacities totaling 25,248 MW at Jaitapur (Maharashtra), Kowada (Andhra Pradesh), Chhaya Mithi Virdi (Gujarat), Haripur (West Bengal), and Bhimpur (Madhya Pradesh).
Way forward:

As such, there are growing concerns that the country’s power infrastructure could be the next target of terrorists looking to cripple its economy. The issue has assumed greater importance as India now has an integrated national power grid, with south India joining the national electricity grid.