Kudankulam Nuclear Power Plant

This article covers the recent news on the cyberattack on the Kudankulam Nuclear Power Plant in Tamil Nadu. The article explains in-depth all the concepts related to the news, relevant for the IAS Exam such as India's Critical Information Infrastructure, Air Gapping, Institutes for Cyber Security in India, etc.

Context: In correlation to the news on the ostensible cyber-attack on the Kudankulam Nuclear Power Plant.

The Kudankulam power plant is located in the coastal Tamil Nadu. It is a Civilian Nuclear Power Plant, built by India in joint-collaboration with Russia. There are a total of 7 operating nuclear power plants in India, and all of these facilities are a part of India’s Critical Information Infrastructure.

Critical Information Infrastructure

- Critical Infrastructure refers to the infrastructure that is the backbone of the country and in a situation wherein the attacks are enforced upon these infrastructures, it can have a severe impact upon the National Security and also on the economy of the country.
- The Information Technology systems which are a part of the country’s critical infrastructure are called Critical Information Infrastructure.
- The following sectors and their Information Technology can be identified as a part of India’s Critical Information Infrastructure:

1. Power and Energy
2. Defence: This includes the Defence Research and Development Organisation (DRDO), Armed Forces, and the Ministry of Defence, etc.
3. Sensitive government departments such as the Prime Minister’s Office, Ministry of Home Affairs, and Ministry of External Affairs which also includes intelligence and security, etc.
4. Banking and Finance, which covers the stock exchanges as well.
5. Space: The Indian Space Research Organisation (ISRO)
6. Railways and Airport

- An attack on the IT Infrastructure of these sectors will have a severe impact on India’s economy and its national security. Hence it becomes quintessential to defend the cyberspace of this critical information infrastructure through special measures, one of which is known as **AIR GAPPING**.

Air Gapping

- It refers to the physical and virtual isolation of the sensitive classified systems from the rest of the network or the rest of the world. A system inaccessible from outside is referred to as an Air-Gapped system or a standalone system.

- Every electronic device is connected to the outside world in multiple ways, such as through a Wi-Fi-router, CD Drives, LAN cable, USB ports, and wireless modes such as through Bluetooth and NFC.
- Such a vast multitude of connections to the outside world make the device susceptible to a cyber-attack. So to ensure a classified computer is prevented from a cyber-attack, it is isolated from the outside world through the concept of Air Gapping.
- This concept is widely utilized in India to protect sensitive information from cyber-attacks in the Prime Minister's office, DRDO, and in the Ministry of Defence, and of nodal importance in computers controlling the operations of the nuclear power plants, Hydropower plants, etc.

What's in News?

- The Kudankulam Nuclear power plant's officials have categorically denied any cyber-attacks on the nuclear power plant, in response to the statement given by an independent cybersecurity expert that the computer systems at the nuclear power plant had been breached and the control systems were taken over, which had resulted in the disruption in the power generation. The officials, however, have denied these allegations and stated that the disruption was a result of a malfunction of a mechanical device and not due to an electronic complication.
- The officials have stated that since the power plant is a part of India's critical information infrastructure, sufficient precautionary measures have been taken and all the computers have been Air-Gapped.
- Nuclear Power Corporation of India Ltd, responsible for managing India's civilian nuclear reactor, stated that, after the Iranian nuclear power plant cyber-attack, further precautionary measures have been implemented to completely isolate such sensitive infrastructure and classified networks in addition to regular cybersecurity audits at such facilities to detect any loopholes in the system's security.
- The officials, in response to the breaching of the physical Air Gap with newer technologies, using handheld devices such as mobile phones stated that it's impossible to bring any handheld device such as mobile phones into the facility due to enhanced physical security and checks.
- The Nuclear Power Corporation of India (NPCIL) has, in the latest statement, admitted to a malware attack on one of the computers in the Kudankulam Nuclear Power Plant. It, however, added that the plant systems were not affected.

Hacking of Air-Gapped System

- Even Air gapped systems are susceptible to cyber-attacks.
- The breaching of an Air-Gapped system is only possible after physical accessibility to the system. Hence for an Air-Gapped system to be breached, an insider has to access the system breaching the physical security of an Air-Gapped system, before being able to place the malware in the network.

- The challenges faced while dealing with an infected system is to transmit the data and to gain remote control over the infected system. This can be done with newer technologies that have come up.
- Hacking can be done through various technologies such as electromagnetic radiation, acoustic waves, thermal radiation, and optical radiation given off by a system. These radiations can be modified by the malware and can be used to transmit data and give remote access to a nearby handheld device.
- Even Air-Gapped systems give off electromagnetic radiation from the memory bus and cables. The computers produce acoustic sound waves from the speakers as well as the fans of the microprocessor.
- The heat generated by the system can also be used for transmittance of the data, even if the speed of transmission of the data is very low.
- The most efficient method to transmit data and give remote access from an infected system to a nearby handheld device is through the optical radiation from the LEDs present on the system.

STUXNET-2010

- The most popular cyber-attack which was carried out by breaching an Air-Gapped system is the Stuxnet. This malware gained a lot of attention in 2010 when several nuclear centrifuge facilities of Iran were destroyed, in turn, crippling Iran's nuclear weapons program.
- This malware was designed by a joint cohort programme by the intelligence agencies of the USA and Israel, to disrupt the nuclear weapons programme of Iran. This involved breaching an Air-Gapped system physically and introducing the malware in the target computers.
- Once the malware was installed, it was used to gain remote access using new technologies to disrupt the functioning of the control systems which were responsible for the spinning of the nuclear centrifuges. After gaining remote access to the control system, the attackers managed to destroy the nuclear centrifuge facilities, in turn disrupting Iran's nuclear weapons programme.

Institutions for Cyber Security in India

- The institutions responsible for defending India's critical infrastructure are CERT-In, National Critical Information Infrastructure Protection Centre, and the Defence Cyber Agency.
- CERT-In refers to Computer Emergency Response Team India and was set up by the Ministry of Electronics and Information Technology in 2004. This is the paramount agency in India for dealing with the security of Indian cyberspace. It is responsible for defending India against all forms of cyber-attacks.
- The National Critical Information Infrastructure Protection Centre was established in 2014. Its establishment was mandated by the National Cyber Security Policy of 2013. It has been set up according to the Information technology Act of 2000. It functions under

the National Technical Research Organization (NTRO) which functions under the National Security Advisor (NSA) in the Prime Minister's Office (PMO), India.

- The Government of India has approved the establishment of the Defence Cyber Agency in 2018 to deal with the threat of cyber warfare. This institution will be raised similar to an armed force and will be responsible for both offensive and defensive operations.