PrepAlpine

Preparation Meets Precision

CURRENT AFFAIRS

For UPSC Civil Services Examination Aspirants

RESEARCH-DRIVEN CONTENT

DAILY COVERAGE WITH MAINS FOCUS

EXAM-READY APPROACH

Stay Informed. Stay Ahead. Succeed.

Disclaimer

The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's discretion and risk.

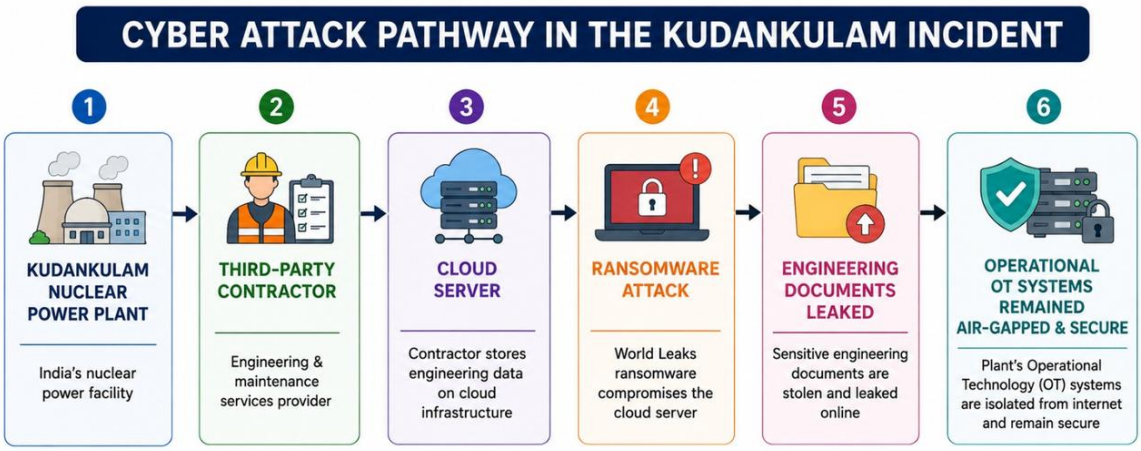
DAILY CURRENT AFFAIRS DATED 17.07.2026

GS Paper III: Security

1. Kudankulam Nuclear Power Plant Data Leak: Strengthening Cybersecurity of Critical Infrastructure

a. Introduction

A ransomware group known as World Leaks allegedly leaked 18,997 files (14.3 GB) related to the Kudankulam Nuclear Power Plant (KKNPP) after compromising a third-party contractor's cloud server. The Nuclear Power Corporation of India Limited (NPCIL) clarified that no nuclear reactor, operational control system or nuclear safety system was compromised, as these systems remain isolated from external networks.



b. Background Context

Critical infrastructure—including nuclear power plants, electricity grids, financial systems, telecommunications networks and transportation infrastructure—is essential for national security and economic stability. As these sectors become increasingly digitised, they also face growing cyber threats from ransomware groups, organised cybercriminals and state-sponsored actors.

Recent cyber incidents worldwide demonstrate that attackers frequently exploit vulnerabilities in contractors, vendors and cloud service providers rather than directly targeting highly secured operational systems. Consequently, the security of critical infrastructure now depends upon protecting the entire digital supply chain, including third-party service providers.

Against this backdrop, the Kudankulam incident highlights the growing importance of securing the wider digital ecosystem surrounding critical infrastructure.

c. Key Developments

- The reported cyber breach originated from a third-party cloud server used by Reliance Infrastructure, the Engineering, Procurement and Construction (EPC) contractor for the Kudankulam Nuclear Power Plant. The cloud infrastructure was reportedly hosted by Yotta.
- The leaked dataset reportedly includes engineering drawings, Balance of Plant (BoP) documents, vendor and supplier information, inspection reports, meeting records and project-related documents, primarily concerning Units 3 and 4, which are currently under construction.
- The Nuclear Power Corporation of India Limited (NPCIL) has stated that the plant's operational technology (OT) networks remain air-gapped, operating independently of external digital networks.

- Consequently, there has been no compromise of reactor controls, nuclear safety systems or security infrastructure.
- The incident is currently under investigation by CERT-In in coordination with NPCIL and other concerned agencies.

Although the operational systems remained secure, the incident exposes broader vulnerabilities within the cybersecurity architecture of critical infrastructure.

d. Significance

The incident carries important implications for India's cyber resilience and national security.

- **Highlights Supply-Chain Risks:** It demonstrates that the security of critical infrastructure is only as strong as the cybersecurity of its contractors, vendors and cloud service providers.
- **Exposure of Sensitive Information:** Engineering drawings, project documents and vendor information may provide valuable intelligence for future cyber espionage, reconnaissance or physical attacks.
- **Emerging Nature of Cyber Threats:** The incident reflects the growing use of ransomware attacks against strategic infrastructure, where attackers increasingly seek sensitive information rather than immediate operational disruption.
- **Strengthening Cyber Governance:** It underscores the need for stronger cybersecurity oversight, regulatory compliance and risk management among private contractors involved in nationally significant infrastructure projects.
- **Comprehensive Cybersecurity Approach:** The breach demonstrates that effective protection must extend beyond operational technology to include engineering databases, project documentation, contractor networks and cloud infrastructure.

These concerns also expose several implementation and governance challenges that require sustained policy attention.

e. Challenges

Several structural and operational challenges continue to affect the cybersecurity of critical infrastructure.

- **Third-Party Vulnerabilities:** Contractors, vendors and cloud service providers remain significant cybersecurity weak links despite secure operational networks.
- **Risk of Cyber Espionage:** Exposure of engineering and project-related information may facilitate reconnaissance and future targeted attacks against strategic infrastructure.
- **Sophisticated Ransomware Operations:** Cybercriminal groups are increasingly employing advanced techniques to exploit weaknesses across interconnected digital ecosystems.
- **Balancing Digitalisation and Security:** Expanding digital infrastructure while maintaining robust cybersecurity safeguards remains a continuing challenge.
- **Regulatory Complexity:** Ensuring uniform cybersecurity standards across multiple contractors, subcontractors and technology partners requires sustained oversight and institutional coordination.

Addressing these vulnerabilities is essential for strengthening India's cyber resilience.

f. Way Forward

- Establish mandatory cybersecurity standards and periodic security audits for all contractors, subcontractors and vendors associated with critical infrastructure projects.

- Adopt a Zero Trust security architecture, supported by strict network segmentation, least-privilege access controls and continuous authentication mechanisms.
- Encrypt sensitive engineering documents and project data throughout their lifecycle and store them only on secure, government-approved digital infrastructure with robust access controls.
- Conduct regular cyber resilience exercises involving NPCIL, CERT-In, NCIIPC and other critical infrastructure operators to improve preparedness and coordinated incident response.
- Develop a comprehensive supply-chain risk management framework for continuous vendor security assessment, timely cyber incident reporting and rapid mitigation of emerging threats.

Conclusion

The Kudankulam data leak demonstrates that safeguarding critical infrastructure requires securing not only operational control systems but also the broader digital ecosystem that supports them. Although the reactor and nuclear safety systems remained fully protected through air-gapped networks, the incident underscores the strategic risks arising from vulnerabilities within contractors and cloud infrastructure. Building a resilient cybersecurity framework for India's critical infrastructure will require stronger supply-chain security, rigorous vendor oversight, robust cyber governance and continuous coordination among specialised national cybersecurity institutions.

Reader's Note — About This Current Affairs Compilation

Dear Aspirant,

This document is part of the PrepAlpine Current Affairs Series — designed to bring clarity, structure, and precision to your daily UPSC learning.

While every effort has been made to balance depth with brevity, please keep the following in mind:

1. Orientation & Purpose

This compilation is curated primarily from the UPSC Mains perspective — with emphasis on conceptual clarity, analytical depth, and interlinkages across GS papers.

However, the PrepAlpine team is simultaneously developing a dedicated Prelims-focused Current Affairs Series, designed for:

- factual coverage
- data recall
- Prelims-style MCQs
- objective pattern analysis

This Prelims Edition will be released separately as a standalone publication.

2. Content Length

Some sections may feel shorter or longer depending on topic relevance and news density.
To fit your personal preference, you may freely resize or summarize sections using any LLM tool (ChatGPT, Gemini, Claude, etc.) at your convenience.

3. Format Flexibility

The formatting combines:

- paragraphs
- lists
- tables
- visual cues

—all optimised for retention.

If you prefer a specific style (lists → paras, paras → tables, etc.), feel free to convert using any free LLM.

4. Monthly Current Affairs Release

The complete Monthly Current Affairs Module will be released soon, optimized to a compact 100–150 pages — comprehensive yet concise, exam-ready, and revision-efficient.