



CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

In Focus

New Delhi

CAPSS In Focus: 20/2026

10 April 2026

Iran's Attacks on the Data Centres: Lessons for India's Emerging Critical Infrastructure

Mr Niranjan Chandrashekhar Oak

Research Analyst, Nuclear and Arms Control Centre, MP-IDSA, New Delhi



Source: Created by the Author using perplexity.ai



Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Aerospace Power and Strategic Studies [CAPSS]

This work is licensed under Creative Commons Attribution – Non-Commercial – No Derivatives 4.0 International License.



Centre for Aerospace Power and Strategic Studies |



@CAPSS_India |



Centre for Aerospace Power and Strategic Studies |



Centre for Aerospace Power and Strategic Studies

Keywords: Critical Infrastructure, Iran War, Data Centres, Small Modular Reactors, Security

Introduction

In response to the joint attacks by the United States (US) and Israel, codenamed 'Operation Epic Fury' and 'Operation Roaring Lion' respectively, which began on February 28, 2026, Iran retaliated with 'Operation True Promise IV', attacking multiple targets in the Gulf, including American data centres in the area. On March 02, 2026, Amazon Web Services (AWS) stated that two of its data centres in the United Arab Emirates (UAE) and one in Bahrain sustained physical damage from a drone strike carried out by Iran, resulting in a temporary disruption of its services.¹

In a letter addressed to the Secretary-General of the United Nations (UN), António Guterres, and the President of the UN Security Council (UNSC), James Kariuki, Iran's Foreign Minister Seyed Abbas Araghchi informed that Tehran considered "all bases, facilities, and assets of hostile forces (US and Israel) in the region legitimate military targets."² Traditionally, the physical and energy infrastructure, such as refineries, bridges, ports, airports, and industrial zones, has been a target in military conflicts. However, as the definition of critical infrastructure has widened to include digital infrastructure, Small Modular Reactors (SMRs), and undersea cables, data centres have emerged as new targets in the ongoing conflict.

Although this is the first time that a US data centre is at the receiving end of a drone and missile attack anywhere in the world, it is unlikely to be the last. Modern warfare is fated to see an increase in such attacks during conflicts for several reasons. First, causing damage to the digital infrastructure is not expensive. In the event of an attack on data centres, a country need not fire a missile or any high-value projectile; a cheap drone can suffice. Since building a data centre requires an investment of millions of dollars, it is an ideal target for attackers.

Second, in the hyperconnected digital world, the consequences of such an attack can be widespread, allowing attackers to demonstrate their power globally and disrupting the investment environment in the area where the data centre is situated. Third, international law³ prohibits making civilian objects, that do not contribute to a military action, targets of attack or reprisals. However, data centres can run unrelated sectors, such as medical, banking, and military, simultaneously. Thus, the attacker may consider a data centre a legitimate target even on the suspicion that it serves the enemy's military purpose.

While companies ensure the physical security of data centres against crimes such as theft and trespassing by installing barbed wire fences and video surveillance, among other measures, few have considered their security against missile or drone threats during conflicts.⁴ A few data

centres in countries such as the United Kingdom (UK),⁵ Sweden,⁶ and China are housed underground, in bunkers, or in caves.⁷ However, the decision to build data centres underground is more an individual decision by owners than a policy of a sovereign state.

Lessons for India

The recent budget for the financial year 2026-27 has introduced long-term tax exemptions lasting until 2047 for foreign cloud service companies that use Indian data centres, aiming to position India as a destination for the emerging data centre ecosystem. According to the Economic Survey 2025–26, India currently has a data centre capacity of 1.2 GW, which is projected to increase more than threefold to approximately 4 GW by 2030.⁸ Therefore, in the coming years, India is expected to witness the proliferation of data centres.

Along with the data centres, India should also consider the upcoming Small Modular Reactor (SMR) industry, which the government has decided to incentivise under the Nuclear Energy Mission (NEM), and through enactment of the Sustainable Harnessing and Advancement of Nuclear Energy for Transforming India (SHANTI) Act, to meet the substantial energy demand of the data centre ecosystem. Thus, the potential external threats to India's critical infrastructure necessitate meticulous planning and implementation of security measures.

During Operation *Sindoor*, the country has seen swarms of drones getting neutralised over the Indian airspace.⁹ One Pakistani missile was intercepted over Sirsa, Haryana.¹⁰ Unfortunately, India has to take into account threats emanating from both the Western and Northern neighbours, as well as from non-state actors. Therefore, the country must consider the possibility of a drone or missile attack targeting the critical infrastructure and take preventive measures to secure it.

Building critical infrastructure underground might be one way to protect it from physical attacks during a conflict. However, doing so will have severe cost implications. In the case of data centres, instead of placing all of them underground, authorities can assess their national security significance and build only the most critical data centres underground.

In the case of SMRs, public sentiment, along with cost implications, also needs to be taken into account. Already, Indian public perception of nuclear energy is unfavourable, according to the National Institute for Transforming India (NITI) Aayog Report on SMRs,¹¹ and any attack on the SMRs could negatively affect public sentiment towards nuclear energy, even if there is no radiological fallout.

Some private SMR entities, such as Deep Fission¹² and NuScale Power,¹³ are already developing designs in which reactors are built underground. It would be prudent for policymakers to

examine such models and conduct a cost-benefit analysis of underground reactors, given the likelihood of proliferation of the SMR ecosystem in the foreseeable future.

For over-the-ground critical infrastructure, the government may consider allotting land parcels specifically for their construction. Such clusters will be easy to protect against contingencies by deploying defensive measures.

Since attacks on critical infrastructure during conflicts are not new, the country must adopt appropriate measures to protect emerging critical assets, such as data centres and SMRs, during emergencies. Low-cost attacks on critical infrastructure are appealing targets for attackers because they harm public opinion as well as investment confidence. Therefore, it is advisable to learn from other conflicts and prepare for future contingencies.



Notes:-

¹ Shubham Kalia, Aditya Soni and Mrinmay Dey, "Amazon Cloud Unit's Data Centres in UAE, Bahrain Damaged in Drone Strikes," *Reuters*, March 02, 2026, <https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/>. Accessed on February 22, 2026.

² Ministry of Foreign Affairs, Republic of Iran, "Iran Requests UN Action Against Israeli and U.S. Aggression," March 01, 2026, <https://en.mfa.gov.ir/portal/newsview/783913>. Accessed on February 22, 2026.

³ "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1)," United Nations Human Rights, United Nations, June 08, 1977, <https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and>. Accessed on February 22, 2026.

⁴ Christopher S. Chivvis and Sam Winter-Levy, "The Gulf is Not the Place to Build the World's AI Infrastructure," *The Washington Post*, July 22, 2025, <https://www.washingtonpost.com/opinions/2025/07/22/data-center-ai-middle-east/>. Accessed on February 22, 2026.

⁵ Matthew Gooding, "Inside the Data Centre Built to Withstand a Nuclear Blast," *Data Centre Dynamics*, December 12, 2025, <https://www.datacenterdynamics.com/en/analysis/inside-the-data-center-built-to-withstand-a-nuclear-blast/>. Accessed on February 27, 2026.

⁶ Dan Swinhoe, "Sweden's Bahnhof Drops Plans for Stockholm Data Centre to Focus on Gothenburg Bunker Facility," *Data Centre Dynamics*, October 01, 2025, <https://www.datacenterdynamics.com/en/news/swedens-bahnhof-drops-plans-for-stockholm-data-center-to-focus-on-gothenburg-bunker-facility/>. Accessed on February 22, 2026.

⁷ Viola Zhou, "Iranian drone strikes at Amazon sites raise alarms over protecting data centres," *Rest of World*, March 04, 2026, <https://restofworld.org/2026/iran-amazon-data-center-strikes/>. Accessed on February 24, 2026.

⁸ Ministry of Finance, Government of India, "Economic Survey 2025-26," January 2026, <https://www.indiabudget.gov.in/economicsurvey/doc/echapter.pdf>. Accessed on February 24, 2026.

⁹ Manjeet Negi, "500 Pak Drones Targeted 24 Cities for 210 Minutes: Army Sources on May 8 Attack," *India Today*, May 09, 2025, https://www.indiatoday.in/india/story/india-pakistan-attack-drones-targeted-cities-jk-punjab-rajasthan-gujarat-3-hours-on-may-8-operation-sindoor-2722241-2025-05-09?utm_source. Accessed on February 24, 2026.

¹⁰ "Pak Missile Intercepted in Sirsa on Night Before Ceasefire," *Hindustan Times*, May 11, 2025, <https://www.hindustantimes.com/cities/chandigarh-news/pak-missile-intercepted-in-sirsa-on-night-before-ceasefire-101746903682797.html>. Accessed on February 24, 2026.

¹¹ National Institute of Transforming India (NITI) Aayog, Government of India, "A Report on The Role of Small Modular Reactors in The Energy Transition," May 2023, <https://www.niti.gov.in/sites/default/files/2023-05/The-Role-of-Small-Modular-Reactors-in-the-Energy-Transition-05162023.pdf>. Accessed on February 24, 2026.

¹² "Deep Fission Begins Drilling First Data Acquisition Well," *World Nuclear News*, March 11, 2026, <https://www.world-nuclear-news.org/articles/deep-fission-begins-drilling-first-data-acquisition-well>. Accessed on February 26, 2026.

¹³ The United States Nuclear Regulatory Commission, United States of America, "NRC Approves Standard Design for NuScale US460 Small Modular Reactor," May 29, 2025, <https://www.nrc.gov/cdn/doc-collection-news/2025/25-033.pdf>. Accessed on March 02, 2026.