CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

In Focus

New Delhi

CAPSS In Focus: 25/2026

04 May 2026

Growing Threats to Dual-use Critical Information Communication Technology (ICT) Infrastructure in Contemporary Wars

Ms Gowri R
Research Associate, Centre for Aerospace Power and Strategic Studies

Source: Created by the Author using AI

Keywords: Dual-use Technology, Data Centres, ICT Infrastructure, Artificial Intelligence

Introduction

Contemporary warfare increasingly relies on non-kinetic means such as cyber intrusions, exploitation of vulnerabilities, zero-day attacks, and supply-chain compromises. State and non-state actors often use Artificial Intelligence (AI) generated images, videos and text to manipulate public opinion and wage information warfare. The 2026 war in West Asia involving Israel, the United States (US) and Iran has escalated beyond a significant threshold by targeting the critical ICT (Information Communication Technology) infrastructure, including data centres, to impose strategic and operational costs. This article analyses the effects of kinetic operations against critical dual-use ICT infrastructure, particularly data centres, which are the backbone of non-kinetic operations. Further, it focuses on the growing threats of targeting dual-use infrastructure with pervasive dependence on emerging technologies in contemporary armed conflicts. Thereby, this article examines the implications for India's digital battlespace, both on Earth and in outer space.

AI as a Modern Military Weapon in Warfare

Recent armed conflicts show that AI has been deeply embedded in both kinetic and non-kinetic operations. The AI-generated videos and AI agentic bots have been used to shape public opinion. It also functions as a strategic signalling tool, projecting military success and resolve to shape adversaries' perceptions of your capabilities, costs, and escalation risks. Advanced AI-based systems are being used by the US military to develop war plans, analyse military deployment, and even suggest the course of operations. [1] The US has deployed military AI applications using Maven Smart Systems (MSS), built by Palantir Technologies, in combination with Large Language Model (LLM) Claude, developed by Anthropic, in the Iran conflict. [2] These systems have been used for decision support systems, drones, cyber and electronic, and information warfare. With AI playing a decisive role in both kinetic and non-kinetic operations, these systems depend on large-scale compute, storage, and connectivity. This reinforces the strategic importance of protecting critical ICT infrastructure and data centres required to build, train, and run cognitive systems in a contested environment, wherein civil and military networks share a common backbone. This dual-use or dual-purpose technology creates a dilemma about the legitimacy of targeting ICT and its supporting infrastructure. At the same time, AI as a weapon system complicates its legitimate use in warfare with its existing technical maturity, as it cannot distinguish between civil and military objects. [3]

Kinetic Strikes on ICT Infrastructure in West Asia

The air strikes conducted by the United States of America (USA) and Israel against the Iranian ICT infrastructure included the destruction of the AI research facility at Sharif University of Technology in Tehran, research centres at Shahid Beheshti University (photonics laboratory), Iran Science and Technology University (satellite development facility) and Bank Sepah digital security centre which hosted Islamic Revolutionary Guard Corps (IRGC) salary and military banking systems. [45] Iran carried out strikes on the Amazon Web Services (AWS) data centres of the United Arab Emirates (UAE) and Bahrain [6] and explicitly warned the 18 privately owned USA technology facilities in the region of West Asia of possible air strikes in the future. [7] This indicates that privately operated cloud and data infrastructure facilities would be treated as legitimate military targets in escalation scenarios. Internet connectivity and datacentres have emerged as digital chokepoints in the current national and military security environment.

Subsea Cables as a Strategic Chokepoint

Subsea fibre optic cables carry the majority of the world's international internet traffic, with an estimated 95 percent of global internet data flowing through them. This is significantly higher than the space-based systems. [8] Across continents, these undersea cables interconnect cloud infrastructure and data centres, enabling large-scale data movement and low-latency connectivity required for AI training and cloud computing. [9] When these cables are threatened or damaged by state or non-state actors, they become strategic chokepoints that can potentially disrupt communications, financial transactions, and critical ICT services across the entire region. As a result, deliberate attacks on subsea cables have emerged as a strategically significant digital chokepoint.

Space Systems for Internet Connectivity

Vulnerabilities and challenges of existing terrestrial and subsea ICT infrastructure have led to the deployment of space systems for internet communication and the ideation of installing data centres in orbit. As subsea cables have become strategic chokepoints, satellite broadband connectivity offers an alternative to mitigate the risks. However, the current space-based capabilities are still being built and maturing. The satellite internet or broadband, formally called Global Mobile Personal Communication by Satellite (GMPCS), is being deployed using Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbit (GEO) or Geosynchronous Earth Orbit (GSO) satellites to extend connectivity across all geographies, including sea, mountains, and other remote areas. In India, OneWeb India Communications, Jio Satellite Communications and Starlink Satellite Communications have received GMPCS licences. These industries are expected to play a central

role in universal connectivity strategies, primarily through LEO constellations. [10] Presently, Indian Defence Forces continue to rely primarily on dedicated military communications satellites and dual-use communication satellites for secure, near-real-time voice, data, and video connectivity in remote and contested environments. Therefore, both internet and operational network connectivity need to be deployed as a resilient satellite communication grid in a layered architecture to meet the future military and civil requirements.

Space-Based Data Centres

Research indicates that data centres currently consume around 1.5 per cent of global electricity, which is expected to grow significantly in the coming years as AI workloads expand. [11] Space-based data centres are being explored as a potential solution to address this sustainability challenge. The availability of continuous solar energy in orbit, the possibility of free radiative cooling, scalability, three-dimensional architecture for low-latency processing, and high-capacity laser communications for data transmission motivate researchers to implement data centres in space. [12] The emergence of space-based data centres is merely a sustainable solution rather than a strategic choice.

However, moving data centres and communication satellites to space does not reduce the risk of kinetic and non-kinetic attacks. The kinetic Anti-Satellite (ASAT) tests conducted by the USA, China, Russia, and India have demonstrated their capabilities to physically destroy satellites. This signalling showcases that states have the credible capabilities to attack satellites at will. This could possibly threaten the data centres in space. Similarly, the potential of non-kinetic attacks is evident during the armed conflicts, such as the famous Viasat KA-SAT cyberattacks in the Russia-Ukraine War, wherein wiper malware was used, and the Global Positioning System/ Global Navigation Satellite System (GPS/GNSS) spoofing and jamming in the Iran-US-Israel conflict, affecting more than 1,100 ships in the Persian Gulf and Strait of Hormuz. [13] The various platforms in the contested area experienced navigation disruptions. This shows that space infrastructures are also vulnerable and services can be degraded or denied even without physical destruction, with cascading effects across multiple domains and geographies.

Dual-Use Technology and Growing Threats

Targeting of data centres is not an irrational act of destruction; it is rooted in the strategic effects of dual-use technology. Dual-use refers to facilities, platforms, and systems that can be used for both civilian and military purposes. As per Article 52 of Additional Protocol I to the Geneva Conventions, only the military objectives shall be attacked, and the objects that offer a definite military advantage by virtue of their nature, location, purpose or use contribute to military action.[14] This raises the following questions: “Is the privately owned ICT infrastructure considered as Critical Information

Infrastructure (CII) ?" and "Do attacks on the private industrial complex violate the Geneva Conventions or International Humanitarian Law (IHL)?"

Under IHL, dual-use ICT infrastructure such as data centres may be lawfully targeted only when it qualifies as a military objective under Article 52(2) of Additional Protocol I. By making an effective contribution to military action, the dual-use ICT infrastructure becomes a valid target as they offer a definite military advantage. The same dual-use logic extends to space-based infrastructure. Communication satellites, navigation systems, and any future orbital data centres can simultaneously support civil functions such as commercial broadband, banking, disaster response, and scientific research, as well as military functions such as command-and-control, facilitating, and ISR analysis. This makes space-based infrastructure a classical dual-use object providing military advantage. At the same time, their global civilian dependence on space-based services creates a dilemma. This means that applying the principles of distinction, proportionality and precaution to attacks on space infrastructure is even more complex than ground-based data centres. Therefore, these concerns are reflected in recent international humanitarian law and space law discussions on cyberspace and counterspace operations.

Securing India's Digital Battlespace on Earth and in Outer Space

The conflicts in West Asia confirm that, in modern warfare, information infrastructure has also become a primary battlespace. Kinetic strikes on data centres in Tehran, Dubai, Manama and other Gulf cities, combined with cyber and electronic attacks on satellite communication networks, show that adversaries now treat data infrastructure, subsea cables and space systems as strategic targets alongside conventional military targets. The evolution of using dual-use technology with modern ICT assets enables AI-driven targeting, command and control, and battlefield intelligence, which has forced militaries to target them to achieve military objectives.

India depends mostly on fibre-optic cables for internet communication, with international connectivity landing in coastal cities like Mumbai, Chennai, Cochin, Tuticorin, and Trivandrum. [15] The major number of data centres are concentrated in Mumbai, Bengaluru, Chennai, Hyderabad, and Noida. [16] As the government is pushing many initiatives to build AI technologies and the underlying infrastructure, it becomes critical to geographically distribute data centres across the country rather than clustering them in important cities. Because dual-use technologies are tightly intertwined, the key national systems, including Unified Payments Interface (UPI), Adhaar, e-governance portals, Banking and Stock Exchanges and defence ICT infrastructure, depend on this shared digital backbone.

Section 70 of the Information Technology Act, 2000, defines Critical Information Infrastructure (CII) as any "computer resource, the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety." This definition aligns with the National Critical Information Infrastructure Protection Centre's (NCIIPC) criteria, which focus on the criticality of functions and services and their impact on national security, economy, public health, or safety. [17] The existing Indian framework for CII offers coverage for the digital ecosystem, but it does not explicitly guarantee security.

The recent West Asia conflict suggests that states have must strengthen their own infrastructure and also actively push for international norms against striking dual-use digital systems. So that the essential digital services are not treated as legitimate targets in the generation of AI-enable conflict.

Notes:

[1] "US Military Confirms Use of 'Advanced AI Tools' in War against Iran | US-Israel War on Iran News," *Al Jazeera*, March 11, 2026, https://www.aljazeera.com/news/2026/3/11/us-military-confirms-use-of-advanced-ai-tools-in-war-against-iran. Accessed on April 10, 2026.

[2] Vinay Singh, "War at Machine Speed: How AI Became a Decisive Force in US-Israel Conflict with Iran," *The Print*, April 22, 2026, https://www.msn.com/en-in/money/news/war-at-machine-speed-how-ai-became-a-decisive-force-in-us-israel-conflict-with-iran/ar-AA21yhUm?ocid=BingNewsSerp. Accessed on April 28, 2026.

[3] "Customary IHL - Rule 71. Weapons That Are by Nature Indiscriminate," https://ihldatabases.icrc.org/en/customary-ihl/v1/rule71. Accessed on April 16, 2026.

[4] Emily Harding, "Data Is Now the Front Line of Warfare," Centre for Strategic and International Studies, March 19, 2026, https://www.csis.org/analysis/data-now-front-line-warfare. Data Is Now the Front Line of Warfare. Accessed on April 10, 2026.

[5] Maziar Motamedi, "Top University says US-Israel Attack Targeted Iran's Progress, AI Learning | US-Israel War on Iran News," *Al Jazeera*, April 07, 2026, https://www.aljazeera.com/news/2026/4/7/top-university-says-us-israel-attack-targeted-irans-progress-ai-learning. Accessed on April 10, 2026.

[6] Shubham Kalia et al., "Amazon Cloud Unit's Data Centers 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 April 17, 2026.

[7] Kai Nicol-Schwarz, "Iran Threatens Nvidia, Apple and Other Tech Giants with Attacks," *CNBC*, April 01, 2026, https://www.cnbc.com/2026/04/01/iran-irgc-nvidia-appple-attack-threat.html. Accessed on April 17, 2026.

[8] Vish Iyer, "The Subsea Cables Powering AI, Cloud, and the Digital Economy," *The Cisco News Network- APJC,* December 01, 2025, https://news-blogs.cisco.com/apjc/2025/12/02/the-subsea-cables-powering-ai-cloud-and-the-digital-economy/. Accessed on April 17, 2026.

[9] Ibid.

[10] Press Information Bureau, Government of India, "Satellite Internet in India," September 23, 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2170091&reg=3&lang=2. Accessed on April 17, 2026.

[11] Philip Johnston, "How Data Centres in Space Sustainably Enable the AI Age," World Economic Forum, January 7, 2026, https://www.weforum.org/stories/2026/01/data-centres-space-ai-revolution/. Accessed on April 16, 2026.

[12] Ibid.

[13] "GPS Jamming Disrupts 1,100 Ships in the Middle East Gulf," *Windward,* March 01, 2024, https://windward.ai/blog/gps-jamming-disrupts-1100-ships-in-the-middle-east-gulf/. Accessed on April 17, 2026.

[14] "IHL Treaties - Additional Protocol (I) to the Geneva Conventions, 1977 - Article 52," International Humanitarian Law Database, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-52. Accessed on April 16, 2026.

[15] "India Poised to Become Global Hub for Submarine Telecom Cable Network," *ET Government*, March 11, 2021, https://government.economictimes.indiatimes.com/news/technology/india-poised-to-become-global-hub-for-submarine-telecom-cable-network/118873661. Accessed on April 20, 2026.

[16] "India Data Centers,"*Data Centre Map,* https://www.datacentermap.com/india/. Accessed on April 20, 2026.

[17] P K Mallick, "Protection of Critical Information Infrastructure," *Vivekananda International Foundation*, 2024. https://www.vifindia.org/sites/default/files/Protection-of-Critical-Information-Infrastructure.pdf. Accessed on April 13, 2026.