Iranian Missile Strikes Demonstrate the Cloud Is No Longer Abstract

Major General Jagatbir Singh, VSM (Retd)

Introduction

During the ongoing Iran war, among the targets hit by Iranian drone and missile strikes were cloud facilities in the Gulf region, including two Amazon Web Services (AWS) data centres in the United Arab Emirates (UAE) and a Bahrain facility that suffered damage from a nearby strike. The attacks disrupted services and forced operators to reroute workloads across other cloud regions due to power disruptions, fire-related water damage, and prolonged outages affecting regional customers, including financial institutions.[1] For the first time, core cloud infrastructure—once seen as abstract and purely commercial technology—has been directly struck in a military conflict.

Throughout the bulk of the digital age, data centres have been thought of as "behind the scenes" infrastructure—the unassuming commercial underpinning of what is referred to as "the cloud." In fact, the cloud is not an ethereal or intangible concept. It is an earthly construct requiring land, concrete structures, transformers, cooling systems, vast cables, and considerable energy usage.[2]

Targeting the cloud threatens more than just military capability, as it hosts financial systems, communications networks, logistics software, and increasingly the computing power behind Artificial Intelligence (AI). Previously the threat was mainly visualised from hackers, ransomware and cyber-attacks. Data centres are now moving to the forefront of targeting lists, demonstrating that the cloud is vulnerable to the logic of war.

The New Strategic Infrastructure

With the increasing reliance on centralised cloud computing systems in different nations' governments, businesses, and military establishments, the places where these computing systems are housed are gaining recognition as critical assets. Data centres are no longer anonymous commercial properties; they are beginning to be recognised as integral parts of the strategic hinterland—immobile, valuable, and energy-intensive assets that can set off economic and operational repercussions if disturbed.[3]

The focus now is on building digital capacity for a variety of uses which includes AI tools for military purposes hence these centres built to enable both economic productivity and warfighting—have become fixed targets that require protection. The belief that the cloud exists above the battlefield no longer holds.

The destruction of these data centres is an indication of a future form of these targeting strategies. AWS reported structural damage, disruptions to power delivery, and failures in fire-suppression systems that caused additional water damage to equipment.[4]

Even brief disruptions of digital infrastructure have the potential to cascade through critical sectors of society, undermining our financial systems, communications, supply chains, our system of governance, and our military command and control systems. These systems are not invisible and intangible anymore; they are now clearly identifiable as strategic assets, just as our more traditional infrastructure of ports, bridges, transportation hubs, and energy pipelines.

Why Data Centres Became Targets

The cloud computing model is conceived as distributed and inherently fault-tolerant, yet it relies on physically clustered infrastructures. This centralisation not only amplifies the strategic value of the data centres but also makes them more vulnerable and susceptible.[5]

Data centres house thousands of servers alongside power distribution systems, fibre connectivity, cooling plants, and backup generation systems. These facilities often span vast campuses. The scale that enhances efficiency in peacetime creates vulnerability in wartime.

Modern warfare increasingly depends on data rather than ammunition alone. The same infrastructure powering civilian services now supports intelligence processing, logistics coordination, satellite integration, and AI-enabled military decision-making.[6]

In practical terms, commercial cloud facilities are now part of military command-and-control systems.

Telecommunications and Energy as Strategic Infrastructure in Wartime

Strikes on critical infrastructure have been at the heart of conflict throughout history, intended to undermine an enemy's economic and operational capabilities. What's new here is not the concept, but the target set—digital infrastructure is being treated with the same level of importance as the physical infrastructure of refineries, ports, rail networks, and power stations.

This was seen in the opening phase of the conflict between Russia and Ukraine, where cyber-attacks were quickly accompanied by attacks on critical infrastructure in the ground, particularly in the energy and communications sectors. Russia's repeated attacks on Ukraine's energy grid illustrate this trend. In Mar 2024, large-scale strikes damaged multiple energy facilities, leaving over one million people without electricity and forcing Ukraine to import power.[7]

Digital resilience is inseparable from power resilience. A data centre without electricity is effectively disabled.

Most importantly, crippling digital systems do not require demolishing data centres. Disrupting support structures such as power grids, transmission nodes, cooling systems, and fibre optic cables is sufficient to trigger chain reactions, and these chain reactions spread rapidly.[8]

Low-cost drones carrying explosive payloads are increasingly capable of targeting high-value infrastructure, making previously secure commercial facilities vulnerable.[9]

The Fallout of the Strikes in the Gulf

The Gulf has traditionally been seen as an attractive destination for data infrastructure due to political stability and access to energy. According to Mordor Intelligence, the UAE hosts approximately 35 data centres, with 42 per cent classified as large-scale facilities.[10]

In May 2025, United States' President Donald Trump announced over USD 2.8 tn in investment pledges across Saudi Arabia, Qatar, and the UAE. A centrepiece project included a USD 700 bn AI data centre in Abu Dhabi, involving OpenAI, NVIDIA, Oracle, and Cisco.[11]

However, the strikes have altered perceptions. The Gulf no longer appears immune to conflict spillover. Infrastructure once considered secure is now exposed.

The economic implications of such asymmetric strikes are significant. They raise the cost of conflict and undermine investor confidence in large-scale digital infrastructure.

Data Centre Security

The strikes have revealed the strategic relevance of data centres, the security of which, lies in moving beyond cybersecurity. Computing power is now the critical asset and it needs to be safeguarded and secured.

Dispersion of assets geographically is now imperative. As concentrating computing capacity in hubs increases wartime risks, distributed architectures can mitigate the impact of attacks.[12]

Traditional physical security measures—fences, surveillance, and controlled access—are insufficient against aerial threats. Protecting data centres now requires integration into air and missile defence frameworks.

These facilities are also highly visible due to their size and thermal signatures, making concealment difficult.

Governments must treat major data centres as critical national infrastructure and incorporate them into civil defence planning.[13]

The idea of creating international agreements to protect data centres is theoretically appealing. However, their dual-use nature—supporting both civilian and military functions—makes such agreements difficult to enforce.

Conclusion

As conflict increasingly intersects with digital infrastructure, technology companies and nations need to acknowledge that the ‘cloud’ cannot be separated from geography or conflict.

Infrastructure protection policies remain largely national in scope, while digital infrastructure is global. This mismatch increases vulnerability.

This war has illustrated that the cloud cannot be considered an abstract borderless entity.

The irony is stark: AI, once used to select targets, is now itself a target. What may appear as a limited strike on a data centre could signal a broader shift in warfare, one that carries the potential for unprecedented global disruption.

Endnotes

[1] “AWS Global Infrastructure and Service Health Updates’, *Amazon Web Services*, accessed 20 Mar 2026 https://aws.amazon.com/about-aws/global-infrastructure/

[2] Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press), 2015 https://syllabus.pirate.care/library/Nicole%20Starosielski/The%20Undersea%20Network%20(397)/The%20Undersea%20Network%20-%20Nicole%20Starosielski.pdf.

[3] Macdonald Amoah, Morgan Bazilian, and Jahara Matisek, “When the Cloud Becomes a Target: The Future of War Is Your Internet,” *The National Interest*, 09 Mar 2026, accessed 20 Mar 2026 https://nationalinterest.org/blog/techland/when-the-cloud-becomes-a-target-the-future-of-war-is-your-internet.

[4] Amazon Web Services, *“AWS Health Dashboard – Service Health”,* accessed 20 Mar 2026, https://health.aws.amazon.com/health/status.

[5] Macdonald Amoah, Morgan Bazilian, and Jahara Matisek, “When the Cloud Becomes a Target”, *The National Interest*.

[6] “DoD Data Strategy”, *United States Department of Defence*, 08 Oct 2020, accessed 20 Mar 2026 https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[7] Macdonald Amoah, Morgan Bazilian, and Jahara Matisek, “When the Cloud Becomes a Target”, *The National Interest*.

[8] Ibid.

[9] Jack Watling and Nick Reynolds, “Iranian Data Strikes Shake Global Digital Infrastructure”, *Royal United Services Institute*, 19 Mar 2026, accessed 20 Mar 2026 https://www.rusi.org/explore-our-research/publications/commentary/iranian-data-strikes-shake-global-digital-infrastructure

[10]"UAE Data Center Market", *Mordor Intelligence*, accessed 20 Mar 2026 https://www.mordorintelligence.com

[11] "Fact Sheet: President Donald J. Trump Secures $200 Billion in New U.S.-UAE Deals and Accelerates Previously Committed $1.4 Trillion UAE Investment", *The White House*, 15 May 2025, accessed 20 Mar 2026 https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-secures-200-billion-in-new-u-s-uae-deals-and-accelerates-previously-committed-1-4-trillion-uae-investment/.

[12] Macdonald Amoah, Morgan Bazilian, and Jahara Matisek, "When the Cloud Becomes a Target", *The National Interest*.

[13] Alexander Klimburg, Akshay Joshi and Filipe Beato, "Why defining and securing systemically important critical infrastructure is so vital", *World Economic Forum,* 24 May 2022, accessed 20 Mar 2026 https://www.weforum.org/stories/2022/05/securing-systemically-important-critical-infrastructure/

Major General Jagatbir Singh, VSM (Retd) is a Distinguished Fellow at the USI of India. Commissioned in 1981 into the 18 Cavalry, he has held various important command and Staff appointments including command of an Armoured Division.

Article uploaded on 20-03-2026