PitchBook
a Morningstar company

Institutional Research Group

Dimitri Zabelin
Senior Research Analyst,
AI and Cybersecurity
dimitri.zabelin@pitchbook.com

pbinstitutionalresearch@pitchbook.com

Published on March 12, 2025

Contents

EMERGING TECH RESEARCH

Iran War Raises New Risks for AI Datacenters

AI datacenters enter the strategic infrastructure battlefield

PitchBook is a Morningstar company providing the most comprehensive, most accurate, and hard-to-find data for professionals doing business in the private markets.

Key takeaways

- Hyperscale datacenters have emerged as a new category of strategic infrastructure targeted during conflict.
- Concentrated AI compute infrastructure creates systemic risk, because disruptions can cascade across the digital economy.
- Trillions of dollars in AI datacenter investment now carry growing geopolitical and security exposure.

Hyperscale datacenters as military targets

Confirmed Iranian drone strikes targeting cloud datacenters in the Gulf mark one of the first cases where hyperscale computing infrastructure has been treated as a physical military target. The attacks damaged Amazon Web Services facilities in the United Arab Emirates (UAE) and Bahrain, disrupting cloud services and highlighting the vulnerability of the physical infrastructure that underpins the global digital economy.

For decades, the hierarchy of critical infrastructure in war followed a relatively stable pattern. Strategic strikes historically targeted:

- Oil facilities
- Power grids
- Telecommunications networks
- Transportation infrastructure

Each layer supported the functioning of the industrial economy. Disrupting them impaired a country's ability to produce energy, communicate, and move goods or military forces. A fifth category is now emerging: compute infrastructure.

Hyperscale datacenters and AI clusters increasingly form the foundation of the digital economy. As AI infrastructure becomes concentrated in multi-gigawatt campuses hosting large clusters of specialized processors, these facilities become more visible and potentially more valuable military targets.

The evolution of targeted infrastructure can be seen in recent conflicts. During the 1999 Kosovo War, NATO strikes targeted Serbian telecommunications facilities in Belgrade to disrupt communications networks and broadcast infrastructure. During the 2003 invasion of Iraq, coalition forces targeted telecommunications exchanges and command infrastructure for similar reasons. In the war in Ukraine, telecommunications towers and internet nodes have repeatedly been targeted in an effort to degrade communications and operational coordination.

Today, many of those functions operate inside hyperscale cloud environments. Datacenters support government workloads, financial systems, logistics platforms, enterprise software, and the computing infrastructure used to train and operate advanced artificial intelligence models.

These facilities underpin a layered AI architecture. Horizontal AI platforms provide the base layer of the modern digital economy. Cloud infrastructure, foundation models, and AI development environments provide the compute, data pipelines, and model capabilities that support thousands of downstream applications. Vertical AI applications across sectors such as healthcare, finance, logistics, defense, and manufacturing increasingly sit on top of these shared infrastructure layers.

This architecture concentrates risk. A relatively small number of infrastructure providers host the compute capacity, models, and data pipelines that support large portions of the digital economy. Disruptions at the infrastructure layer therefore have the potential to cascade across many sectors simultaneously.

A single large AI campus can have electricity needs equivalent to a midsize city.

Hyperscale datacenters concentrate this infrastructure in a limited number of physical locations. A single campus can support the digital operations of thousands of companies simultaneously. Large AI campuses increasingly operate at power scales measured in hundreds of megawatts, with several facilities designed to approach or exceed one gigawatt of capacity. Energy demand is a defining feature of the new AI infrastructure cycle. A single large AI campus can have electricity needs equivalent to a midsize city. This scale of demand has pushed power availability, grid interconnections, and energy infrastructure to the center of AI infrastructure planning.

The economics of these facilities reinforce their strategic importance. Global datacenter construction costs have risen sharply as demand for AI capacity has accelerated. Average construction costs increased from roughly $7.7 million per megawatt in 2020 to approximately $10.7 million per megawatt by 2025.[1] At those levels, a 100-megawatt hyperscale facility represents more than $1 billion in construction costs before accounting for the value of GPUs, servers, networking hardware, and supporting power infrastructure.

The scale of capital required to build this infrastructure is expanding rapidly. McKinsey estimates global capital expenditure on datacenter infrastructure could reach roughly $6.7 trillion by 2030, with approximately $5.2 trillion tied specifically to AI-optimized facilities.[2] The build-out of hyperscale AI infrastructure therefore represents one of

1: "2026 Global Data Center Outlook," JLL, January 5, 2026.
2: "The Cost of Compute: A $7 Trillion Race to Scale Data Centers," McKinsey, Jesse Noffsinger, et al., April 28, 2025.

the largest industrial investment cycles currently underway. Development timelines are also lengthening. The shell of a hyperscale facility can typically be constructed in roughly 18 to 24 months, but power availability is increasingly the primary constraint. In major markets, grid interconnection delays are pushing total development timelines toward four to six years.

Replacement lead times for high-voltage transformers and specialized cooling equipment can extend for months.

The infrastructure supporting these facilities introduces additional vulnerabilities. Hyperscale campuses depend on stable power delivery, large transformers, advanced cooling systems, and high-capacity fiber connectivity. Damage to any of these components can disable a facility even if the server infrastructure itself remains intact. Replacement lead times for high-voltage transformers and specialized cooling equipment can extend for months. The infrastructure surrounding these campuses introduces additional exposure. Hyperscale facilities rely on nearby substations, fiber backbones, and submarine cable landing stations that connect them to global networks. Many of these systems sit outside secured campuses and may be easier to disrupt than the facilities themselves.

The scale of capital tied to this infrastructure is already substantial. Gulf sovereign investors have become increasingly active participants in global AI infrastructure financing. Abu Dhabi's ADQ partnered with Energy Capital Partners on a $25 billion platform focused on datacenters and power infrastructure in the United States. Dubai-based DAMAC Properties announced plans to invest approximately $20 billion in US datacenter development. Saudi-backed DataVolt has outlined roughly $20 billion in investment tied to AI datacenters and supporting energy infrastructure.

In parallel, the Gulf is developing large domestic AI infrastructure clusters. One of the most prominent examples is Stargate UAE, a planned AI campus in Abu Dhabi expected to exceed $30 billion in construction costs and ultimately scale toward roughly 5 gigawatts of computing capacity.[3] The project involves partnerships between G42, OpenAI, Oracle, NVIDIA, Cisco, and SoftBank and is designed to anchor a broader UAE-US AI ecosystem supporting sovereign AI development and regional cloud infrastructure.

Gulf capital is also embedded in broader global infrastructure vehicles. Abu Dhabi's MGX has invested in OpenAI's broader Stargate initiative and participates in international AI infrastructure financing efforts alongside major technology firms and infrastructure investors. These investments reflect the central role artificial intelligence infrastructure now plays in national economic strategies. Saudi Arabia and the United Arab Emirates have positioned AI infrastructure, cloud computing, and sovereign AI capabilities as core pillars of their long-term economic diversification plans.

Attacks on hyperscale infrastructure could therefore alter how this capital is deployed. Sovereign investors and governments may reassess the geographic concentration and security assumptions behind large AI infrastructure projects. If datacenters are increasingly perceived as targetable infrastructure during geopolitical conflict,

3: "Introducing Stargate UAE," OpenAI, May 22, 2025.

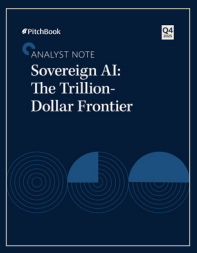
governments and institutional investors may reconsider where tens of billions of dollars in planned AI infrastructure investment are deployed.

The broader pattern suggests the definition of strategic infrastructure is evolving. Energy assets dominated the strategic landscape of the twentieth century. Telecommunications networks became central targets as digital communications expanded. Artificial intelligence infrastructure is emerging as the next foundational layer. The shift mirrors the evolution of semiconductor fabrication plants (fabs). Once viewed primarily as industrial assets, fabs are now treated as strategic infrastructure tied to national security and industrial policy. Hyperscale AI campuses appear to be moving in a similar direction.

As compute infrastructure becomes central to economic activity, technological competitiveness, and national digital capacity, hyperscale AI campuses are becoming strategic assets in their own right.

PitchBook provides actionable insights across the global capital markets.

Additional research:



Q4 2025 Analyst Note: Sovereign AI: The Trillion-Dollar Frontier

Download the report here

Q4 2025 AI VC Trends

Download the report here

PitchBook Insights is an online compendium of in-depth data, news, analysis, and perspectives that shape the private capital markets.

PitchBook subscribers enjoy exclusive access to a comprehensive suite of private market insights, including proprietary research, news, data, tools, and more on the PitchBook platform.

COPYRIGHT © 2026 by PitchBook Data, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, and information storage and retrieval systems—without the express written permission of PitchBook Data, Inc. Contents are based on information from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. Nothing herein should be construed as any past, current or future recommendation to buy or sell any security or an offer to sell, or a solicitation of an offer to buy any security. This material does not purport to contain all of the information that a prospective investor may wish to consider and is not to be relied upon as such or used in substitution for the exercise of independent judgment.

Nizar Tarhuni
Executive Vice President of Research and Market Intelligence

Paul Condra
Senior Director, Global Head of Private Markets Research

James Ulan
Director, Industry & Technology Research

Report created by:

Dimitri Zabelin
Senior Research Analyst, AI and Cybersecurity

Chloe Ladwig
Graphic Designer

Learn more about PitchBook's Institutional Research team.

Click here for PitchBook's report methodologies.