Billions Under Fire: How Tech Giants Are Paying the Price of War

The battlefields of the U.S.–Israeli war on Iran are no longer confined to ports, refineries, and military bases. In recent weeks, they have extended into the very heart of the Middle East's digital infrastructure.

This shift comes at a moment when Gulf states have been rapidly transforming into hubs for massive cloud investments. Technology companies have poured billions of dollars into building and expanding data centers, turning these facilities into integral components of the region's economic and political landscape not merely background technical infrastructure.

Key Developments on the Ground

A turning point came on March 1, when Iran launched a barrage of drones and missiles toward Gulf countries.

Amazon Web Services (AWS) announced that two of its facilities in the United Arab Emirates sustained direct hits, while a drone strike near a third facility in Bahrain caused what it described as a "material impact."

The company said the attacks resulted in structural damage, power outages, and additional water damage caused by firefighting efforts leading to a prolonged recovery. This marks the first known instance in which a military operation has disrupted a data center belonging to a major American technology firm.

On March 23, Amazon reported that its "Bahrain region" experienced disruptions due to drone activity, adding that it was assisting customers in migrating operations to other regions.

The company did not confirm whether the facility had been directly hit but emphasized that the operational environment in the region had become unpredictable—marking a second disruption within a single month.

Then, on April 1, Bahrain's Interior Ministry announced that civil defense teams had extinguished a fire at a company facility following what it described as an "Iranian attack." The following day, Reuters cited Iran's Revolutionary Guard as claiming responsibility for targeting an Amazon facility in Bahrain.

The targeting has not been limited to the Gulf. Bloomberg reported that Israel and the United States struck two data centers in Tehran during the early weeks of the war, one of which was linked to the Revolutionary Guard.

The Royal United Services Institute (RUSI) noted that these strikes reveal a new logic of targeting: data centers host both civilian and military applications,

including command-and-control systems and projects such as the U.S. “Project Maven,” making them dual-use assets.

It added that the Revolutionary Guard had published a list of “legitimate” targets that included Amazon, Microsoft, Google, IBM, Oracle, and Nvidia reflecting a shift in how these facilities are viewed, from commercial infrastructure to assets of direct military value.

Cloud Infrastructure in the Middle East

Today, critical cloud infrastructure in the Middle East is concentrated primarily in the Gulf particularly in the UAE, Saudi Arabia, Bahrain, and Qatar.

According to Emirates NBD, the UAE hosts 35 data centers, followed by Saudi Arabia with 20 and Qatar with five. This underscores the prominence of Abu Dhabi, Dubai, Riyadh, and Jeddah, alongside a smaller footprint in Manama and Doha.

The Gulf has become a regional hub for cloud computing thanks to abundant energy resources and capital. Yet these same facilities have grown more visible and more vulnerable—in times of war.

Within this landscape, AWS operates cloud regions in Bahrain, the UAE, and Israel. As the Associated Press explains, each region consists of multiple independent data centers designed to ensure redundancy and continuity. However, they are not immune to missile strikes or drone attacks.

Amazon launched its cloud region in Israel in 2023, while Google activated its first local cloud region there in 2022 to serve government and military clients.

This highlights how the region’s cloud infrastructure stretches from the Gulf to the eastern Mediterranean and how it is tied not only to commercial services but also to government and security contracts.

The expansion is underpinned by massive investments. Microsoft plans to invest $15.2 billion in the UAE between 2023 and 2029 and had already spent $7.3 billion by the end of 2025. In partnership with G42, it also announced plans to expand UAE data center capacity by 200 megawatts, with operations expected before the end of 2026.

Amazon, for its part, has committed more than $5.3 billion to build a new cloud region in Saudi Arabia. Meanwhile, Google and Saudi Arabia’s Public Investment Fund are working on a $10 billion project to establish a “global AI hub” in the kingdom.

Oracle continues to expand its presence in Jeddah and is opening a new region in Riyadh, while preparations are underway for the “Stargate” project in Abu Dhabi

envisioned as the nucleus of a massive, multi-gigawatt data center campus.

These facilities do far more than store data. They provide the computational power needed to run artificial intelligence models, host government systems and financial infrastructure, and support startups and public institutions alike.

Yet this very role increases their vulnerability. They depend on electricity, telecommunications, and water and remain large, easily identifiable installations.

The Associated Press notes that AWS relies on redundancy across water, power, telecommunications, and internet connectivity to ensure continuity. However, its physical security measures are primarily designed to prevent intrusion not to withstand military strikes making these centers closer to critical industrial facilities than to silent “data warehouses.”

Economic and Operational Implications

The strikes have made clear that data centers are no longer merely technical components they are now critical infrastructure.

AWS and similar services underpin the digital backbone of government, financial, educational, and commercial sectors. This is why Amazon has urged customers to migrate their operations and data to other regions.

While the Associated Press warned that the loss of a single data center may be manageable, losing multiple centers within the same region could create a real capacity shortfall and trigger broader outages.

Operationally, the crisis has revealed that choosing a cloud location is no longer merely a technical or financial decision it is a strategic one tied to political and geographic stability. AWS has advised customers to back up their data and shift operations to unaffected regions.

The Center for Strategic and International Studies noted that adversaries who once targeted oil pipelines and refineries can now, in the “age of computing,” shift toward data centers, the power infrastructure that supports them, and fiber-optic chokepoints.

This shift helps explain why such facilities are increasingly treated as targets of economic and operational value on par with ports and power plants.

Economically, the strikes do not appear to be isolated incidents but rather a warning: massive investments in cloud infrastructure are now exposed to the same geopolitical risks that threaten maritime routes and energy installations.

Disabling a single data center can paralyze banks and government offices and cost institutions millions of dollars in a short time, according to Bloomberg.

Data centers in the Middle East are no longer peripheral to the economy they are

part of its core equation, much like ports, refineries, and power stations.

In its broader meaning, the war reveals that the digital economy does not operate in a vacuum. It depends on energy, water, fiber optics, and security stability. When any of these links is disrupted or threatened, the applications, services, and transactions that appear “virtual” are affected as well.

What has unfolded since early March shows that modern warfare no longer targets only what moves on land or passes through sea lanes but also the systems that manage data, communications, and services above them.