Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Soňa Muzikárová

Iran war warns that digital infrastructure is a security question

The Iranian strikes on data centers in the Gulf have revealed a vulnerability that many wanted to ignore.

The infrastructure underpinning AI, cloud computing, and other industries is not just a cyber or commercial asset. It is also an enticing target.

Iran drove the point home on March 1, when Shahed drones hit two Amazon Web Services (AWS) data centers in the United Arab Emirates and damaged a third facility in Bahrain, disrupting services across banking, payments, and consumer applications.

Iran's Islamic Revolutionary Guard Corps then issued a list of 29 additional targets that it planned to attack across the Gulf, including regional assets belonging to US hyperscalers such as Google, Microsoft, Oracle, Nvidia, IBM, and Palantir, some of whose AI services the US Department of Defense has used against both Iran and Venezuela.

This is the first time that a country has targeted commercial data-center infrastructure in an organized fashion.

Europe, especially, should pause and reflect on the assumptions underlying digital-infrastructure investments and deployments, because Iranian drone strikes on data centers in the Middle East have implications for its own economic security.

To see why, one first must understand how deployments of cloud and network compute infrastructure have already changed.

Infrastructure is being brought physically closer to the user

In the past, cloud computing relied largely on large-scale, centralized hubs that were often located outside the user's immediate environment; for example, a European manufacturer or financial intermediary would route workloads to AWS data centers in Northern Virginia.

But now, such infrastructure is being brought physically closer to the user and the enterprises, public services, industrial systems, and individual devices that depend on it—what the industry refers to as "edge computing."

Since even small lags can degrade performance, accuracy, or service quality, such systems depend on low-latency processing close to where the data is generated and used

Recent European research shows that EU edge nodes grew from 498 in 2022 to 1,836 in 2024, with 75% of European enterprises expected to integrate cloud-edge solutions into their operations by 2030.

This localization reflects two mutually reinforcing trends. The first is the rapid expansion of AI applications that rely on intensive computing and real-time data processing.

Many of these—such as autonomous vehicle perception and control systems and high-frequency trading algorithms—cannot tolerate delays.

Since even small lags can degrade performance, accuracy, or service quality, such systems depend on low-latency processing close to where the data is generated and used.

Data localization

The second trend is the growing push for data localization, privacy, and regulatory compliance—which is particularly strong in Europe, owing to the EU's General Data Protection Regulation (GDPR) and AI Act.

Previously globalized cloud architectures are fragmenting into jurisdiction-bound deployments that must operate within legal borders, each with its own compute, storage, and processing stacks.

As matters stand, however, the distributed, layered data infrastructure underpinning Europe's critical functions—across communications, finance, health care, logistics, and industrial operations—creates a disadvantage.

> It is more difficult for European operators to pursue the kind of dynamic rerouting that a hyperscaler could execute in response to a facility outage or physical disruption

If you are a major telecommunications company operating sovereign cloud and edge infrastructure across multiple member states, you cannot reroute workloads across jurisdictions with the same freedom and speed that big (mostly US-based) hyperscalers can.

Your network data—traffic logs, subscriber metadata, and interconnect records—are subject to the GDPR, national telecommunications law, and EU network and information systems security and resilience rules.

In cases where AI systems are deployed across networks, they must comply with the AI Act's governance requirements, which means jurisdiction-specific constraints are locking the underlying architecture in place.

These systems are also typically deployed as separate instances, rather than as a globally integrated whole.

As a result, it is more difficult for European operators to pursue the kind of dynamic rerouting that a hyperscaler could execute in response to a facility outage or physical disruption.

The geography of the cloud has become a geopolitical risk

This limitation matters even more now that the geography of the cloud has become a geopolitical risk.

The strikes on Gulf data centers show that physical exposure needs to be factored not only into siting decisions but also into broader resilience strategies, redundancy models, and regulatory frameworks.

For European businesses, the new risk-assessment process might start with identifying physical vulnerabilities in the tech stack—including third-party and cloud infrastructure—and stress-testing to determine whether redundancies that exist on paper actually function as intended during physical disruptions.

The EU must start treating digital infrastructure as a security question, rather than only as a regulatory concern

Unlike the United States, Europe has no dominant hyperscalers to protect, no single security apparatus to protect them, and no unified command structure that could extend a governmental umbrella over fragmented, nationally bound instances of digital infrastructure.

Even so, the EU must start treating digital infrastructure as a security question, rather than only as a regulatory concern.

Since a nationally siloed system that checks every regulatory box can still be a single point of failure, Europe urgently needs to close the gap between how critical digital infrastructure is governed and how it is deployed.

For policymakers, that starts with being honest about the concentration risks that

come with locally confined deployments that have no fallback.

It also means coordinating with industry to stress-test cross-border redundancies, investing in cross-border incident coordination mechanisms that can function under stress, and raising EU-wide minimum resilience standards to account for physical concentration and geographic exposure.

Iran may have struck Gulf data centers to raise the costs of US-Gulf technological cooperation, to rattle US-anchored financial markets, or to strike at the AI infrastructure that increasingly underpins American military might.

But it would be a mistake for Europe to treat such tactics as someone else's problem.

The war has already fundamentally changed the calculus for anyone who relies on digital infrastructure. Reinforcing the European tech stack must start now.

Soňa Muzikárová, a former economist at the European Central Bank, a former diplomat at the OECD, and a former senior adviser to the Deputy Minister of Foreign Affairs of the Slovak Republic, is a non-resident senior fellow at the Atlantic Council.