INSS Insight

Clouds of Competition—China's Rise in the Middle East Cloud Market

Yuval Less | No. 1987 | May 26, 2025

The cloud market in the Middle East is emerging as a battleground in the global struggle for technological influence, where the United States and China are competing for control over digital infrastructure, the setting of technological standards, and the shaping of the rules that will govern the flow of information and data. China's technological expansion in the region may gradually pose increasing challenges for Israel—necessitating the development of a strategic and technological policy to safeguard Israeli interests amid evolving trends in both the technological and geopolitical arenas.

In May 2025, US President Donald Trump conducted a diplomatic visit to the Gulf states—Saudi Arabia, Qatar, and the United Arab Emirates. The visit focused on strengthening the United States' strategic partnerships in the Middle East and advancing economic deals, particularly in defense and technology, totaling hundreds of billions of dollars. A special emphasis was placed on artificial intelligence, including an agreement between the United States and the UAE to establish a new AI campus in Abu Dhabi—expected to be the largest of its kind outside the United States. The Emirati company G42 will build the campus, together with leading American tech companies, and will provide infrastructure for data centers and cloud services in the region.

These American investments aim to reinforce the US technological position in the Middle East, while China is concurrently working to strengthen its regional and global presence in advanced technologies—AI, big data, and cloud computing. A prominent example of this is the announcement in February 2025 by the Chinese company Tencent Cloud regarding the launch of its first cloud region in the Middle East, located in Saudi Arabia. A cloud region is a geographic location where a cloud provider operates separate data centers, ensuring service continuity and high performance. The choice of region affects speed, reliability, and regulatory compliance. The announcement was made at the LEAP 2025 technology conference—supported by Saudi Arabia's Ministry of Communications and Information Technology (MCIT)—where Tencent Cloud pledged over $150 million in future investments to support the country's digital transformation in sectors such as media, gaming, commerce, finance, and communications. Tencent Cloud now joins Chinese tech giants Alibaba Cloud and Huawei Cloud, which already operate cloud regions in Saudi Arabia and continue to expand their technological presence in the region. These developments reflect the intensifying competition between the United States and China for technological leadership in the Middle East, with both superpowers committing extensive resources to advanced technologies, AI applications, and cloud infrastructure.

Cloud Computing

Cloud computing provides access to computing resources via the internet—including storage, databases, networks, software, and security services—without the need for physical hardware or local servers. The field has gained significant importance over the past decade, especially following the COVID-19 pandemic, which accelerated the shift to digital models. According to Canalys, global spending on cloud services surged by 21% in the third quarter of 2024 compared to the previous year, reaching $82 billion. Cloud technology is also a central pillar of the digital economy, enabling data storage, processing, and access while enhancing efficiency and innovation. This technology offers economic benefits such as cost savings, but it also requires security measures to protect data and prevent cyberattacks.

Beyond its economic and technological significance, cloud computing carries strategic geopolitical weight. In the digital age, technology is a core component of national security, influencing a country’s capacity to respond to threats in military, technological, intelligence, and economic domains. Nations strive to achieve technological advantages to strengthen their global standing, enhance national security, and promote innovation-driven economic growth. In this context, control over cloud technologies and the data flowing through them is essential for governments and organizations—particularly in sensitive sectors such as defense, finance, healthcare, and transportation. Vulnerabilities in these systems—whether through security breaches or disruptions to critical services—can pose serious risks to national security and economic and political stability. Protecting data sovereignty has likewise become a strategic issue, given that data is a vital asset for national security, privacy, and the economy. As a result, countries are enacting laws and regulations to limit access to data and ensure that it remains under local control, thereby reducing the risk of exploitation by foreign actors.

The Battle for the Cloud—China’s Rise as a Technological Power

The technological arena is at the core of the competition between the United States and China, with each power striving for leadership to secure strategic, military, and economic advantages. Amid the US-imposed restrictions, China views control over advanced technologies—including cloud computing—as a means to reduce dependence on foreign technologies, establish global influence, promote innovation, and strengthen its digital economy. The Chinese government designated cloud computing as a strategic field in its 12th Five-Year Plan (2011–2015), supporting the development of local infrastructure and encouraging the growth of Chinese cloud companies. In its 14th Five-Year Plan (2021–2025), China continues to advance cloud computing to ensure digital sovereignty and global technological leadership—consolidating its control over digital infrastructure, shaping global standards, and expanding into emerging markets, including the Middle East. Today, Chinese companies dominate the cloud market within China and are steadily expanding their global operations.

China’s growing presence in the cloud computing sector has raised concerns among states and organizations, particularly around data security, privacy breaches, unauthorized access to information, and the transfer of data to external parties—especially the Chinese government. While the launch of the Chinese AI model *DeepSeek* attracted global interest, the issue of cloud infrastructure has received less attention, even though the model's data is stored on servers under Chinese control and accessible via cloud infrastructure managed by Chinese companies. Furthermore, the American company NowSecure revealed major security issues, including unencrypted data transfers and insecure storage practices, with data being sent to servers in China controlled by the Chinese firm ByteDance. The risks associated with the use of Chinese cloud technologies also extend to smart vehicles, where data such as real-time location, driving patterns, users' personal information, and the vehicles' technical conditions are collected and stored. This data could be exposed or manipulated—especially when stored on external cloud services such as servers in China, which are subject to government access. Another concern is that data collected via Chinese cloud technologies could be exploited for purposes beyond its original intent—such as user surveillance or industrial and security espionage.

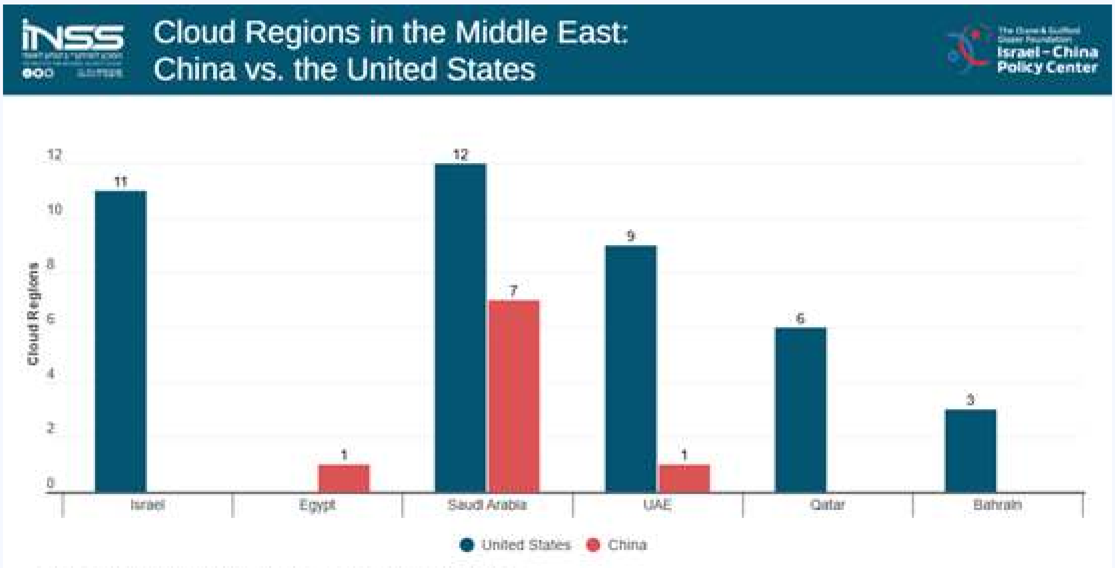
The US government has also expressed concern about the operations of Chinese cloud providers. In August 2020, as part of the Clean Network initiative, the Trump administration issued a warning against the use of Chinese cloud providers in an effort to protect the data of American citizens and businesses from potential exposure to the Chinese government. In January 2022, the Biden administration launched an investigation into Alibaba's cloud operations to assess whether they posed a threat to US national security. The inquiry focused on how the company stores American customers' data—particularly personal information and intellectual property—and whether the Chinese government has access to that data. To date, the findings of the investigation have not been published.

The Dragon in the Cloud—China's Deepening Involvement in the Middle East

China is intensifying its regional involvement in the Middle East through global initiatives, particularly the Digital Silk Road (DSR)—the technological component of China's Belt and Road Initiative (BRI). Over the past decade, Chinese tech giants such as Alibaba, Huawei, and Tencent have become key players in the region's technological landscape. They have expanded their presence through partnerships, the establishment of cloud regions and data centers, training programs, and investments in advanced technologies and infrastructure. While Chinese companies continue to work toward closing the technological gap, US firms still hold a competitive advantage in the Middle East's cloud market due to their long-standing presence and ongoing collaborations with countries across the region.

As of 2024, the United States maintains a dominant position in the global cloud market. The three leading cloud providers are Amazon Web Services (AWS), with a 32% market share, followed by Microsoft Azure at 22%, and Google Cloud at 11%. The Chinese company Alibaba Cloud ranks fourth with 4% of the global market. The US companies Oracle and IBM follow at 3% and 2.5%, respectively, along with China's Tencent Cloud, which holds 2% of the global market.

Figure 1.


Cloud Regions in the Middle East: China vs. the United States

Data:TeleGeography; Processing and Analysis: Yuval Less

According to data from TeleGeography—which specializes in mapping global digital infrastructure—the United States benefits from broad geographic distribution and a higher number of cloud regions in the Middle East. In Qatar, Bahrain, and Israel, US cloud providers dominate the local market, while Chinese companies have only a limited presence. In contrast, in Egypt, the Chinese firm Huawei Cloud operates an active cloud region in Cairo, whereas the three major US tech companies—AWS, Microsoft Azure, and Google—do not currently operate cloud regions there. However, AWS maintains an Edge Location in Cairo, which is a relatively small point of presence compared to a full-fledged cloud region, offering limited compute and storage services.

In Saudi Arabia and the United Arab Emirates, both US and Chinese cloud providers are active, but the United States retains a more prominent presence, with 12 cloud regions in Saudi Arabia and nine in the UAE. By comparison, China has 7 cloud regions in Saudi Arabia and one in Dubai. US investments in the cloud domain in the Middle East also outpace those of their Chinese counterparts. In March 2024, AWS announced plans to establish a cloud region in Saudi Arabia with an investment of $5.3 billion. In comparison, in May 2024, Huawei Cloud launched its first cloud region in Egypt and North Africa with a five-year investment of $300 million.

Although China's investment volume and geographic spread in the Middle East remain limited compared to those of the United States, Chinese companies are making rapid progress into the market. Their success is fueled in part by government support, flexible regulatory environments, and lower development and operating costs, which allow them to offer competitive services. China recognizes the potential of emerging markets and the growing demand for advanced technologies in the Middle East, particularly in the Gulf region. Moreover, the alignment of interests between China and countries in the region provides a solid foundation for long-term cooperation, including in cloud computing. China seeks to leverage its technological strengths to gain economic and strategic influence in the region, while Middle Eastern countries view China as an attractive partner for upgrading digital infrastructure and advancing technological innovation—offering services that are cost-effective, swiftly implemented and free of political conditions. This convergence of interests may lead China to increase its investments in digital infrastructure in the Middle East, with the aim of establishing a technological foothold and promoting its digital models as part of a broader strategy to deepen global influence. While still limited in scope, this trend holds the potential to gradually erode US digital hegemony in the region.

In Israel, Chinese cloud providers have a limited presence, primarily catering to private companies seeking cost-effective pricing or those working in Asian markets. For example, Alibaba Cloud services are available in Israel through the local company Sela, which provides support, guidance, and assistance to Israeli firms interested in using Chinese cloud services. However, Alibaba does not currently operate a local data center in Israel. At the same time, Israeli companies continue to rely on US cloud providers due to their connections with the market and investors in the United States. In 2021, as part of the government-led Project Nimbus initiative, AWS and Google were selected to establish secure public cloud infrastructure for Israeli government and defense entities.

However, China's rise as both a regional and global technological power will gradually pose growing challenges for Middle Eastern countries—including Israel. First, China's rise in the Middle East's cloud market, through investments in digital infrastructure and regional partnerships, adds another layer of tension to the ongoing competition with the United States. This competition is not just limited to technological aspects; it reflects a broader struggle to shape geopolitical spheres of influence, with the Middle East emerging as a key strategic arena. In this context, the deployment of Chinese digital infrastructure across the region could become fertile ground for Chinese cyber activity—such as espionage, surveillance, and intelligence gathering—and could further exacerbate regional tensions in light of US pressure to reduce Chinese involvement in technology and infrastructure.

Second, China's technological expansion—especially in Egypt, the United Arab Emirates, and Saudi Arabia—demands strategic and diplomatic attention from Israel, as these are areas of direct geopolitical and security relevance for the country.

Third, while there is awareness in Israel about data security and the risks of foreign technological influence, the dangers associated with Chinese cloud infrastructure—even in seemingly neutral fields like smart vehicles—are not fully recognized. In 2023, Israel became the third-largest export market for vehicles from China. These vehicles are equipped with smart systems that collect real-time data—such as location, vehicle movement, and system performance. This data is transmitted via cloud infrastructure and may be stored on servers in China or controlled by Chinese firms, raising concerns about the potential use of such information for espionage, intelligence gathering, or even remote control. These risks apply to all smart vehicles, regardless of country of origin. However, given the recurring reports and concerns about Chinese companies violating data privacy and security, the use of Chinese-made vehicles in Israel—particularly within government and defense institutions—should be carefully evaluated. This includes assessing potential national security risks and considering safer alternatives for use in sensitive environments.

In light of the challenges China presents in the technological and geopolitical arenas, it is crucial that Israel thoroughly assess the long-term implications of China's growing role as a regional technological power. Israel should work to formulate a well-coordinated strategic and technological policy—aligned with Western countries, particularly the United States—to ensure its national interests, especially in the areas of data protection, privacy, and national security.

Editors of the series: Anat Kurtz, Eldad Shavit and Ela Greenberg