Why America's Data Centres are Becoming Defence Infrastructure

15 SEPTEMBER 2026

Nicole Siembieda

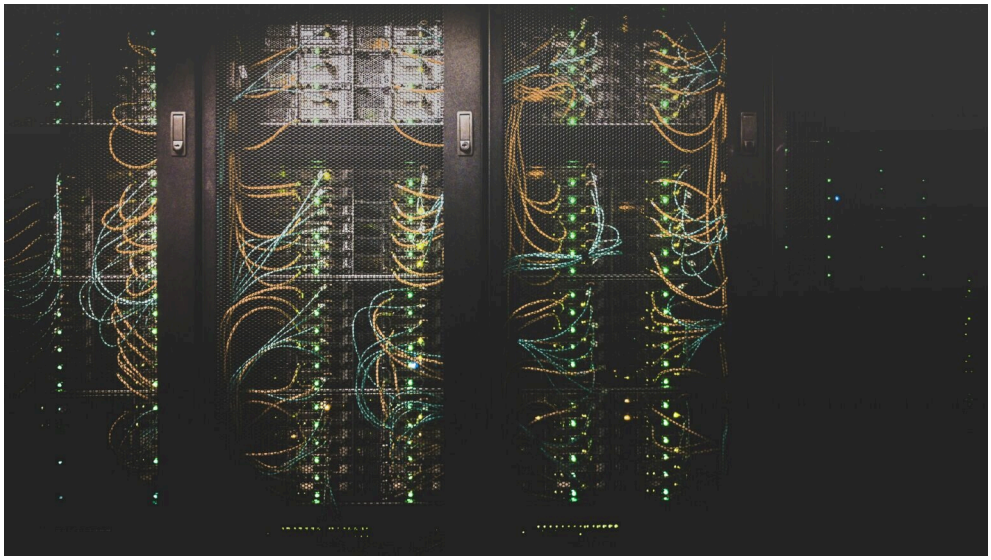

Photo by Taylor Vick on Unsplash

In the aftermath of Operation Epic Fury, the Islamic Revolutionary Guard Corps (IRGC) used drones to strike three Amazon Web Services (AWS)-owned data centres in the Middle East, two in the United Arab Emirates and one in Bahrain (Chan, 2026). In late July, the IRGC further targeted AWS data centres in Bahrain with missiles, which were analysed using the European Space Agency's satellite imagery (Solon, 2026). Similarly, these attacks have also been prevalent in Russia's full-scale invasion of Ukraine, where civilian energy infrastructure has been continuously targeted (International Energy Agency, 2024). This reflects a broader trend in hybrid warfare, as strikes are not only confined to traditional military targets but also extend to digital and energy infrastructure due to their dual-use nature.

As commercially owned AI data centres, such as those owned by Amazon's AWS, become targets in the contemporary warfare landscape, this highlights the need to treat such infrastructure as a critical defence priority. This need is further highlighted by the dual-use nature of AI data centres, which provide both civilian and military functions. Additionally,

the expansion of American commercial AI data centres abroad compounds the challenge of protecting them. Thus, this paper discusses how the role of data centres has evolved with generative artificial intelligence and its implications for U.S. national security.

Context

Data centres are physical facilities that house information technology (IT) infrastructure for building and running computing services and for storing data (Susnjara & Smalley, n.d.). With the development of cloud computing, data centres hosting multiple servers became more widespread due to substantial economies of scale, replacing companies' historical in-house servers (Armbrust et al., 2009). This transition to outsourcing and the consolidation of data centres occurred throughout the 2010s to accommodate the expansion of cloud computing. However, demand for larger and numerous data centres accelerated with the rise of generative artificial intelligence, as training and running AI models required greater electricity use and specialised infrastructure (Shehabi et al., 2024). For example, the Government Accountability Office (GAO) conducted a study on data centre consolidation and recommended that government agencies outsource and consolidate their data centres (U.S. Government Accountability Office, 2016). As a result, government agencies and companies turned to hyperscale data centres for efficiency, profit maximisation, and a strategic competitive edge.

Furthermore, building the infrastructure to gain a technological advantage in AI over adversaries became strategically important amid the AI arms race. The race increasingly unfolds within a hybrid warfare environment, in which technological superiority has become a primary asset in great-power competition. Jensen (2025) explored how advanced AI agents, for example, could give the U.S. advantages in deterring cyber espionage and in modelling and anticipating hostilities. These capabilities have already been demonstrated in Ukraine, as the Armed Forces of Ukraine have used Microsoft to protect themselves against cyberattacks and Clearview AI for counterespionage purposes (Harding, 2026). As AI becomes more advanced and reliable in operations, its strategic importance will only increase. This development is evident in Operation Epic Fury, where Anthropic's Claude was used to identify and prioritise precise targets to simultaneously strike multiple targets (Copp et al., 2026).

Meanwhile, artificial intelligence has become an integral part of military operations, communication, and strategy. For example, during Operation Epic Fury, the U.S. military utilised Palantir's Maven Smart System with Anthropic's Claude to simultaneously strike 1,000 targets at the beginning of the offensive (Copp et al., 2026). Similarly, Ukraine has relied on aid from the U.S.-based technology and AI companies, such as SpaceX, Microsoft, and ClearviewAI (Harding, 2026). Advanced AI in warfare is used not only for targeting and simulations but also for embedding in

defence communications networks and for analysing intelligence. As a consequence, data centres that were built for commercial purposes now have high strategic value for the military.

Data Centres as Dual-Use Infrastructure

The Critical Infrastructure Protection Act of 2001 defines critical infrastructure in a consequence-based manner, considering infrastructure critical when its absence or destruction would have ramifications for public safety, national security, or the economy (Cybersecurity and Infrastructure Security Agency, n.d.). This definition carries significant weight when assessing AI data centres because it means that critical infrastructure can be essential to national security yet remain commercially owned and not directly used in defence. However, AI data centres are dual-use infrastructure, meaning they serve a purpose in both civilian life and the military. Dual-use infrastructure and goods are multifaceted in that they can be targeted as defence infrastructure even when they are primarily used commercially.

This dilemma reflects a broader trend in the defence industry: militaries becoming more reliant on dual-use technologies from the private sector, especially start-ups (Nicastro, 2024). A prime example of this shift is the company Palantir, which has two similar systems to help organise and analyse data into accessible dashboards – one functions as a logistics agent for commercial use, while the other works as an investigative tool for defence and law enforcement (Haskins, 2025). As explicated above, Palantir's software was used for targeting in Operation Epic Fury, and the Department of War has designated it a "program of record", indicating its long-term intention to contract Palantir (Mande & Allen, 2026).

The incentive behind this shift to the private sector, particularly with emerging technologies, is both strategic and economic. Dual-use technologies in the private sector often face greater competition from domestic and international rivals, prompting them to innovate faster and smarter and remain competitive on price. Additionally, because of their dual-use nature, they are not entirely dependent on revenue from government contracts. Strategically, dual-use technologies are readily available and can be deployed on the battlefield immediately, rather than being made from scratch through a complex Research and Development process. This adaptability has proven essential in the contemporary warfare environment, where having the latest technology can supersede enormous military budgets (Bondar, 2025). In particular, AI is developing quickly, and the strategic advantage of having the most advanced AI system is crucial. The U.S. government is thus incentivised to use commercially owned data centres for defence needs to bypass the cost and time constraints of building government-exclusive data centres.

While efficient, the U.S. government's contracting with the private sector to source dual-use data centres for defence raises some complexities.

Following Iran's targeting of data centres after Operation Epic Fury, adversary militaries may target data centres for their potential to contribute to military operations. In this case, the responsibility of protection becomes blurred, as commercial entities may be unwilling to shoulder the burden of protecting and insuring their infrastructure from war, yet these facilities are neither owned nor operated by the military or the government (Harding, 2026).

Overseas Data Centres

As the demand for data centres increases, American companies have built abroad to avoid zoning laws and politics, and to take advantage of high investment and low energy costs (Belle et al., 2026). Overseas data centres carry a higher risk than domestic centres because they hold sensitive and high-value assets, and can be vulnerable to geopolitical tensions (Belle et al., 2026). Additionally, building data centres abroad subjects the United States to another nation's legal requirements, meaning the US cannot guarantee the same level of control over sensitive data and infrastructure as it would domestically (Belle et al., 2026). The profit maximisation of dual-use facilities, therefore, creates a tension between commercial incentives and national security safeguards.

The AWS-linked data centres in the United Arab Emirates and Bahrain illustrate this vulnerability. The Gulf attracts energy infrastructure due to its high capital investments and low energy costs (Belle et al., 2026). The data centres' physical proximity to Iran made targeted strikes viable, while their value made them a target. Iranian state media claimed that the data centres were targeted for their military and intelligence capabilities (Belle et al., 2026). However, it is unlikely that the IRGC would have known whether the United States was using these exact facilities for military purposes, and thus likely targeted these centres as a message to both the United States and centres' host countries (Jarnecki & Sylvia, 2026). Data centres are the physical infrastructure behind the U.S. digital economy. As a result, attacks on data centres can serve a symbolic purpose of striking a physical extension of American economic and technological power. Thus, as AI data centres evolve and geopolitical tensions intensify, continuing to build overseas data centres creates national security vulnerabilities.

Adapting the U.S. Critical Infrastructure Framework

When defining critical infrastructure, the U.S. currently operates under a framework that categorises it into 16 general sectors (Cybersecurity and Infrastructure Security Agency, n.d.). Within this framework, data centres fall under the Information Technology Sector, which is broadly defined as "functions [that] produce and provide hardware, software, and information technology systems and services and—in collaboration with the Communications Sector—the Internet" (Cybersecurity and Infrastructure Security Agency, n.d.). In addition, there have been several executive orders

from President Donald Trump that allude to AI and AI data centres as critical infrastructure, such as the Promoting Advanced Artificial Intelligence Innovation and Security and the Accelerating Federal Permitting of Data Centre Infrastructure acts (Executive Order No. 11409, 2026; Executive Order No. 14318, 2025).

While these frameworks are valuable, they do not explicitly identify data centres as a distinct category of critical infrastructure, nor do they state a clear protection mechanism. This is problematic because data centres supporting AI for both the military and civilian sectors are recent targets of adversaries. Furthermore, since many data centres are privately owned, they "do not have their own armies" nor a vast intelligence network like the government to protect data centres (Harding, 2026, para. 4). Therefore, it is important to establish criteria for when data centres need to be protected as defence assets so that the government can partner with the company to protect the facility. Finally, the current critical infrastructure framework focuses primarily on domestic infrastructure, leaving a policy gap on the protection of overseas data centres. As the United States seeks to maintain a competitive advantage in AI and technology, it is essential that the U.S. government closes these policy gaps to ensure strategic resilience and deterrence.

Conclusion

Data centres are no longer facilities for computer systems but complex critical infrastructure that supports artificial intelligence for civilian and military use. In the contemporary geopolitical environment, AI data centres contribute to the technological leverage that facilitates the AI arms race and occupy significant physical space in the U.S. digital economy. AI data centres also reflect a trend of the government relying more heavily on the private sector for R&D in emerging technologies in favour of adaptability and efficiency. With this shift towards the private sector, the mechanisms for protecting data centres that contribute significantly to defence become less clear, as responsibility is divided between a commercial entity, which can be overseas, and the government. The current critical infrastructure classification system adds to this confusion, as protection guidance is generalised by sector. As AI becomes increasingly important to modern warfare, protecting AI data centres will be essential to U.S. national security.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2009, February 10). Above the clouds: A Berkeley view of cloud computing (Technical Report No. UCB/EECS-2009-28). University of California, Berkeley, Electrical Engineering and Computer Sciences. https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/Archive/EECS-2009-28.pdf

Belle, D., Nadgir, N., Rocha, A., Tabassi, E., Wirtschafter, V., & Wright, T. (2026, August 3). The national security implications of building frontier AI data centers overseas. Brookings Institution. https://www.brookings.edu/articles/the-national-security-implications-of-building-frontier-ai-data-centers-overseas/

Bondar, K. (2025, January 13). How Ukraine rebuilt its military acquisition system around commercial technology. Center for Strategic and International Studies. https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology

Chan, K. (2026, March 4). Iranian strikes on Amazon data centers highlight industry's vulnerability to physical disasters. AP News. https://apnews.com/article/amazon-aws-data-center-uae-iran-bahrain-71066b0a822c4cfd88b61e3fe79af917

Copp, T., Dwoskin, E., & Duncan, I. (2026, March 4). Anthropic's AI tool Claude central to U.S. campaign in Iran, amid a bitter feud. The Washington Post. https://www.washingtonpost.com/technology/2026/03/04/anthropic-ai-iran-campaign/

Cybersecurity and Infrastructure Security Agency. (n.d.). Critical infrastructure sectors. Retrieved August 27, 2026, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Executive Order No. 14318, 90 Fed. Reg. 35523 (July 23, 2025). https://www.whitehouse.gov/presidential-actions/2025/07/accelerating-federal-permitting-of-data-center-infrastructure/

Executive Order No. 14409, 91 Fed. Reg. (June 2, 2026). https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/

Harding, E. (2026, March 19). Data is now the front line of warfare. Center for Strategic and International Studies. https://www.csis.org/analysis/data-now-front-line-warfare

Haskins, C. (2025, August 11). What does Palantir actually do? Wired. https://www.wired.com/story/palantir-what-the-company-does/

International Energy Agency. (2024, September 19). Ukraine's energy system under attack. https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack

Jarnecki, J., & Sylvia, N. (2026, March 19). Iranian data strikes shake global digital infrastructure. Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/commentary/iranian-data-strikes-shake-global-digital-infrastructure

Jensen, B. (2025, May 7). Protecting our edge: Trade secrets and the global AI arms race [Congressional testimony]. Center for Strategic and International Studies. https://www.csis.org/analysis/protecting-our-edge-trade-secrets-and-global-ai-arms-race

Mande, M., & Allen, G. C. (2026, June 2). What is Maven Smart System, and what does it do? The flagship software platform of AI-enabled warfare, explained. Center for Strategic and International Studies. https://www.csis.org/analysis/what-maven-smart-system-and-what-does-it-do

Nicastro, L. A. (2024, September 23). The U.S. defense industrial base: Background and issues for Congress (CRS Report No. R47751). Congressional Research Service. https://www.everycrsreport.com/reports/R47751.html

Shehabi, A., Newkirk, A., Smith, S. J., Hubbard, A., Lei, N., Siddik, M. A. B., Holecek, B., Koomey, J., Masanet, E., & Sartor, D. (2024). 2024 United States data center energy usage report. Lawrence Berkeley National Laboratory. https://doi.org/10.71468/P1WC7Q

Solon, O. (2026, July 28). Amazon data centers hit in Iran strikes, satellite images show. Yahoo Finance. https://finance.yahoo.com/technology/articles/amazon-data-centers-hit-iran-083832960.html

Susnjara, S., & Smalley, I. (n.d.). What is a data center? IBM. Retrieved August 27, 2026, from https://www.ibm.com/think/topics/data-centers

U.S. Government Accountability Office. (2016, March 3). Data center consolidation: Agencies making progress, but planned savings goals need to be established (GAO-16-323). https://www.gao.gov/products/gao-16-323