The Gulf Is America's Next AI Security Test

by Elizabeth Dent **(/experts/elizabeth-dent)**

Nov 19, 2026

Also published in Foreign Policy

ABOUT THE AUTHORS



Elizabeth Dent (/experts/elizabeth-dent)

Elizabeth Dent is the Nathan and Esther K. Wagner Senior Fellow at the Washington Institute for Near East Policy, where she focuses on U.S. foreign and defense policy toward the Gulf states, Iraq, and Syria.

Articles & Testimony

Even after the Nvidia scandal ushered in new U.S. government rules to counter Chinese tech risks, significant loopholes remain open in the Gulf states.

In the wake of Jensen Huang's stunning resignation as CEO of Nvidia over his alleged affair with a Chinese spy, the U.S. Commerce Department this week announced **new export controls (https://www.bis.gov/press-release/bis-issues-rule-addressing-remote-access-american-super-intelligence-technology)** on artificial intelligence and semiconductors. These rules mark the most serious effort to close the loopholes that have allowed Chinese companies to obtain access to U.S. chips and computing power. The new interim rules target three vulnerabilities: Chinese rerouting of U.S.-made AI chips through third countries, rented access to AI computing power, and Chinese chip designers' ability to manufacture advanced chips at non-Chinese facilities.

The Nvidia scandal—including the alleged rerouting of Nvidia's most advanced chips to China and the Trump administration's apparent quiescence—underscores the scope of the Chinese threat to U.S. artificial intelligence technology. The new rules close important gaps, but they do not resolve the threat. The next area where the United States is especially exposed is the Gulf, where the most advanced U.S. chips are now **arriving (https://www.reuters.com/business/us-authorizes-export-advanced-american-semiconductors-companies-saudi-uae-2025-11-19/)** , to be utilized in data centers operated by partners that maintain extensive ties with China.

The Gulf magnifies the Nvidia problem. Both the United Arab Emirates and Saudi Arabia are trying to shift their economies away from oil, and they're placing AI at the center of their strategies. In May 2025, U.S. President Donald Trump **announced (https://www.reuters.com/business/us-authorizes-export-advanced-american-semiconductors-companies-saudi-uae-2025-11-19/)** that both countries would be able to purchase advanced U.S. chips to help facilitate these efforts. Abu Dhabi and Riyadh are financing massive AI buildouts, where Nvidia chips

will be installed, operated, and even rented to customers or cloud tenants. The two monarchies are taking advantage of their desert land areas, access to lower-cost energy, and deep coffers, offering Nvidia an appealing market and affording Washington an opportunity to keep U.S. technology at the center of the AI buildout.

Both the Saudis and the Emiratis, however, also maintain deep relations with China. Washington fears that Beijing could gain access, intentional or not, through its contractors or cloud customers—or via hardware or software that may be connected to U.S. systems or chips. Chinese infiltration could occur through a trusted partner, with or without their knowledge, without directly acquiring the restricted chips.

That's why companies such as the UAE's Group 42 have caught the eye of China watchers and technology hawks. The group's past links to China and its tech sector, even though the company **publicly (https://fortune.com/2023/12/07/emirati-ai-company-picks-side-against-china-g24-us-sanctions/)** renounced them after the Biden administration declared it a security risk, raise questions that diplomatic assurances cannot resolve. The issue is not what the company says but whether its operations, ownership, partnerships, and access to sensitive technology can be independently verified and insulated from possible Chinese exploitation.

Saudi Arabia presents a similar challenge. The kingdom is pursuing AI **autonomy (https://www.washingtoninstitute.org/policy-analysis/saudi-ai-ambitions-create-us-opening)** by seeking control over every layer of the technology stack. But Washington will want evidence that Saudi officials can protect their data centers and cloud services from unauthorized access. And that case is increasingly difficult to make as Saudi Arabia continues to partner with both U.S. and Chinese technology companies.

The new rules make the Gulf an important litmus test for whether Washington can enforce its new approach in third-country data centers. Gulf-based facilities will need to prevent restricted users from accessing compute power enabled by U.S. chips, including indirectly through the cloud or other intermediaries. It's not just about whether a Chinese company or user can rent compute power through a Gulf partner, but also whether the safeguards are in place for partners who maintain U.S. compute power to verify ownership and the affiliations of users.

U.S. export controls were designed for trade in tangible goods, but the Commerce Department has now acknowledged that simply controlling the physical movement of chips is not enough. The new rules extend export controls to some forms of remote access and computing power—intended, for example, to prevent a Chinese company from renting access to a processor through a data center or cloud provider. The new rule is a major step forward but not a complete solution. Safeguarding U.S. chips will require more than protecting the physical product or regulating direct access. It will require oversight of the people and systems that can use the computing power that those chips provide. That means guarding not just the chips' physical location but also their ownership, network architecture, and consumer access.

Instead of determining which country or firm is purchasing a chip, an export policy will need to ask who will own and operate the facility, who can administer the compute power, which customers can rent its processors, what the networking and software infrastructure is made of, the nationality of users, and even whether the systems can be accessed outside of where they are housed. A processor being utilized in a Gulf data center, for example, may be used to provide computing power to a restricted Chinese company or state institution through the cloud—so controls must follow the user, not just the export.

Nvidia sells the most advanced chips in the business. Its former CEO, who made himself the face of the company's strategy and government relations, was close with Trump and has decried more stringent export controls on AI chips, arguing that such restrictions will merely move more consumers toward Chinese suppliers like Huawei. His influence may have helped **persuade (https://www.nytimes.com/2026/11/07/business/economy/nvidia-chips-chinese-firms.html)** Trump to sell limited amounts of the H200 chip to China. But the concern extends beyond

Huang's influence. Questions about the administration's handling of the policy—including conflicts of interest involving U.S. Commerce Secretary Howard Lutnick (https://www.nytimes.com/2026/11/15/us/politics/trump-lutnick-ai-chips-nvidia-cantor-fitzgerald.html) , Trump's own financial interests (https://www.washingtonpost.com/business/2026/11/16/trumps-stake-nvidia-grew-much-62-million-before-scandal-broke-out/) in Nvidia, and other relationships between U.S. officials and companies that may have benefited from certain sales, like Jared Kushner (https://www.vanityfair.com/story/jared-kushner-hacked-phone-secret-negotiations?srsltid=AYCX9vJAkOGBUfYAMsSTpKmjiSKMZXAu_JYKM7JDtfor9QzkbJhH9o8r) 's—warrant a review of these decisions. Regulators should begin by reexamining the decision (https://www.commerce.gov/news/press-releases/2025/11/statement-uae-and-saudi-chip-exports) to allow the sale of Nvidia's most advanced chips to Saudi Arabia and the UAE.

A new oversight policy would not entail a crackdown on Nvidia or a blanket ban on selling further advanced chips to Gulf states. Instead, Washington would expand access only when Gulf states meet specific conditions and establish guidelines for continuously evaluating who can access the technology. The new framework should become the baseline for future Gulf licenses that can identify approved facilities and consumers; limit chip quantities and aggregate compute power; prohibit restricted access and rentals; and require oversight of inventories, access logs, and control standards. Washington should also retain the right to suspend a license at any time. China has already sought to lease (https://www.cnbc.com/2026/11/05/moonshot-ai-nvidia-chips-europe-china.html) capacity through data centers in Europe and accessed U.S. chips to train its models through systems (https://www.cnbc.com/2026/07/23/moonshot-kimi-nvidia-ai-chips-export-ban.html) in Thailand.

When the Democrats take control of the U.S. Congress in January, they will likely press (https://www.politico.com/live-updates/2026/11/10/congress/two-key-democrats-signal-tougher-scrutiny-of-nvidia-chip-exports-01160036) for tougher oversight of foreign chip deals—as they should. Democrats and Republicans have a considerable opportunity to work together (https://www.banking.senate.gov/newsroom/minority/banks-warren-introduce-ai-overwatch-act) on this issue. Even though this week's new rules help address some of the areas of concern, they are an executive branch policy and thus subject to change at any moment. Congress can focus on passing the Remote Access Security Act (https://www.congress.gov/bill/119th-congress/house-bill/2683) , which will require export policy to include remote access controls, and the AI Overwatch Act (https://www.congress.gov/bill/119th-congress/senate-bill/4456/all-info) , which will give Congress more oversight over foreign chip sales.

For the UAE and Saudi Arabia, access to the most advanced chips is still possible but now comes with stronger U.S. demands—and any failure to adhere to those conditions should mean that access is immediately cut off. Fair or not, the Nvidia scandal raises the cost of assuming that trust is enough protection.

However, tighter U.S. restrictions also carry some risk. If U.S. requirements become too stringent, intrusive, costly, or unpredictable, Gulf governments may turn back toward Chinese tech or tilt toward other suppliers with fewer restrictions. Greater reliance on Chinese tech would not replace the U.S. technological edge overnight but over the long term, it could well reduce U.S. influence.

The UAE and Saudi Arabia are seeking slightly different things. The UAE is leading the space in dealmaking and pushing the next generation of AI models, while Saudi Arabia is seeking to build out local compute capacity. For both, ongoing relationships with Chinese tech companies will remain an issue, and Washington will need stringent controls and verifications on who can access and use the systems.

China's challenge to U.S. AI is a serious threat, and the United States must strengthen its technological defenses in the Gulf and elsewhere. The Commerce Department's new rules are a meaningful step in closing the regulatory gap in U.S. export policy on chips. The Saudis' and Emiratis' AI ambitions make them key tests of whether the United

States can enforce this approach. That requires systematic and continuous scrutiny of many more layers of the AI value chain than current U.S. export controls offer, including ownership, users, infrastructure, and remote access. The Saudis and Emiratis will, of course, say that they can be trusted. But in the post-Huang AI space, it is simply too risky to rely on assurances alone.

Elizabeth Dent is the Wagner Senior Fellow at The Washington Institute and former director for the Gulf and Arabian Peninsula at the Pentagon. This article was originally published ***on the Foreign Policy website (https://foreignpolicy.com/2026/11/19/nvidia-huang-scandal-ai-security-chips-export-controls-gulf-saudi-uae/)*** *.* ❖

RECOMMENDED



ARTICLES & TESTIMONY

Iran's Shift from Soft to Hardened Targets: Preliminary Observations from the RAF Fairford Incident

Nov-Dec 2026

◆

Crispin Smith,
Matthew Levitt

(/policy-analysis/irans-shift-soft-hardened-targets-preliminary-observations-raf-fairford-incident)



BRIEF ANALYSIS

Moroccan Police Training Can Help Break the Gaza Deadlock

Nov 18, 2026

◆

Salma Annasse

(/policy-analysis/moroccan-police-training-can-help-break-gaza-deadlock)



BRIEF ANALYSIS

Lebanon’s Explosives Case Highlights the Judicial Obstacles to Disarming Hezbollah

Nov 17, 2026

◆

Hanin Ghaddar

(/policy-analysis/lebanons-explosives-case-highlights-judicial-obstacles-disarming-hezbollah)

TOPICS

Energy & Economics (/policy-analysis/energy-economics)

Great Power Competition (/policy-analysis/great-power-competition)

Gulf & Energy Policy (/policy-analysis/gulf-energy-policy)

REGIONS & COUNTRIES

Gulf States (/policy-analysis/gulf-states)