ASP | AI IMPERATIVE 2030

SPUTNIK REPORT

Huawei and Hyperscalers:

The Race to Deploy and Defend The AI Cloud

www.AmericanSecurityProject.org

July 2025

Huawei and Hyperscalers:

The Race to Deploy and Defend the AI Cloud

As artificial intelligence ushers in the next industrial revolution, the war over who will lead it is already in full force. China's aggressive, state-driven push for global AI dominance has splintered America's allies over the values of responsible innovation and sparked a technology arms race between Washington and Beijing. If urgent action is not taken to expand and secure American AI infrastructure, the Chinese Communist Party will weaponize global cloud networks to undermine free markets, oppress its people, and covertly influence foreign states and citizens.

If AI competition is a war, then global cloud architecture is the theater. Microsoft, Amazon, and Google control 63% of the world's $900 billion cloud market, a critical win for American AI leadership. But Beijing is on the offensive, infiltrating U.S. systems and proliferating its own predatory AI infrastructure. Worse, some U.S. firms are trading data and compute for Chinese market access, putting U.S. national security at risk. *Huawei and Hyperscalers* explores how Beijing exploits global AI infrastructure and pressures firms to sacrifice safety for growth, then provides actionable solutions for U.S. policymakers to help deploy and defend the cloud.

The Problem

- America's global AI partnerships have rapidly extended U.S. cloud computing infrastructure to the furthest edges of the globe, straining federal oversight capacity and creating critical cybersecurity gaps that CCP-aligned hackers and other cyber criminals exploit for geostrategic gain.
- Anticompetitive state subsidies and loan rates allow Chinese firms to aggressively expand their cloud infrastructure and undercut U.S. and allied firms in global markets. The Chinese Communist Party uses this infrastructure to absorb massive volumes of foreign data while creating lasting technological dependencies in the Global South and elsewhere.
- U.S. hyperscalers cooperate with the CCP's protectionist policies and predatory data ecosystem to gain access to lucrative Chinese markets. This one-way flow of AI resources facilitates Beijing's aggressive weaponization of artificial intelligence and places America's AI development at risk.

The Solution

- To begin reducing the hundreds of millions of cyber attacks on American cloud networks daily, the United States must treat cloud infrastructure as critical infrastructure and afford it the same oversight and protection mechanisms as America's energy, healthcare, and transportation networks.
- Clear rules governing which infrastructure projects threaten U.S. national security would save American firms tens of millions of dollars annually by reducing government delays and cancellations of data cables and other cloud infrastructure. More diplomacy is needed to persuade third nations to work with the United States and not China.
- New legislation is urgently needed to prevent U.S. firms from selling CCP-aligned actors cloud-hosted access to their restricted AI resources. Multi-cloud infrastructure can improve the government's ability to procure competitively priced cloud services from firms that do not transfer U.S. intelligence to China.

Introduction

Amidst escalating great power competition between the United States and China, global leadership in artificial intelligence has become an urgent national security imperative.

Those who can effectively wield AI gain unparalleled insight into human behavior and an incalculable strategic advantage in critical sectors. In defense, AI algorithms slash fog and friction by automating military surveillance, analysis, and logistics. In healthcare, AI revolutionizes diagnostics by synthesizing petabytes of patient data at inhuman speed and accuracy. In finance, high frequency trading algorithms shrink average trade times from minutes to microseconds.[1]

Designing and deploying these revolutionary tools requires prohibitive volumes of data and computing power, or "compute." For this reason, over 90 percent of users access AI through distributed data architecture: the cloud. Cloud networks link supercomputers and data centers to consumers across the world through nearly one million miles of private cable infrastructure and 5G cell phone towers. Three supermassive cloud providers—Amazon, Google, and Microsoft—account for 63% of the $900 billion cloud market,[2] forming a decisive foundation for U.S. AI leadership in the 21st century.

This CMC data center in Vietnam is connected to U.S. cloud infrastructure through undersea data cables. CC: Daoducquan.

However, global cloud dominance comes with risks.

Economies of scale and global AI adoption have rapidly extended American cloud computing infrastructure to the furthest edges of the globe, straining federal oversight capacity and exposing critical cybersecurity gaps. CCP-aligned hackers exploit these vulnerabilities by persistently penetrating U.S. cloud systems at its weak points, while Chinese state-owned enterprises aggressively expand competing infrastructure to displace American firms in the Global South and elsewhere.

These risks are exponentially magnified when U.S. cloud providers choose to work with the Chinese Communist Party to gain access to Chinese markets. Beijing's stringent data laws require American firms to transfer billions of bytes of data and export-restricted processing power to the CCP, creating a one-way transfer of AI resources that grants Chinese firms an unfair edge over their competitors in the United States. These American assets then fuel Beijing's development of AI-powered weapons, surveillance technologies, and cyberattacks targeting U.S. citizens and infrastructure.

As China's AI cloud grows in scale, sophistication, and influence, U.S. policymakers face an unprecedented challenge: how to safeguard American cloud networks from CCP predation without impeding the expansion of this critical AI infrastructure.

Without strong protections, the United States and its citizens remain vulnerable to the CCP and other powerful actors that aim to weaponize its AI infrastructure for malign purposes. But Washington must also promote the global expansion of its cloud computing architecture, or else U.S. AI developers will fall behind China—putting national and international security at risk.

Cloud Market Dominance: America's Biggest AI Advantage

By providing the data and computing capacity needed for all but the biggest firms to leverage artificial intelligence, cloud computing networks are critical for global AI diffusion. The United States is the global pioneer in deploying this infrastructure, far surpassing its nearest competitors in both scale and innovation—but China is on the offensive.

The Rise of Decentralized Cloud Computing

The resources required to store, transmit, and convert data into AI models exceed the capacity of the vast majority of users and organizations. AI training datasets have tripled in size each year since 2010,[3] with computing bandwidth doubling every five months.[4] Deploying these models at scale soon requires even more energy and computing bandwidth than was initially needed for training.[5] As a result, AI data center power demand has grown tenfold since 2022 and is unlikely to peak for at least two decades.[6]

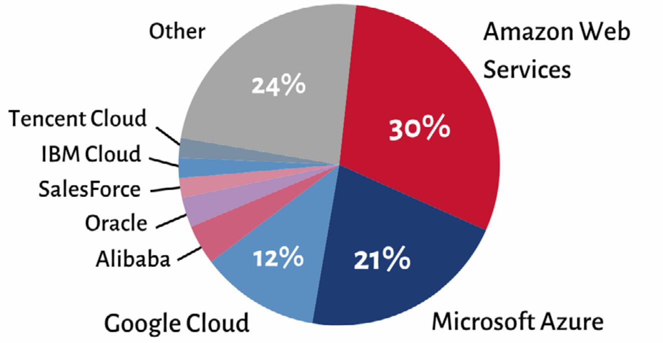
To overcome these barriers, nearly all individuals and firms develop and access AI products and services through the cloud.[7] Cloud computing is the provision of server capacity, processing power, AI software, cybersecurity, and other computing services over internet networks.[8] By outsourcing these foundational resources to a cloud service provider (CSP), users can benefit from the most advanced machine learning and AI tools without building or maintaining any of the underlying architecture. As a result, the global cloud market has grown 46% since 2022,[9] with generative artificial intelligence alone driving over half of all growth.[10]

America's Cloud Computing Hyperscalers

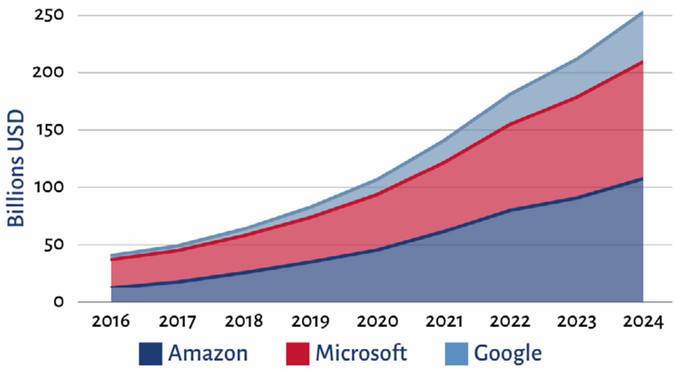
Just three U.S. firms—Amazon Web Services (AWS), Microsoft Intelligent Cloud, and Google Cloud Platforms (GCP)—comprise 63 percent of the global cloud market,[11] 41 percent of worldwide data storage capacity,[12] and 70 percent of global bandwidth usage.[13] In addition to supplying AI's underlying infrastructure, these "hyperscalers" maintain the cloud-native algorithms and platforms that nearly all organizations use to develop AI tools.[14]

Due to their expansive economies of scale, hyperscalers' cloud operating margins are among the highest in the world. In 2024, GCP posted margins of 17 percent,[15] AWS exceeded 38 percent,[16] and Microsoft Intelligent Cloud hit a staggering 72 percent profit.[17] These figures would be even higher if hyperscalers were not also aggressively investing in infrastructure expansion. Microsoft and AWS reinvested around 50% of their 2024 revenue into new data centers and transmission lines,[18] while GCP redirected over 120% of its fourth-quarter revenue to catch up with its supermassive competitors.[19] Global spending on new data centers alone surpassed $255 billion in 2024, with hyperscalers driving most of this growth.[20]

ASP Global Cloud Market Share
(Data: Synergy Research Group, Q4 2024 Cloud Report)



ASP Annual Cloud Segment Revenue
(Data: Amazon, Microsoft, Google Financial Statements)

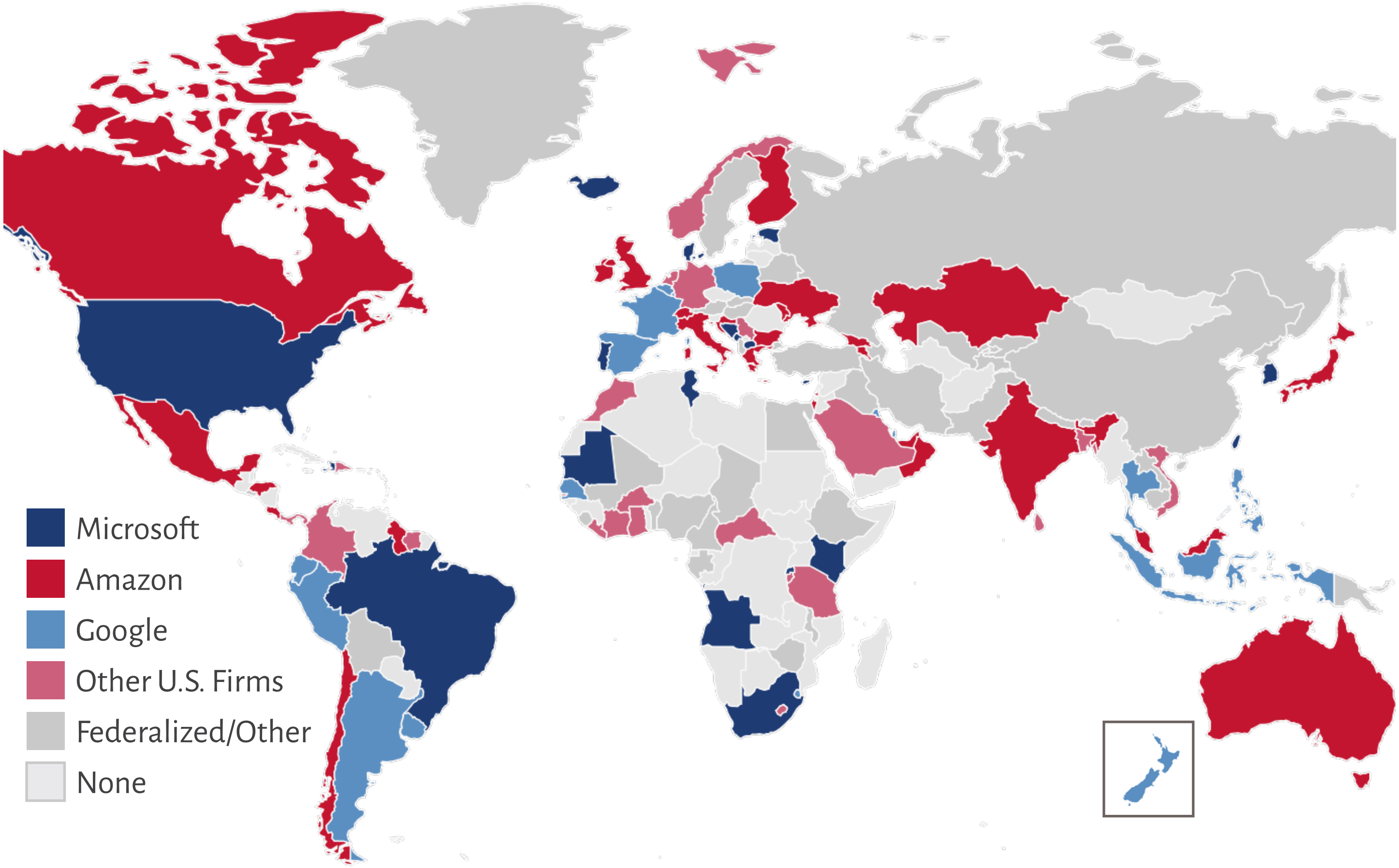


Strategic Advantages of Hyperscaler Dominance

In addition to providing the foundation for American AI leadership, hyperscaler dominance in the cloud computing industry has national security advantages. According to the U.S. Department of the Treasury, before moving to the commercial cloud, government data systems were at risk of “catastrophic failure” due to being ill-equipped, outdated, and far from federal buildings.[21] Outsourcing their computing, storage, and network capacity allows federal and defense agencies to focus on their primary missions while benefitting from the newest advancements in cloud-hosted AI and cybersecurity. Despite hyperscalers’ high capital spending and profits, these services remain more cost-effective for the public sector than new data infrastructure.

As cloud computing networks reach new markets, these advantages extend across the international system. Hyperscalers provide U.S. allies and partners cutting-edge processing power, AI tools, and data protection, strengthening global security and prosperity in peacetime[22] and defense system interoperability in wartime.[23] Cloud network expansion also improves U.S. intelligence and investigative capacity, as the 2018 CLOUD Act requires American CSPs to transfer data from across their global networks to the U.S. government for law enforcement and national security purposes.[24]

America’s Global Government Cloud Network Partnerships



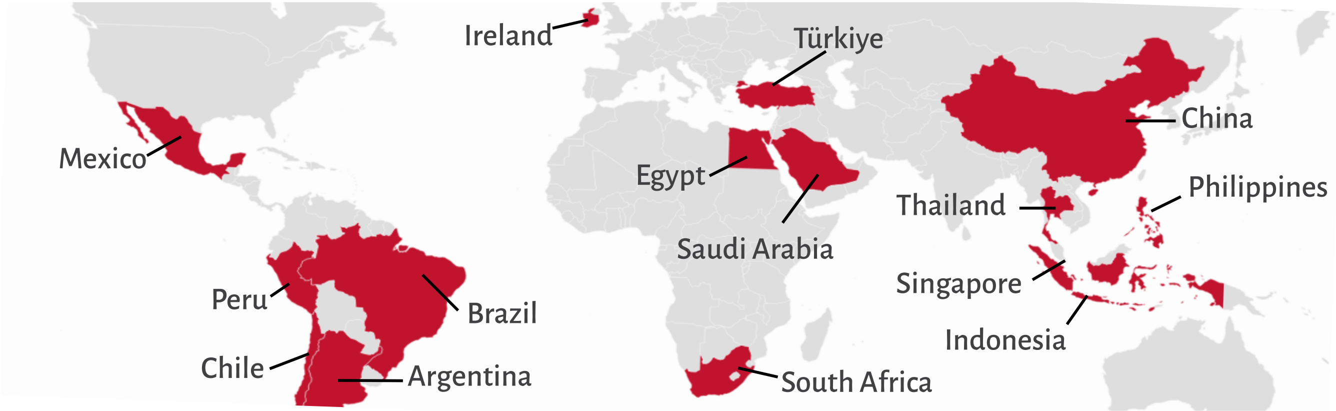
U.S. influence over global strategic cloud networks is demonstrated by how many governments around the world store their most sensitive data and information systems on major American cloud platforms.

China's Global Cloud Infrastructure Expansion

To gather sensitive intelligence and advance its AI ambitions, the CCP floods global markets with state-backed data infrastructure at artificially low prices and loan rates. Strategically undercutting U.S. firms in global technology markets allows the CCP to absorb mass volumes of foreign data and compute while creating lasting technological dependencies in the Global South and elsewhere.

Huawei's Subsidized 5G Leadership

Data sent "to the cloud" from wireless devices is first transmitted over radio networks to the nearest router or cell tower. 5G networks are faster and lower latency than previous generations of cellular infrastructure, enabling up to 100 times more capacity for cloud computing.[25] While South Korea and the U.S. were first to commercialize 5G, Chinese subsidies and loans soon propelled Huawei to the top of the global market.[26] Huawei has been repeatedly accused of stealing U.S. trade secrets,[27] aiding the ongoing genocide in Xinjiang,[28] and placing infrastructure near U.S. military bases that could disrupt nuclear communications.[29] Its greatest threat, however, is its large-scale theft of nearly all U.S. and allied data flowing through its cloud-linked infrastructure. The U.S. launched the Clean Network Project in 2020 to counter this threat, reducing Huawei's international partnerships from 91 to 13.[30] While its lead is narrowing, the firm still owns over 70 percent of global 5G base stations and serves 25 percent of global 5G users.[31]



Huawei's remaining global cloud partnerships as of July 2025.

Beijing's Rising Control over Undersea Data Cables

Nearly all military and intelligence communications between the United States and its NATO and Five Eyes partners—as well as the sensitive health, biometric, and financial data of all U.S. and allied citizens—flow through just 88 undersea data cables connecting the U.S. to the rest of the world.[32] While private firms in France and the United States own over 60% of this infrastructure,[33] heavy subsidies and diplomatic pressure have made CCP-aligned HMN Technologies the fastest-growing cable builder in the world.[34]

Chinese state-backed firms also dominate the Software-Defined Networking (SDN) technologies that control what data moves through which cables and landing stations at what speed.[35] This allows Beijing to redirect data from cables and landing stations it does not own into its own networks. In one case, all Google Cloud data in Nigeria was rerouted by China into Russia for over an hour.[36] In another, data exchanged locally between 368 million European IP addresses was rerouted into China for two full hours.[37]

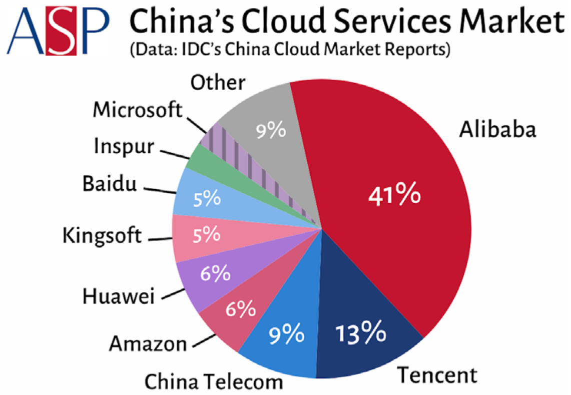
In addition to owning and surveilling foreign data cables, Beijing repeatedly sabotages them. Since 2023, Chinese vessels have been implicated in at least 11 undersea cable cuttings near Taiwan.[38] As Chinese firms operate the vast majority of cable repair ships in the Indo-Pacific, they are able to install surveillance equipment as cables are repaired.[39] In 2024, U.S. officials identified submarine cable wiretapping by ships belonging to Submarine Systems, a firm majority-owned by state-owned China Telecom.[40]

Huawei and Hyperscalers: The Cloud Cartel

Protectionist policies and predatory data laws create a one-way flow of American data and compute into China, facilitating Beijing's aggressive weaponization of artificial intelligence and placing America's AI development at risk. However, these risks have not stopped U.S. hyperscalers from cooperating with the CCP in order to gain access to lucrative Chinese markets.

China's Cloud Computing Barriers and Protectionism

Recognizing the inherent risks of linking its networks to the United States, the CCP allows only domestic firms to operate cloud infrastructure in China. Alibaba, Huawei, Tencent, and Baidu comprise 80% of China's cloud market, with 20% held by smaller firms and joint ventures.[41] This is soon to change, as Beijing's national cloud strategy—called Eastern Data Western Compute, or *Dongshu Xisuan*—aims to redistribute all privately-owned data infrastructure to state-owned firms within the next decade.[42]


China's Cloud Services Market
(Data: IDC's China Cloud Market Reports)

U.S. Hyperscalers' Compromises in China

Despite these restrictions, China's nearly $20 trillion market size incentivizes U.S. cloud companies to operate in China however they can.[43] To offer limited cloud services, CSPs must enter into a foreign-domestic joint venture that grants the Chinese firm one-sided advantages in data localization, security, and pricing. Sales of foreign AI models are completely banned, and foreign firms are required to store all local data within China and transfer foreign data to the Chinese Communist Party upon request.[44]

Two of three U.S. hyperscalers have taken this deal: Amazon Web Services accounts for 6 percent of the mainland Chinese cloud market through partnerships with Beijing Sinnet Technology Co. Ltd. and state-backed Ningxia Western Cloud Data Technology Co,[45] while Microsoft works with VNET Group to provide cloud services in Beijing, Hong Kong, and Shanghai.[46] VNET Group also manages data centers for Alibaba and other Chinese CSPs, imposing additional security vulnerabilities and conflicts of interest.

Google is the only hyperscaler to chart a different path. After failed attempts to launch cloud services in mainland China through partners Tencent and Inspur,[47] GCP announced "GCP region asia-east2," an assortment of regional cloud infrastructure for Hong Kong.[48] Google advertises to Chinese citizens that "services … not available within the Hong Kong region can still be utilized via the Google Network, and can be combined with other GCP services deployed around the world."[49] The CCP launched an antitrust probe into the company in February 2025;[50] if it decides that Google's activities violate Chinese law, it could impose a wide range of penalties, including banning sale of Google's products and services and granting free access to its Android operating system.[51]

Cloud Loopholes in U.S.-China Export Controls

In April 2024, after years of chronic compute shortages due to U.S. semiconductor chip export controls, Beijing lifted some foreign cloud ownership restrictions and allowed users in "special economic zones" to access restricted U.S. hardware and software through the cloud.[52] To gain access to these markets, foreign CSPs had to partner with one of three state-owned internet operators (China Mobile, Unicom, and Telecom) and were required to agree to strict CCP censorship, data transfer, and surveillance policies.[53]

American hyperscalers immediately began advertising cloud-supported access to restricted AI models and compute in China.[54] By August, *Reuters* published proof that at least eleven Chinese state-backed entities sought or acquired this access.[55] To close the loophole, Representative Michael Lawler introduced the Remote Access Security Act (H.R. 8152, 118) in September 2024.[56] Despite passing the House, however, the bill died in the Senate without a vote and was reintroduced in April 2025.[57] In the meantime, Chinese state and commercial actors continue to access restricted data and compute through American cloud networks.

Cyber Attacks and Social Engineering Campaigns

The CCP conducts millions of cyber-attacks on global data networks each day,[58] with cloud intrusions increasing 110% in 2024 alone.[59] To combat these threats, the U.S. Federal Bureau of Investigation opens a new Chinese cyber case every 12 hours.[60] However, Chinese hackers outnumber FBI cyber agents 50 to 1,[61] making it impossible to hold accountable the vast majority of perpetrators.

Advanced persistent threats (APT) affiliated with the Chinese Communist Party seek "zero-day vulnerabilities": novel weaknesses in cloud network architecture for which there is no known defense.[62] These vulnerabilities are sold on dark web marketplaces for upwards of $20 million,[63] including to CSPs and nation-state actors aiming to prevent penetrations.[64] In 2024, Chinese APTs gained access to U.S. government cloud networks through compromised accounts purchased from a dark web marketplace.[65]

However, the vast majority of cloud system breaches are not APT hacks. Over 90% are due to users selecting easy-to-guess passwords, reusing them on multiple websites, or erroneously providing them to scammers.[66] Manipulating users into granting access to systems or data is called "social engineering." While these attacks can target both wired and cloud systems, a hacker who gains access to a shared public cloud can access the data of all other actors on that network.[67] As shared public cloud services are far cheaper than sovereign cloud services, 95% of U.S. firms store data on a shared cloud.[68] Whether through social engineering or shared cloud access, 98% of organizations work with a CSP that has experienced a data breach in the last two years.[69]

The CyWatch cyber center is the FBI's first point of contact for CCP computer intrusions, ransomware attacks, and financial crimes. CC: U.S. FBI.

The U.S. Strategy to Deploy and Defend Cloud Infrastructure

With both Huawei and hyperscalers jeopardizing U.S. national security in exchange for global influence, policymakers must act quickly to defend America's data infrastructure. Diplomatic pressure and executive orders aim to convince governments and firms to decouple from China, but new interventions are urgently needed to close loopholes in the regulatory ecosystem.

Preventing China from Penetrating U.S. Cloud Systems

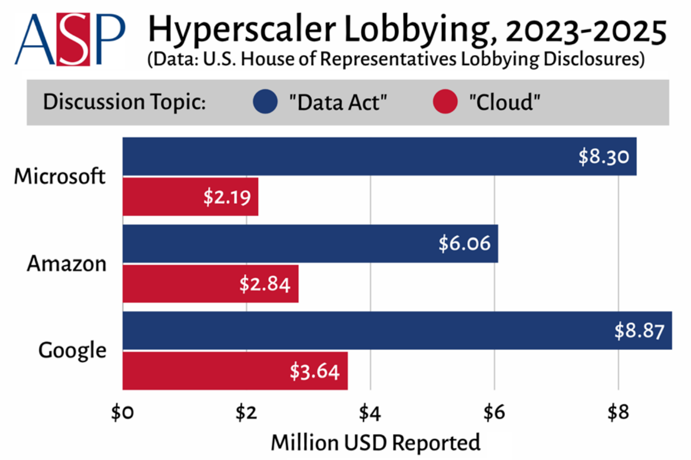
Ongoing penetration of federal cloud networks poses an urgent threat to U.S. national security by granting the CCP access to sensitive military and political intelligence that it uses to develop new AI weapons, disinformation campaigns, and surveillance tools. In 2021, EO 14028 strengthened information-sharing policies for cloud security breaches and directed federal agencies to adopt Zero Trust Architecture standards designed by the National Institute of Standards and Technology.[70] Additional FedRAMP cybersecurity standards were congressionally mandated in 2022;[71] however, their enforcement remains inconsistent at best.[72]

Commercial and personal cloud networks are also in dire need of protection. Extensive and interconnected U.S. and Chinese networks make Microsoft-hosted government cloud systems particularly vulnerable to breaches from commercial entry points.[73] However, even when not connected to federal information systems, commercial and personal clouds are valuable CCP targets in their own right. The Federal Trade Commission began requiring public companies to disclose cloud intrusions in 2023,[74] but preventing these attacks is critical to stop the CCP from leveraging U.S. industry intelligence and bulk U.S. data for AI development.

Preventing U.S. Cloud Providers from Transferring Sensitive Data to China

In addition to defending cloud networks from attack, it is vital to prevent U.S. firms from willingly transferring cloud-hosted data and compute to Beijing. In 2024, Congress passed the Protecting Americans' Data from Foreign Adversaries Act (PADFA), which bars third-party data brokers from transferring sensitive U.S. data to a foreign adversary or adversary-controlled enterprise.[75] However, PADFA targets only data brokers that do not provide services, leaving CSP-facilitated data transfers in a grey zone.

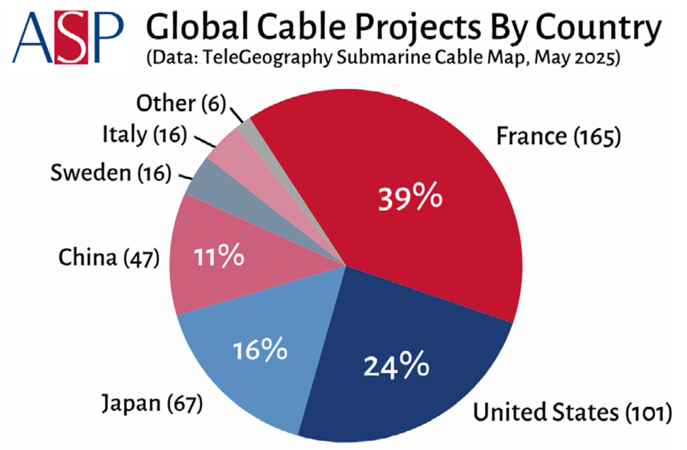
In January 2025, the U.S. Department of Justice prohibited sales of bulk U.S. sensitive and government data to countries of concern, including China.[76] However, CSPs were exempted from key requirements under the rule, CCP-mandated data transfers were not addressed, and sales of most types of data—including AI training data—were not prohibited. While Microsoft insists that it does not transfer data to the CCP,[77] its users regularly report their data crossing into China without consent,[78] demonstrating the importance of including CSPs in data transfer rulings and regulations.

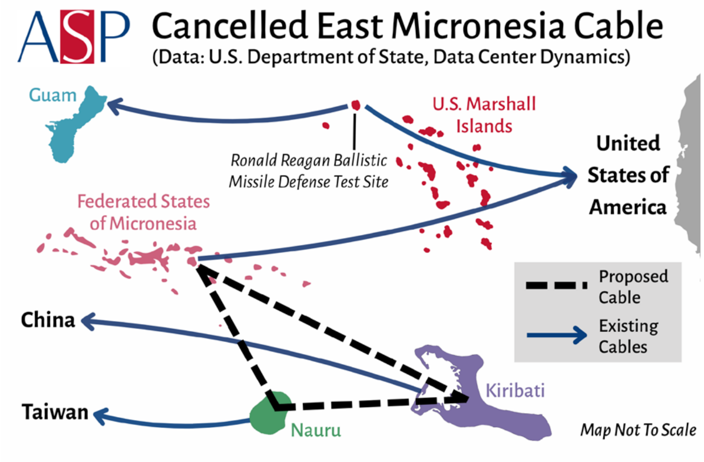

Hyperscaler Lobbying, 2023-2025
(Data: U.S. House of Representatives Lobbying Disclosures)

Disconnecting American and Allied Cloud Infrastructure from China

The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) advises the Federal Communications Commission on approvals for new data infrastructure projects that connect to U.S. cloud networks.[79] Since 2019, the group has shut down nearly all proposed deals that would allow China to access or intercept U.S. undersea data cables. Commerce Department sanctions, like those on Chinese-owned Huawei and HMN International,[80] restrict transactions between Chinese and U.S. firms to protect U.S. cloud infrastructure from Chinese surveillance and control.

However, the broad internationalization and interconnection of global cloud architecture renders domestic-only approaches ineffective. Sustained diplomacy is vital to prevent intermediary nations from linking U.S. and Chinese-owned data networks, which could grant Beijing access to all other nodes. These efforts have already averted potential disaster; in 2021, a Huawei cable project connecting China to several U.S.-linked Pacific Islands was scrapped after diplomats pressed the risks of working with both the U.S. and China.[81] The project would have connected U.S.-sanctioned Huawei to the Ronald Reagan Ballistic Missile Defense Test Site, introducing a critical failure in U.S. operational security.


Global Cable Projects By Country
(Data: TeleGeography Submarine Cable Map, May 2025)


Cancelled East Micronesia Cable
(Data: U.S. Department of State, Data Center Dynamics)

Policy Recommendations

On July 23, 2025, the Trump Administration introduced the AI Action Plan: a roadmap for securing America's AI future. Deploying and defending cloud infrastructure is vital to ensure that this roadmap becomes a racetrack. The following recommendations aim to strengthen U.S. cloud expansion while preventing U.S. companies from enabling China's predatory practices.

To Defend and Deploy America's AI Cloud Infrastructure:

Prevent American Hyperscalers from Transferring U.S. Data and Compute to China. Washington must pass a federal statute prohibiting the transfer of American data and restricted technologies to U.S. adversaries, including through the cloud. If firms decide—or are forced—to transfer restricted U.S. data and compute to China, they should be required to report these transfers to affected users and the U.S. government. A liability regime for unauthorized disclosures can impose penalties for infractions.

Promote a Multi-Cloud Federal Ecosystem. For security reasons, it is vital to ensure that no one company has exclusive control over America's federal and military data networks. Bills like the Multi-Cloud Innovation and Advancement Act of 2023 should be reintroduced to limit the individual power of any CSP and ensure that the United States government is able to fairly procure competitively priced cloud services from across the commercial marketplace.

Strengthen Extraterritorial Prosecution of Cloud Intruders. While the Chinese government has no problem holding foreigners liable for cybercrimes committed abroad, America's failure to prosecute malicious cyber predators empowers the CCP to continually target U.S. cloud infrastructure. Prosecution can be enforced multinationally through the United Nations Convention Against Transnational Organized Crime, bilaterally through Mutual Legal Assistance Treaties, and domestically through laws like the Maritime Drug Law Enforcement Act and Racketeer Influenced and Corrupt Organizations Act.

Treat U.S. Cloud Infrastructure as Critical Infrastructure. In addition to supplying the foundation for global AI leadership, cloud networks provide the backbone of global trade, communication, and military cooperation between the U.S. and its allies. Washington currently entrusts oversight and defense of these networks to the private sector, creating risks as most U.S. cloud providers either work in China or are unable to defend against sophisticated Chinese attacks. To begin reducing the hundreds of millions of cyberattacks on cloud networks daily, the United States must treat cloud infrastructure as critical infrastructure and afford it the same oversight and protection mechanisms as America's energy, healthcare, and transportation networks.

Improve Security of U.S. Cloud Networks Abroad. The U.S. Navy's Integrated Undersea Surveillance System defends select U.S. military cables through a sophisticated early warning system and submarine surveillance. However, no similar protections are afforded to the commercial cloud infrastructure that transmits and stores all sensitive and bulk U.S. data, allowing China to rapidly meet its espionage and AI development objectives. While Team Telecom is an important stopgap measure, unclear regulations governing which global cloud infrastructure projects put U.S. national security at risk frequently lead to last-minute delays and cancellations of undersea data cable projects—costing U.S. cloud computing firms tens of millions of dollars annually. The Government Accountability Office's recommendations for securing global cloud networks must be rapidly adopted to prevent continuing Chinese predation of these vital supply lines.

About the Author

Courtney Manning is the Director of AI Imperative 2030 at the American Security Project, where she leads a team of cross-disciplinary stakeholders investigating the critical geostrategic forces driving the global AI race in the 21st century. Formerly, she led ASP's research portfolios on military recruitment and readiness, strategic competition with China, and emerging technology risks. Before ASP, she worked as a geopolitical risk consultant for the Peruvian government and a special advisor for the Permanent Mission of Afghanistan to the United Nations. Courtney holds an MIA in international security policy and conflict resolution from Columbia University and a BA in international relations from the University of Denver Korbel School.

Endnotes

[1] Wilhelmina Afua Addy et al., "Algorithmic Trading and AI: A Review of Strategies and Market Impact," *World Journal of Advanced Engineering Technology and Sciences* 11, no. 1 (February 28, 2024): 258–67. https://doi.org/10.30574/wjaets.2024.11.1.0054

[2] Felix Richter, "Amazon and Microsoft Stay Ahead in Global Cloud Market," *Statista*, February 27, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

[3] "Machine Learning Trends," *EpochAI*, January 13, 2025, https://epoch.ai/trends

[4] "Artificial Intelligence Index Report 2025," Human-Centered Artificial Intelligence, *Stanford University*, April 18, 2025, https://hai-production.s3.amazonaws.com/files/hai_ai_index_report_2025.pdf

[5] OECD, "A Blueprint for Building National Compute Capacity for Artificial Intelligence," *OECD Digital Economy Papers*, vol. 350, February 28, 2023, https://doi.org/10.1787/876367e3-en

[6] Konstantin Pilz, Yusuf Mahmood, and Lennart Heim, "AI's Power Requirements Under Exponential Growth," *RAND*, January 28, 2025, https://www.rand.org/pubs/research_reports/RRA3572-1.html

[7] Jason Lopez, "AI, Cloud Native and Hybrid Cloud Fuse to Run Apps and Data Anywhere," *The Forecast*, August 1, 2024, https://www.nutanix.com/theforecastbynutanix/podcasts/ai-cloud-native-and-hybrid-cloud-work-together

[8] "What Is Cloud Computing?" *Microsoft*, accessed May 2025, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing

[9] "Cloud revenues poised to reach $2 trillion by 2030 amid AI rollout," *Goldman Sachs*, September 4, 2024, https://www.goldmansachs.com/insights/articles/cloud-revenues-poised-to-reach-2-trillion-by-2030-amid-ai-rollout

[10] "Cloud Market Jumped to $330 billion in 2024," *Synergy Research Group*, February 6, 2025, https://www.srgresearch.com/articles/cloud-market-jumped-to-330-billion-in-2024-genai-is-now-driving-half-of-the-growth

[11] "State of the Network 2025 Edition," *TeleGeography*, April 2025, https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2025.pdf

[12] "Hyperscale Operators and Colocation Continue to Drive Huge Changes in Data Center Capacity Trends," *Synergy Research Group*, August 7, 2024, https://www.srgresearch.com/articles/hyperscale-operators-and-colocation-continue-to-drive-huge-changes-in-data-center-capacity-trends

[13] "State of the Network 2025 Edition," *TeleGeography*.

[14] Michael Brenner, "How AI and Cloud Computing Together Drive Change," *The Forecast*, September 10, 2024, https://www.nutanix.com/theforecastbynutanix/technology/ai-in-the-cloud

[15] Georgia Butler, "Google Cloud Q3 2024 revenue hits $11.4bn, data center spend set to increase in 2025," *Data Center Dynamics*, October 30, 2024, https://www.datacenterdynamics.com/en/news/google-cloud-q3-2024-revenue-hits-114bn-data-center-spend-set-to-increase-in-2025/

[16] Jordan Novet, "Amazon's cloud unit records highest profit margin in at least a decade," *CNBC*, https://www.cnbc.com/2024/10/31/amazons-cloud-unit-records-highest-profit-margin-in-at-least-a-decade.html

[17] "Earnings Release FY24 Q1," Investor Relations, *Microsoft*, https://www.microsoft.com/en-us/investor/earnings/fy-2024-q1/performance

[18] “Form 10-K: Annual Report,” SEC Filings, *Amazon*, https://ir.aboutamazon.com/sec-filings/sec-filings-details/default.aspx?FilingId=18165478, p. 68; Aditya Soni, Yuvraj Malik and Anna Tong, “Microsoft’s slow cloud growth signals AI payoff will take longer,” *Reuters*, July 31, 2024, https://www.reuters.com/technology/microsoft-beats-quarterly-revenue-estimates-2024-07-30

[19] “Google Cloud breaks records – CapEx climbs to $13 billion,” *The Stack*, July 24, 2024, https://www.thestack.technology/google-cloud-breaks-records-capex-climbs-to-13-billion/

[20] “Data Center Capex Surged 51 Percent to $455 Billion in 2024, According to Dell’Oro Group,” *Dell’Oro Group*, March 19, 2025, https://www.delloro.com/news/data-center-capex-surged-51-percent-to-455-billion-in-2024/

[21] “The Financial Services Sector’s Adoption of Cloud Services,” *U.S. Department of the Treasury*, February 8, 2023, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf, page 66.

[22] “Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act,” *U.S. Department of Justice*, April 2019, https://www.justice.gov/d9/press-releases/attachments/2019/04/10/department_of_justice_cloud_act_white_paper_2019_04_10_final_0.pdf

[23] “Le Marché Ukrainien des Services Cloud pendant la Guerre,” *OptimNow*, October 22, 2023, https://www.optimnow.io/post/ukrainian-cloud-services-market-during-the-war-2

[24] Kenneth Propp, Peter Swire, Josh Fox, “Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services,” *European Law Blog*, July 11, 2023, https://www.crossborderdataforum.org/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services/

[25] Joe O’Halloran, “Cloud-based networks to account for half of all cellular traffic by 2028,” *Computer Weekly*, August 6, 2024, https://www.computerweekly.com/news/366600077/Cloud-based-networks-to-account-for-half-of-all-cellular-traffic-by-2028

[26] Steven Levy, “Huawei, 5G, and the Man Who Conquered Noise,” *Wired*, November 16, 2020, https://www.wired.com/story/huawei-5g-polar-codes-data-breakthrough/

[27] Chuin-Wei Yap et al., “Huawei’s Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics,” *Wall Street Journal*, May 25, 2019, https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858; Laurel Wamsley, “A Robot Named ‘Tappy’: Huawei Conspired To Steal T-Mobile’s Trade Secrets, Says DOJ,” *NPR*, January 29, 2019, https://www.npr.org/2019/01/29/689663720/a-robot-named-tappy-huawei-conspired-to-steal-t-mobile-s-trade-secrets-says-doj

[28] Rew Harwell and Eva Dou, “Huawei tested AI software that could recognize Uighur minorities and alert police, report says,” *The Washington Post*, December 8, 2020, https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/

[29] Katie Bo Lillis, “CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications,” *CNN*, July 25, 2022, https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html

[30] Sean Keane, “Huawei ban timeline: Detained CFO makes deal with US Justice Department,” *CNET*, September 30, 2021, https://www.cnet.com/news/privacy/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department/

[31] Hosuk Lee-Makiyama, “US Sanctions Against Chinese 5G: Inconsistencies and Paradoxical Outcomes,” *ECIPE*, October 2021, https://ecipe.org/blog/us-sanctions-against-chinese-5g/; Dan Jones, “RAN sales grow in U.S., Decline Globally, Dell’Oro says,” *Fierce Network*, June 2, 2025, https://www.fierce-network.com/broadband/delloro-declares-ran-world-2-halves-q1-2025

[32] Madison Long, “Information Warfare in the Depths,” *U.S. Naval Institute*, May 2023, https://www.usni.org/magazines/proceedings/2023/may/information-warfare-depths-analysis-global-undersea-cable-networks

[33] “Submarine Cable Map,” *TeleGeography*, accessed May 2025, https://www.submarinecablemap.com/

[34] Joe Brock, “U.S. and China wage war beneath the waves – over internet cables,” *Reuters*, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/

[35] Carlo Caro, “Underwater Geopolitics,” *Real Clear Defense*, November 26, 2024, https://www.realcleardefense.com/articles/2024/11/26/underwater_geopolitics_1074698.html

[36] Aftab Siddiqui, “Route Leak Causes Major Google Outage,” *Internet Society*, November 15, 2018, https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/

[37] Anthony Cuthbertson, “European mobile traffic mysteriously routed through China for two hours,” *Independent*, June 11, 2019, https://www.the-independent.com/tech/china-europe-mobile-traffic-telecom-mobile-data-hackers-a8953786.html

[38] Erin Hale, “As undersea cables break off Europe and Taiwan, proving sabotage is tough,” *Al Jazeera*, March 10, 2025, https://www.aljazeera.com/news/2025/3/10/as-undersea-cables-break-down-proving-sabotage-a-difficult-task

39 Caro, “Underwater Geopolitics.”

40 Dustin Volz et al., “U.S. Fears Undersea Cables Are Vulnerable to Espionage From Chinese Repair Ships,” *Wall Street Journal*, May 19, 2024, https://www.wsj.com/politics/national-security/china-internet-cables-repair-ships-93fd6320

41 Julia Yang, “A Deep Dive Into China’s Cloud Providers,” *GLUCN*, April 6, 2024, https://glucn.com/posts/2024-04-07-cloud-providers-in-china

42 Anrew Stokols, “China is trying to create a national network of cloud computing centers,” *Sinocities*, March 21, 2025, https://sinocities.substack.com/p/china-is-trying-to-create-a-national

43 Aaron O’Neill, “The 20 countries with the largest gross domestic product (GDP) in 2025,” *Statista*, May 28, 2025, https://www.statista.com/statistics/268173/countries-with-the-largest-gross-domestic-product-gdp/

44 “Translation: Data Security Law of the People’s Republic of China,” *DigiChina*, June 29, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

45 Matthew Murphy and Fei Dang, “Cloud Computing in China,” *Lexology*, March 21, 2019, https://www.lexology.com/library/detail.aspx?g=998fe1a0-6634-41e7-a670-19ca406709e5; “Amazon Cloud Infrastructure Map,” *TeleGeography*, accessed May 2025, https://www.cloudinfrastructuremap.com/#/cloud-service-provider/amazon-web-services

46 “Microsoft Cloud Infrastructure Map,” *TeleGeography*, accessed May 2025, https://www.cloudinfrastructuremap.com/#/cloud-service-provider/microsoft-azure

47 “Google Is in China Cloud Talks With Tencent, Others,” *Bloomberg News*, August 3, 2018, https://www.bloomberg.com/news/articles/2018-08-03/google-is-said-to-be-in-china-cloud-talks-with-tencent-others

48 “Cloud Locations,” *Google*, accessed July 2025, https://cloud.google.com/about/locations#lightbox-regions-map; “Google Cloud Region asia-east2 Hong Kong,” *Google*, accessed July 2025, https://gcloud-compute.com/asia-east2.html

49 Kirill Tropin, “Growing our presence in Asia Pacific: New GCP regions in Hong Kong and Jakarta,” *Google Cloud Blog*, November 28, 2018, https://cloud.google.com/blog/products/gcp/gcps-region-in-hong-kong-is-now-open; “Google Cloud Summit Hong Kong 2025,” *Google Cloud*, accessed June 2025, https://cloudonair.withgoogle.com/events/summit-hongkong-2025

50 Zen Soo, “China launches an antitrust probe into Google. Here’s what it means,” *Associated Press*, February 4, 2025, https://apnews.com/article/google-china-antitrust-investigation-tariffs-ab02b906733666cb0d348d2b416b7fa5

51 “China announces measures against Google, other US firms, as trade tensions escalate,” *Reuters*, February 4, 2025, https://www.reuters.com/technology/china-anti-monopoly-regulator-launches-probe-into-google-2025-02-04/

52 “China removes foreign ownership restrictions on more value-added telecom services,” *Geopolitechs*, April 10, 2024, https://www.geopolitechs.org/p/china-removes-foreign-ownership-restrictions

53 Yan Luo, “China Issues New Measures on Cybersecurity Review of Network Products and Services,” Inside Privacy, *Covington*, April 27, 2020, https://www.insideprivacy.com/international/china/china-issues-new-measures-on-cybersecurity-review-of-network-products-and-services/

54 Eduardo Baptista, Fanny Potkin, and Karen Freifeld, “Exclusive: Chinese entities turn to Amazon cloud and its rivals to access high-end US chips, AI,” *Reuters*, August 23, 2024, https://www.reuters.com/technology/chinese-entities-turn-amazon-cloud-its-rivals-access-high-end-us-chips-ai-2024-08-23/

55 Ibid.

56 “H.R.8152 - 118th Congress (2023-2024): Remote Access Security Act,” *Congress.gov*, September 10, 2024, https://www.congress.gov/bill/118th-congress/house-bill/8152

57 “H.R.2683 - 119th Congress (2025-2026): Remote Access Security Act,” *Congress.gov*, April 9, 2025, https://www.congress.gov/bill/119th-congress/house-bill/2683

58 “Microsoft Digital Defense Report 2024,” Microsoft Threat Intelligence, *Microsoft*, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf, page 23.

59 “2024 CrowdStrike Global Threat Report: Cloud Infrastructure Under Attack,” *CrowdStrike*, February 21, 2024, https://www.crowdstrike.com/en-us/press-releases/2024-crowdstrike-global-threat-report-release/

60 Evan Perez, “FBI Director Wray, MI5 chief raise alarm over China spying,” *CNN*, July 6, 2022, https://www.cnn.com/2022/07/06/politics/fbi-mi5-wray-china/index.html

61 Kwan Wei Kevin Tan, “Chinese hackers would outnumber FBI cyber agents by 50 to 1 even if the agency threw all its resources at China: FBI chief,” *Business Insider*, January 31, 2024, https://www.businessinsider.com/china-hackers-outnumber-fbi-cyber-agents-50-to-1-2024-2

62 Patrick Howell O'Neill, "How China built a one-of-a-kind cyber-espionage behemoth to last," *MIT Technology Review*, February 28, 2022, https://www.technologyreview.com/2022/02/28/1046575/how-china-built-a-one-of-a-kind-cyber-espionage-behemoth-to-last/

63 Niamh Ancell, "The Zero-Day Market Explained," *CyberNews*, May 13, 2024, https://cybernews.com/editorial/zero-day-market-explained/

64 Patrick Howell O'Neill, "2021 has broken the record for zero-day hacking attacks," *MIT Technology Review*, September 23, 2021, https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/

65 "Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization," *CISA*, February 15, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-046a; "Treasury Sanctions China-based Hacker Involved in the Compromise of Sensitive U.S. Victim Networks," *U.S. Department of the Treasury*, March 2025, https://home.treasury.gov/news/press-releases/sb0042

66 "Microsoft Digital Defense Report 2024," *Microsoft*.

67 "UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion," *Google Cloud Blog*, June 10, 2024, https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion/

68 "2024 Cloud and AI Business Survey," *PwC*, accessed June 2025, https://www.pwc.com/us/en/tech-effect/cloud/cloud-ai-business-survey.html

69 "SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party," *SecurityScorecard*, February 1, 2023, https://securityscorecard.com/company/press/securityscorecard-research-shows-98-of-organizations-globally-have-relationships-with-at-least-one-breached-third-party/

70 "Executive Order 14028: Improving the Nation's Cybersecurity," *Executive Office of the President*, May 17, 2021, https://www.federalregister.gov/d/2021-10460/p-5

71 "H.R.8956 - 117th Congress (2021-2022): FedRAMP Authorization Act," *Congress.gov*, October 11, 2022, https://www.congress.gov/bill/117th-congress/house-bill/8956

72 "Cloud Security: Federal Authorization Program Usage Increasing, but Challenges Need to Be Fully Addressed," *U.S. Government Accountability Office*, January 18, 2024, https://www.gao.gov/products/gao-24-106591

73 Elias Groll, "Microsoft downplays damaging report on Chinese hacking its own engineers vetted," *CyberScoop*, July 31, 2023, https://cyberscoop.com/microsoft-china-breach-encryption-key/

74 "88 FR 51896 - Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," *Securities and Exchange Commission*, August 4, 2023, https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

75 "H.R.7520 - 118th Congress (2023-2024): Protecting Americans' Data from Foreign Adversaries Act of 2024," Congress.gov, March 21, 2024, https://www.congress.gov/bill/118th-congress/house-bill/7520/text

76 "90 FR 1636 - Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," *U.S. Department of Justice*, https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern

77 Karen Weise, "Lawmakers Question Microsoft's President About Its Presence in China," *The New York Times*, June 13, 2024, https://www.nytimes.com/2024/06/13/technology/microsoft-hearing-security.html

78 u/TheMicrosoftMan, "Microsoft DNS Queries Going to China," r/nextdns, *Reddit.com*, https://www.reddit.com/r/nextdns/comments/1d22hkn/microsoft_dns_queries_going_to_china/

79 "Executive Order 13913: Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," *Federal Register* 85, no. 19643 (April 4, 2022): https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states

80 Alexandra Alper and Daphne Psaledakis, "U.S. curbs Chinese drone maker DJI, other firms it accuses of aiding rights abuses," *Reuters*, December 17, 2021, https://www.reuters.com/markets/us/us-adds-more-chinese-firms-restricted-entity-list-commerce-2021-12-16/

81 Sebastian Moss, "East Micronesia subsea cable scrapped as US says Chinese firms pose threat," *Data Center Dynamics*, June 18, 2021, https://www.datacenterdynamics.com/en/news/east-micronesia-subsea-cable-scrapped-as-us-says-chinese-firms-pose-threat/