OCTOBER 2025

Countering the Digital Silk Road

Vivek Chilukuri and Ruby Scanlon

CNAS

About the Authors

Vivek Chilukuri is the senior fellow and director of the Technology and National Security Program at the Center for a New American Security (CNAS). His work focuses on the responsible development and deployment of artificial intelligence; the U.S.-China technology competition; and the intersection of technology, democracy, and geopolitics. Before joining CNAS, Chilukuri served as a senior technology policy advisor, deputy chief of staff, and legislative director for Senator Michael Bennet (D-CO)—a member of the Senate Select Committee on Intelligence. Previously, Chilukuri served at the Department of State as a policy advisor to the undersecretary for civilian security, democracy, and human rights, and as a program officer at the National Democratic Institute. He received a master's in public policy from the Harvard Kennedy School and a bachelor of arts in international studies from the University of North Carolina at Chapel Hill, where he graduated as a Robertson Scholar.

Ruby Scanlon is a research associate for the Technology and National Security Program at CNAS, supporting the Center's research on U.S.-China technology competition, China's innovation ecosystem, and artificial intelligence (AI) policy. Before CNAS, Scanlon worked at the Department of Justice's Antitrust Division, where she assisted on technology cases such as United States v. Google and served as speechwriter for Assistant Attorney General Jonathan Kanter. Scanlon holds an MS in global affairs from Tsinghua University in Beijing, where she wrote her thesis on China's National AI Development and Regulation Strategy, and a BA from Northwestern University in international relations with a focus in international economics.

About the Technology and National Security Program

The CNAS Technology and National Security Program produces cutting-edge policy research to secure America's edge in emerging technologies while managing potential risks to security and democratic values. The Program produces bold, actionable recommendations to drive U.S. and allied leadership in responsible technology innovation, adoption, and governance.

The Technology and National Security Program focuses on three high-impact technology areas: AI, biotechnology, and quantum information sciences. It also conducts cross-cutting research to strengthen U.S. technology partnerships to promote secure, resilient, and rights respecting digital infrastructure and ecosystems abroad. A focus of the program is convening the technology and policy communities to bridge gaps and develop solutions.

Acknowledgments

This report would not have been possible without the many officials and experts—across Washington, D.C., Jakarta, São Paulo, Brasília, Nairobi, Riyadh, and Abu Dhabi—who shared their insights over the course of the project. The authors also wish to thank Melanie Hart, Jonathan Hillman, Erin Murphy, and Kyle Chan for their feedback on earlier drafts.

The report benefited from the excellent substantive, editorial, and design contributions of CNAS current and former colleagues Bill Drexel, Janet Egan, Tim Fist, Maura McCarthy, Melody Cook, Emma Swislow, and Caroline Steel. This work was made possible by the generous support of the Smith Richardson Foundation.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues, and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

Project Overview

The year 2025 marks the 10th anniversary of the Digital Silk Road (DSR), China's ambitious initiative to shape critical digital infrastructure around the world to advance its geopolitical interests and technology leadership. A decade after the initiative's launch, digital infrastructure and emerging technologies have only grown more vital and contested as demand for connectivity, digital services, and advanced technologies like artificial intelligence (AI) expands. Against this backdrop, the DSR has become increasingly central to China's broader strategy to challenge and ultimately supplant the U.S.-led digital order, and in doing so, reap potentially vast security, economic, and intelligence advantages.

To assess the DSR's impact a decade after its inception—and to examine how the United States and its allies can offer a more compelling and coherent alternative—the CNAS Technology and National Security team undertook a major research project that combined extensive desk research and field interviews in emerging markets to produce in-depth case studies of four geostrategically critical nations: Indonesia, Brazil, Kenya, and Saudi Arabia. This final report brings together insights from these case studies, while offering a comprehensive analysis of the origins, evolution, and effectiveness of China's Digital Silk Road and its implications for the United States and its allies. The report also provides an in-depth examination of U.S. and allied efforts to counter the DSR and offers detailed recommendations to strengthen those efforts going forward.

TABLE OF CONTENTS

Executive Summary

The year 2025 marks the 10th anniversary of the Digital Silk Road (DSR), China's effort to strengthen its global ties and influence through technology. In the decade since the initiative's launch, technology has moved to the center of emerging market priorities, China's domestic and foreign policy, and the U.S.-China competition. Rapid digitalization, spurred by emerging market policies seeking to harness technology's potential, has led to surging global demand for the connective infrastructure and cutting-edge services that will power the modern world. But even as technology vaults to the top of government and corporate agendas, the DSR's origins, goals, and tools remain obscured, complicating U.S. and allied efforts to assess its effectiveness and mobilize a response.

Those seeking official strategies and plans behind the DSR will be disappointed. Its nature is amorphous, expanding alongside Beijing's growing interest in strategic technologies and receding as commercial and political interests require. Ten years after its inception, the Digital Silk Road is, paradoxically, at once less visible and more ubiquitous than ever. Launched in 2015 as the digital arm of China's Belt and Road Initiative (BRI), the DSR grew into its own effort as technology leadership became increasingly important to Beijing. Rising backlash against the BRI and the DSR abroad, however, made formal affiliation with a state-led initiative a liability, and Chinese officials and companies now rarely tout official linkages. Domestic economic headwinds and fiscal pressures also caused Beijing to retrench from the earlier years of massive state-backed infrastructure projects in favor of a "small yet smart" approach that emphasized technology as a low-cost, high-impact avenue of continued developmental support.[1] At home, Beijing embraced technology as a path to economic diversification, development, and security consistent with the Made in China 2025 initiative. Private and semiprivate companies—Huawei, ZTE, Alibaba, and Tencent—led the way, with considerable success. Huawei is now the world's top provider of telecommunications equipment and operates in over 170 countries.

Beijing's public retreat from the DSR should not be mistaken for failure. On the contrary, the DSR's ambition—to strengthen China's economic and geopolitical leadership through technology—has now suffused Beijing's broader domestic and foreign policy. The DSR has largely disappeared because it has succeeded and become subsumed. The DSR may not be state directed, like the BRI, but it is undoubtedly state *enabled*. At every

stage, government support drives the innovation, deployment, and scale needed within China to underprice and outcompete in the wider world—in 5G telecommunications equipment, facial recognition cameras, legacy semiconductors, and, more recently, commercial drones and electric vehicles.

Over the past decade, U.S. and allied policymakers have slowly awoken to the varied, overlapping dangers of the DSR. Concern has focused on how the diffusion of Chinese-linked digital infrastructure could create cybersecurity and espionage risks and avenues of coercive influence for Beijing over emerging markets, akin to the dynamics of the BRI. Others have focused on the spread of techno-authoritarianism. All these concerns are valid and troubling. At the same time, it is neither realistic nor desirable to arrest, let alone reverse, the diffusion of all Chinese-linked digital infrastructure and services everywhere. China remains the top trading partner for most of the world, and technology represents an increasing share of that trade. Not all Chinese-linked technology diffusion is inherently nefarious; indeed, much of it involves innocuous consumer goods that pose little or no risk. Hysteria about Chinese technology diffusion is not a strategy. U.S. and allied policymakers must therefore prioritize the key countries and technology domains that both implicate core economic and security interests and represent credible opportunities to outcompete Chinese offerings.

With this in mind, the report suggests six priority technology domains: subsea cables, next-generation telecommunications, low Earth orbit (LEO) satellites, data centers and cloud services, artificial intelligence (AI), and smart cities. Together, these domains form the foundation of the digital infrastructure and services that will power the economies and governments of the modern world. The United States and its allies must not allow China to dominate these domains in key emerging market security partners, such as the Philippines, Indonesia, Kenya, and Egypt, recognizing that any strategy that seeks to stop Chinese technology everywhere—even in these countries—is doomed to fail.

The case for countering the DSR is as much about seizing opportunity as mitigating risks. Unlike the global transition to 4G and 5G networks, when the West lacked competitors that could match Huawei and ZTE's state-subsidized offerings, the United States and its allies have a formidable hand to play in several vital technology transitions now unfolding across the globe. U.S. firms dominate the AI frontier, dwarfing competitors in capital investments and model capabilities. U.S. firms command 70 percent of the global cloud market. Over 90 percent of the global subsea cable infrastructure was built by U.S. or allied companies. Since 2020, Starlink has launched more LEO satellites than all its competitors combined. Washington and its allies now have a generational opportunity to wield these strengths to positively shape digital ecosystems around the world, secure first-mover advantages, and box out Chinese companies' ability to reinvest overseas revenue to close gaps in strategic technologies.

But doing so will require a bold new approach. Over the past decade, the United States and its allies have haltingly rolled out new offices, initiatives, and funding mechanisms to match the DSR. The G7 touts a new Partnership for Global Infrastructure and Investment (PGI) to deploy $600 billion; the United States has mobilized just one-tenth of that amount to date. The Quad's ambition to support subsea cables, cybersecurity, and other digital infrastructure across the Indo-Pacific is well directed but similarly under-resourced. The European Union's Global Gateway committed $350 billion for global infrastructure, but meaningful coordination with U.S. investments and the PGI remains sparse.

The U.S. government has mounted several reforms to level up America's technology statecraft. The State Department established the new Bureau of Cyberspace and Digital Policy. Congress created new investment tools through the International Development Finance Corporation, International Technology Security and Innovation Fund, and Countering PRC Influence Fund. Administrations of both parties have pursued efforts to promote a standards-based model for secure and trusted technology promotion abroad, such as the Clean Network initiative from President Donald Trump's first administration and the now-rescinded Framework for AI Diffusion from President Joe Biden's administration. At the same time, U.S. allies like the EU, Japan, and Australia have embraced a more security-minded approach to foreign assistance and strengthened coordination. These efforts are welcome, overdue, and wholly insufficient.

In the short term, as the Trump administration considers a new iteration of the AI Diffusion Rule, it should raise its sights and offer the world not only a framework for accessing cutting-edge AI chips, but advanced technologies more broadly to draw them into the U.S. technology ecosystem. The administration should also recognize that it cannot ask emerging markets to limit Beijing's leverage through the DSR as the United States exploits its own economic leverage through rapidly shifting tariff and export control policies. Long-term technology partnerships require a foundation of trust that recent policies risk undermining.

In the longer term, the United States must recognize that the lesson of the 5G race is that market forces alone cannot guarantee U.S. and allied tech adoption—especially as China doubles down on support for strategic technologies. The answer, however, is not to mirror Beijing's government-driven approach, but to pursue more ambitious statecraft fit for an era of global technology competition.

To that end, the report offers the following recommendations:

Strategy and Coordination

Craft a Global Technology Competition Strategy. The White House should direct the State Department, led by the undersecretary for economic growth, energy, and the environment and the Bureau of Cyberspace and Digital Policy, to develop a detailed strategy that (1) prioritizes countries for U.S. engagement, (2) identifies the most strategically vital technology domains, and (3) aligns U.S. investments and other tools accordingly.

Establish a Strategic Competition Council. The White House should create an interagency Strategic Competition Council to elevate and better coordinate U.S. efforts to counter Chinese influence in strategic markets and sectors abroad, including digital infrastructure and emerging technologies.

Strategic Investment

Establish a new U.S. Partnership Agency by consolidating the U.S. International Development Finance Corporation (DFC), Export-Import Bank of the United States (EXIM), U.S. Trade and Development Agency (USTDA), PGI, and the International Trade Administration's Global Markets and Industry & Analysis functions. At the same time, consolidation must not be a pretext for cutting the overall resources that these agencies receive, beyond any efficiencies from streamlining. This moment demands more investment in proactive commercial engagement, not less.

Alternatively, the White House and Congress should reform the DFC and EXIM for the global technology competition.

- ***DFC***—Congress should quadruple its total lending authority to $240 billion and designate emerging technologies and digital infrastructure as a priority area.[2] Congress should also loosen restrictions that often block the DFC from supporting digital infrastructure projects that may incidentally benefit high-income countries and modernize how the DFC accounts for equity investments, consistent with the Enhancing American Competitiveness Act.[3]
- ***EXIM***—Policymakers should require the EXIM to allocate at least half its lending support to projects that counter China and promote advanced technologies, relax U.S. shipping and content requirements for China and Transformational Exports Program investments, and at least double the EXIM's default cap to 4 percent.

Review and potentially expand the International Technology Security and Innovation Fund (ITSI), administered by the State Department, which promotes secure telecommunications networks and resilient information and communications technology (ICT) and semiconductor supply chains abroad.[4] ITSI currently has $500 million in funding over five years.

Expand and reform the Countering PRC Influence Fund (CPIF). Congress should revise the CPIF's authorizing language to make countering the DSR an explicit priority and scale it to at least $1 billion, increasing it further based on performance.[5]

Expand the USTDA's Global Procurement Initiative. The Global Procurement Initiative improves the capacity of foreign public officials to account for the full life cycle of costs, such as security, reliability, and maintenance, when making significant procurement decisions.

Leverage U.S. influence over multilateral development banks to raise standards for all ICT projects. Washington and its allies should leverage their financial contributions to multilateral development banks, such as the World Bank and Inter-American Development Bank, to raise procurement standards to further emphasize quality, trust, and security, drawing on insights from the USTDA's Global Procurement Initiative.

Identify and prepare for critical procurement decisions for digital infrastructure and services in priority emerging markets. The State Department should direct embassies to identify the life cycle of digital infrastructure, determine future procurement junctures when such infrastructure will require modernization or replacement, and work now to prepare U.S. and allied alternatives.

Technology Diplomacy

Pilot a cohort of Foreign Technology Officers. A pilot class of Foreign Technology Officers would receive extensive training in critical and emerging technology policy and deploy to priority posts abroad.

Expand training for Cyberspace and Digital Policy Statecraft at the Foreign Service Institute. Established in 2024, the class is routinely oversubscribed. The State Department should increase offerings and require this training for Regional China Officers.

Appoint more ambassadors with leadership experience in the technology sector. Few U.S. diplomats, and especially ambassadors and senior Foreign Service Officers, have a deep background in technology, limiting their ability to elevate and shape technology policy on the ground.

Expand the number of U.S. Commercial Service Officers and DFC employees deployed abroad to increase support for U.S. technology companies to identify and secure strategic opportunities in emerging markets.

Focus the U.S. Department of Defense's Office of Strategic Capital. The White House should ensure that the office focuses on providing analysis about which emerging markets deserve prioritization from the Defense Department's perspective; otherwise, it should focus investments on U.S. and allied defense-relevant technologies overlooked by current market incentives.

Leverage NATO member-state investment funds. NATO should convene a summit to explore opportunities for member-state sovereign wealth funds and other investment funds to support digital ecosystems in priority emerging markets. Canada, Denmark, Italy, Norway, and Türkiye—and perhaps, soon, the United States—have sovereign wealth funds. Norway's fund is the largest in the world, with $1.8 trillion in assets.[6]

Technology Partnerships

Create a mechanism for countries to request strategic technology partnerships with the United States. Washington should create a framework for foreign governments to request strategic technology partnerships with the United States. Washington could lay out clear, broadly consistent criteria—as it did with the now-rescinded Framework for AI Diffusion—as a condition for these partnerships, such as robust intellectual property and cybersecurity protections and divestment from China-linked digital infrastructure. In exchange, Washington would fast-track approvals and support from bodies like the new U.S. Partnership Agency and expand technology trade missions, research collaboration, and talent exchanges.

Strengthen and focus the American AI Exports Program on key emerging markets. The July 2025 executive order on Promoting the Export of the American AI Technology Stack requires industry proposals for a full-stack AI technology export package. Given limited capacity and resources, the administration should focus the newly created program on priority emerging markets. The Economic Diplomacy Action Group empowered under the July 2025 executive order should undertake a comprehensive review of all relevant federal tools and resources to identify opportunities to streamline application procedures, requirements, and review timelines.

Elevate smart cities in the AI Exports Program. In developing the new AI Exports Program, the Trump administration should clarify that it will prioritize AI-enabled smart city applications that respect democratic values to jump-start the development of integrated rights-respecting U.S. offerings able to compete with China's techno-authoritarian alternatives.

Focus coordination with allies and partners in strategic regions to maximize impact. The United States should work more closely with technology-leading allies and partners to identify select "swing states" and strategic technology areas and align investments and engagement to the maximum extent possible—for instance, by leveraging the EU's Global Gateway and the Trilateral Infrastructure Partnership between Australia, Japan, and the United States.

Create a U.S. Partnership Portal for both U.S. and foreign companies, universities, and research institutions to harness existing U.S. government tools and resources. The White House should create a single point of entry where U.S. companies and foreign counterparts can access all the relevant resources and personnel.

Revive Digital Ecosystem Country Assessments. Before its closure, the U.S. Agency for International Development conducted in-depth assessments of emerging market digital ecosystems.[7] These assessments are vital for effectively targeting U.S. public and private sector engagement.

I.

Introduction

Introduction

The year 2025 marks the 10th anniversary of the Digital Silk Road (DSR), China's ambitious initiative to deepen ties through global technology diffusion. A decade after its launch, the DSR's scope and effectiveness remain poorly understood, even as technology has become central to Chinese domestic and foreign policy, the U.S.-China competition, and government agendas across the Global South. In every region, capitals and corporate boardrooms seek to harness accelerating digitalization and rapidly progressing technologies like artificial intelligence (AI) to benefit their economy, society, and security.

Across the Global South, governments have embraced technology's potential to mature their economies, create good-paying jobs, and burnish their global stature. Indonesia's president, Prabowo Subianto, views the country's digital sector as vital to diversifying its commodity-reliant economy.[8] Crown Prince Mohammed bin Salman has made AI fundamental to his "Vision 2030" for Saudi Arabia's economic and social transformation.[9] Kenyan president William Ruto has touted the country's "Silicon Savannah" to attract billions in new investment from foreign technology firms.[10] Ambitions from Brasília to Delhi are no less bullish. All of this has fed surging demand for digital infrastructure and services in emerging markets, catalyzing intense competition between China and the United States to shape the digital future of strategic "swing states" around the world.[11]

A decade after the DSR's inception, digital infrastructure and services have only become more important as military, intelligence, commercial, and government activity moves online and powerful capabilities arise from AI, the Internet of Things (IoT), and next-generation telecommunications. America has long benefited from the U.S.-led global information and communications technology (ICT) infrastructure, and these trends increase both Washington's interest in defending its position and Beijing's interest in supplanting it. A core component of Beijing's goal to upend the U.S.-led global order is replacing the U.S.-centric digital order with a new one routed through Beijing.

At stake is a future in which entire countries and regions could become further ensnared in China's digital ecosystem—surrendering the data of their governments and citizens, handing Beijing new leverage over emerging economies, and exporting its techno-authoritarian model to emerging democracies. If China succeeds, it will reap massive security, intelligence, and economic benefits. It could also accelerate the fragmentation of the global internet and erode market share for U.S. and allied firms in rapidly digitizing rising powers across the Global South.

The case for countering the DSR is as much about seizing opportunities as limiting risks: The United States and its allies have a powerful hand to play as emerging markets make generational policy, partnership, and investment decisions for advanced digital infrastructure and services. The opportunity is not merely commercial; it is about using America's technology offerings as a catalyst for deeper government, business, and societal ties to pull strategically important rising powers closer to its orbit. It is also about offering the world competitive technologies—and, in turn, shaping technology ecosystems—rooted in democratic values of openness, freedom, fair competition, due process, and respect for civil liberties. Failure to make such an offering risks ceding not only emerging markets to Chinese companies, but emerging democracies to Chinese technology-enabled surveillance and social control.

America's longtime technology leadership has given its firms a commanding global presence. Google and Microsoft now derive half their annual revenue from foreign markets.[12] Growing foreign revenue allows U.S. companies to reinvest and maintain their competitive edge, feeding a virtuous cycle. Beyond the commercial motivations of U.S. firms, their global presence bestows a powerful organic means to influence the governance and use of new technologies consistent with democratic values. U.S. companies have long championed a free, open, and secure internet not only because it suits their commercial interests, but because it also reflects their values. Of course, not all U.S. technology diffusion is inevitably good for democracy: American social media, for instance, has empowered both freedom fighters and dictators. One does not have to view U.S. technology companies as angels, however, to fear a future in which Chinese technology firms dominate.

The case for countering the DSR is as much about seizing opportunities as limiting risks.

And there is reason for worry. Across the globe, Chinese firms are expanding their footprint by underpricing U.S. and allied offerings through generous domestic industrial policies, overseas financing, strategic partnerships, and a range of other tools from workforce training to outright pressure and bribery.

During President Trump's first administration, Washington began to fight back. U.S. efforts to restrict Chinese telecommunications firms Huawei and ZTE drew global attention to the success—and dangers—of Beijing's push to dominate next-generation wireless networks. There has been decidedly less attention, however, to how the DSR has evolved in response to rising U.S. and allied restrictions, changing technology capabilities and priorities within China, and trends in emerging market demand. Concerns about the data security of Chinese telecommunications networks, for instance, have not been matched by worries about the proliferation of Chinese data center, cloud, and AI partnerships with foreign governments. Concerns about China's successes in deploying 5G have not been mitigated by an understanding of its failures—for example, the deployment of ineffective "smart city" infrastructure in Islamabad and Lahore, Pakistan.[13] Policymakers would benefit from a clear-eyed assessment of the DSR's effectiveness to date; its evolution into next-generation digital infrastructure, skilling, and services; and the consequences for U.S. and allied interests.

Even as the global technology competition intensifies, the United States and its allies have largely failed to adapt their strategies, institutions, and tools to this new reality. China has not made this mistake. Against this backdrop, clarifying the true nature and effectiveness of the DSR gains new urgency. So does clarifying where the United States and its allies have fallen short in competing with China in the Global South and outlining a credible way to win. If there is broad recognition that China won the last technology transition to 4G and 5G networks in emerging markets, there is far less agreement about how the United States and its allies can learn from that failure and win the critical technology transitions now unfolding around the world.

Fortunately, the United States and its allies enter this phase of global technology competition with formidable advantages in key domains—from fiber-optic cables beneath the waves to advanced satellites in low orbit to next-generation data centers and AI services powering a new era of digital cognition. As more sectors and services integrate with these technologies, the countries and companies able to lay this new digital foundation will gain profound, long-term influence in the 21st century—for better or worse—akin to the U.S. dominance of the global financial system in the 20th century.[14] America's technology strengths are not a cause for complacency, but a call to action—to preserve its position, counter China's DSR, and offer the world a vision of technology development rooted in human freedom and shared opportunity.

This report seeks to help U.S. and allied policymakers meet the moment. Specifically, it draws on 18 months of historical and comparative research, open-source analysis, and more than 40 expert interviews to offer an in-depth study of the DSR and U.S. and allied efforts to counter it in key emerging markets. It also outlines an ambitious agenda for the United States and its allies to win the key technology transitions now unfolding across the globe. To balance the report's analysis with emerging market perspectives, the authors conducted field visits to Indonesia, Brazil, Kenya, and Saudi Arabia, where they interviewed leaders from government, academia, civil society, technology start-ups, national telecommunications champions, and multinational tech firms. These visits resulted in four in-depth case studies published previously under this project, and whose insights inform this report.[15]

America's technology strengths are not a cause for complacency, but a call to action—to preserve its position, counter China's DSR, and offer the world a vision of technology development rooted in human freedom and shared opportunity.

Following this introduction, **Part II** reviews the case for countering the DSR, focusing on four principal arguments related to lost market share for U.S. and allied firms; expanded risks of Chinese surveillance, data security, and sabotage; strengthened Chinese leadership in strategic technologies; and spreading techno-authoritarianism.

Part III provides a detailed study of the DSR. It examines the DSR's origins and goals; its evolution and expansion over the past decade; and its key actors, authorities, and tools.

Having examined the origins, evolution, and key actors of the DSR, **Part IV** surveys the primary tools that enable China to compete in global markets, focusing on its domestic industrial policy, overseas project financing, strategic bundling, nonmarket incentives, commercial diplomacy, international standards setting, and tech upskilling.

Part V of the report reviews the six priority domains of competition between China, the United States, and its allies in the Global South: subsea cables, next-generation

telecommunications, low Earth orbit (LEO) satellites, data centers and cloud services, AI, and smart cities. For each domain, the report provides a high-level overview of the key players, trends, stakes, and state of play.

In **Part VI**, the report turns to the United States to assess its efforts—for better or worse—to counter the DSR and offer a compelling alternative. It reviews key institutions and initiatives at the State Department, U.S. International Development Finance Corporation (DFC), Export-Import Bank of the United States (EXIM), and other organizations to surface successes, redundancies, and opportunities for reform.

Part VII surveys key initiatives of U.S. allies and partners, including the European Union's Global Gateway Program, Japan's Official Development Assistance, and Australia's active cyber diplomacy.

The report then concludes with **recommendations** for the United States and its allies to help win the technology competition with China in key emerging markets with a newly ambitious vision of technology statecraft.

II.

The Case for Countering the Digital Silk Road

The Case for Countering the Digital Silk Road

Given competing demands on U.S. resources and policymakers' attention, it is worth clarifying the specific case for countering the DSR. It is not about halting the diffusion of all Chinese technology in emerging markets, which is neither realistic nor desirable. China is the principal trading partner for most of the world, and as its economy has advanced, a growing share of its trade now encompasses data and digital services. Policymakers should not view all Chinese technology exports as inherently nefarious; they often meet genuine demand around the world for low-cost technologies such as smart appliances and computer monitors. A policy that seeks to reverse the diffusion of Chinese technology products is both undesirable and doomed for failure. Instead, policymakers should proceed with a clear-eyed understanding of when and where such diffusion carries meaningful consequences for U.S. interests and values. This section will identify those conditions to inform a more targeted and effective response to China's DSR.

The case for countering the DSR rests on four principal concerns:

Lost Market Share for U.S. and Allied Firms

Demand for digital infrastructure and services is surging in the Global South, driven by growing populations, rapid digitalization, and new policies that elevate technology as a national priority. In Latin America, nearly 100 million people are expected to gain internet access over the next decade, and mobile internet traffic is growing faster across the region than in most of the world.[16] Brazil alone could see over $350 billion in data center investments over the next decade.[17] In the Middle East, Gulf states like Saudi Arabia and the UAE are investing billions in advanced technologies to modernize their economies, and the region's data center market could nearly triple by 2029.[18] Southeast Asia's digital economy grew 27 percent per year between 2021 and 2023 and could reach $1 trillion by 2030.[19] Africa's digital economy could exceed $700 billion by 2050 as millions of new internet users drive up demand for mobile payments, cloud services, and e-commerce.[20] Former U.S. ambassador to Kenya Meg Whitman emphasized the stakes: "Africa is the last, and largest, emerging market … with opportunities like Southeast Asia presented 20 years ago."[21]

The countries and companies able to meet surging demand across the Global South will not only reap significant commercial rewards—allowing them to reinvest in R&D to maintain their innovative edge—but also secure longer-term vectors to positively influence the trajectory of fast-growing technology ecosystems worldwide.

Surveillance, Security, and Sabotage

Washington and its allies have long warned that Chinese technology companies pose risks to data security, pointing to Chinese national security laws and the close cooperation between the Chinese state and domestic companies.[22]

Mounting evidence of compromised Chinese-linked networks and products has only reinforced these concerns. In 2018, African Union staff discovered that its headquarters, which was built and IT-equipped by Chinese firms, had been transferring data nightly to servers in Shanghai for over five years.[23] In a similar case, a Huawei-built government data center in Papua New Guinea had "critically vulnerable" architecture, seemingly by design.[24] Despite growing evidence,

> **The Snowden leaks undermined U.S. credibility on surveillance, and emerging markets often saw Washington's pressure campaign as an attempt to protect its own access to global dataflows instead of a sincere concern for security.**

Washington's data security case has often fallen flat across much of the Global South. The Snowden leaks undermined U.S. credibility on surveillance, and emerging markets often saw Washington's pressure campaign as an attempt to protect its own access to global dataflows instead of a sincere concern for security. In interviews conducted for this report, certain emerging market officials admitted, "We don't care about being listened to by the Chinese."[25]

Whether or not emerging market leaders care about data security, the reality is that ongoing technology transitions in the form of data centers, cloud services, AI, smart cities, and IoT devices will collect and process far more data than conventional networks.[26] Huawei has already built 160 smart cities in over 100 countries that collate data on driver's licenses, mobile payments, and traffic management.[27] Data centers built by Alibaba and Tencent host sensitive data and records for dozens of

Hikvision cameras on display in a Beijing mall—part of an estimated 4.8 million Hikvision camera networks operating worldwide, each containing up to 24 cameras. The company's dominance in global surveillance exports, coupled with its provision of AI-enabled analytics, underscores the security risks of placing sensitive public data in the hands of partially state-owned Chinese vendors. (Fred Dufour/AFP via Getty Images)

governments globally.[28] Hikvision has exported surveillance cameras to over 155 countries, often bundled with AI-enabled analytics that can recognize faces and flag unusual movements.[29] Foreign governments or critical sectors that become dependent on such systems could hand Chinese firms—and Beijing—valuable strategic insights.

Strengthened Chinese Leadership in Strategic Technologies

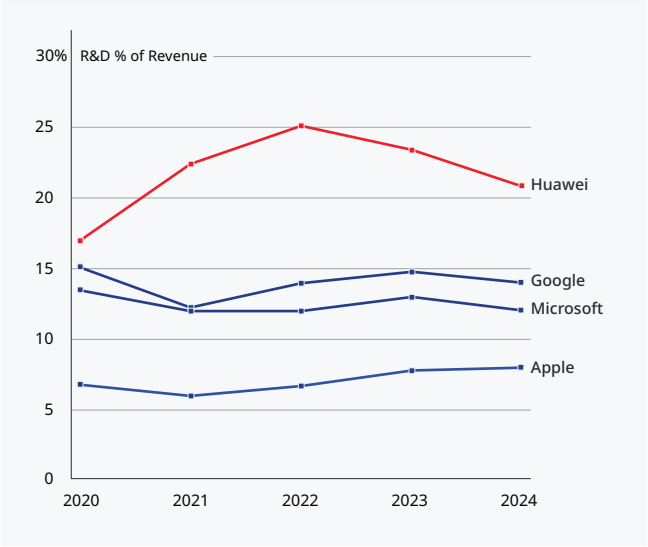
Among the DSR's goals is securing market share across the Global South for Chinese technology firms, which now face heavy restrictions—if not outright bans—in many wealthier markets. Overseas revenue, in turn, supports greater reinvestment by Chinese technology firms in R&D to keep pace with capital-rich U.S. tech giants. With U.S. firms pouring hundreds of billions of dollars into advanced technologies, Chinese companies face mounting pressure to close the gap and remain competitive.

The relationship between Huawei's overseas revenue and reinvestment illustrates the dynamic. In 2024, Huawei earned nearly $50 billion from overseas sales, representing 41 percent of its total revenue.[30] Huawei's foreign revenue helps sustain one of the most aggressive R&D programs in the world.[31] In 2024, the company reported a $25 billion investment in R&D—over 20 percent of its total revenue. This reinvestment rate rivals or exceeds that of many leading U.S. tech companies: Apple allocates roughly 8 percent of its annual revenue to R&D, while Microsoft and Google allocate 12 and 14 percent, respectively.[32]

Although Huawei's total revenue is smaller than these U.S. counterparts, its higher R&D intensity reflects both its focus on innovation and the imperative to invest a higher share of its total revenue to keep pace. In this way, Huawei's expansion into fast-growing foreign markets sustains its high levels of R&D reinvestment, supporting China's broader ambition to close technology gaps in areas such as advanced AI chips.[33]

Expansion into foreign markets also gives Chinese firms access to unique datasets that help refine and improve their technologies.[35] For instance, CloudWalk

FIGURE 1: HUAWEI REINVESTS A HIGHER SHARE OF REVENUE IN INVESTMENT THAN MANY U.S. FIRMS (2020–2024)[34]



This figure compares research and development (R&D) reinvestment as a percentage of revenue for Huawei, Apple, Microsoft, and Google, illustrating how Huawei leverages overseas revenue to sustain one of the world's most aggressive reinvestment rates.

Technology struck a deal with the government of Zimbabwe to build a national facial recognition system.[36] In exchange, the company gained access to Zimbabwe's facial imagery database, which contained racial and phenotypic features that differ markedly from China's ethnically Han-majority population. These expanded data enabled CloudWalk to strengthen its facial recognition algorithms, improving its global edge.[37]

Diffusion of Techno-Authoritarianism

According to Freedom House, 2024 was the 18th consecutive year of democratic backsliding around the world.[38] The global retreat from democracy has many causes, but the proliferation of advanced surveillance platforms, censorship-enabling firewalls, and automated behavioral tracking have emerged as powerful, relatively low-cost instruments of authoritarian control. A perennial challenge for autocrats is centrally managing societies and economies that have grown exponentially more complex. Advances in AI and smart city offerings may help close that gap, for instance, by dramatically lowering the cost of real-time population monitoring and behavioral tracking.[39]

A growing number of countries have shown interest in China's techno-authoritarian model. Chinese technology offerings already support repressive governance around the world through high-definition surveillance cameras, centralized databases, and AI-powered monitoring tools.[40] At least 80 countries have adopted Chinese surveillance technology, such as Huawei's "Safe City" surveillance networks.[41] In Venezuela, Nicolás Maduro's government partnered with ZTE to build a nationwide digital ID and database known as the "Fatherland" system that aggregates data on citizens—tracking everything from financial transactions and welfare benefits to social media use and voting history.[42] In 2024, Pakistan began testing a nationwide internet firewall built with Chinese technology, drawing comparisons to China's Great Firewall.[43]

Chinese technology offerings support repressive governance around the world through high-definition surveillance cameras, centralized databases, and AI-powered monitoring tools.

To be fair, the effect of Chinese technology diffusion on a country's politics ultimately hinges on how those technologies are used and governed. Facial recognition cameras, for instance, may be inherently ripe for abuse by an autocratic regime, but they can also be deployed responsibly by free societies with rules limiting their data collection, retention, and use. Governments can wield AI to monitor and dox critics, or to improve transparency, accountability, and services; in the end, governments and citizens can use technology to strengthen or undermine democracy.

***

Left unchecked, the DSR threatens to erode U.S. and allied market share in key technologies, expose partners to CCP surveillance and cyber risks, weaken America's technological edge vis-à-vis China's, and accelerate the global spread of techno-authoritarianism. The task ahead is not to restrict all Chinese technology, but to identify where its diffusion poses real consequences for U.S. interests and act accordingly.

III.

The Digital Silk Road in Focus

The Digital Silk Road in Focus

As the DSR marks its 10th anniversary, its true nature remains poorly understood. Since its inception, the DSR's evolution has mirrored the rising importance of technology in China's economy and foreign policy, Global South economies, and the U.S.-China competition broadly. These dynamics have combined to make the DSR at once more important and more obscured than at any time since its launch. Paradoxically, the DSR has receded as a publicly touted, state-led initiative over the past decade, even as Beijing has elevated technology leadership and diffusion at home and abroad. This section seeks to explain these dynamics and shed light on the DSR's origins, evolution, tools, and effectiveness to date, and in doing so, help U.S. and allied policymakers tailor a more effective response.

Origins and Goals

China announced the DSR in a 2015 white paper as a new pillar of the Belt and Road Initiative, China's flagship initiative to strengthen global ties to Beijing through large-scale infrastructure projects.[44] Whereas the BRI focused on physical infrastructure such as roads, bridges, and ports, the DSR has focused on digital infrastructure in the form of telecommunications networks, terrestrial and subsea cables, cloud computing, and smart cities. By 2017, the DSR had become one of the BRI's central pillars. By 2019, Chinese officials began referring to the DSR as its own initiative, signaling its elevation.[45] The lines between the DSR and the BRI have always been blurry, mirroring the growing overlap between physical and digital infrastructure.

As Beijing's interest in strategic technologies expands, the criteria for DSR projects remain porous by design. Indeed, Beijing and Chinese companies have applied the DSR label flexibly to tout their technology exports and engagement abroad when it suits their interests—for example, to advance narratives of technological leadership and Global South solidarity. At the same time, viewing the DSR as a mere branding exercise risks downplaying Beijing's role in enabling the diffusion of Chinese-linked digital infrastructure and technologies across the globe.

This report adopts a more expansive definition of the DSR as the *state-enabled* diffusion of Chinese digital infrastructure and technologies in foreign markets. The term *state enabled* encompasses the full spectrum of Chinese state support for global technology diffusion, which includes domestic subsidies that allow firms to offer below-market offerings abroad; ecosystem-level support through standards setting, upskilling, and high-level political support for government-to-government agreements; and direct financing and nonmarket incentives for specific projects.

A narrower definition focused only on projects explicitly branded under the DSR would dramatically understate the extent of Chinese state-supported technology diffusion worldwide. However, this report does not mean to suggest that all Chinese technology diffusion is *state directed*. Unlike the BRI, which is managed by China's National Development and Reform Commission, the DSR is more market driven, with a handful of top technology firms spearheading virtually all its projects.

Beijing's expansive support for the DSR reflects the intertwined economic, strategic, and political goals that the initiative aims to advance:

- **Reduce reliance on U.S.-dominated global ICT infrastructure.**
- **Strengthen China's digital economy and technology innovation.**
- **Absorb industrial overcapacity.**
- **Secure overseas markets for Chinese firms.**
- **Strengthen bilateral ties and leverage.**

The following sections will review these goals in turn.

REDUCE RELIANCE ON U.S.-DOMINATED GLOBAL ICT INFRASTRUCTURE

The DSR mitigates China's long-standing security concerns about dependence on Western technology and, more recently, U.S. ICT infrastructure. U.S. and allied firms control 70 percent of the global cloud market and built over 90 percent of the world's subsea cable infrastructure.[46] Significant global internet traffic also routes through the United States, fueling concerns about surveillance and data security. In 2013, these concerns deepened in Beijing and many foreign capitals after leaks from Edward Snowden revealed that Washington had leveraged its position as the global ICT hub to feed its expansive surveillance capabilities.[47] Beyond concerns about reliance on foundational digital infrastructure, Beijing also saw a broader global technology stack dominated by U.S. firms, from search to social media to computer operating systems to advanced semiconductor design. The DSR is inseparable from China's broader campaign to replace—or at least mitigate—America's dominance of global digital infrastructure and services. Both ambition and anxiety motivate the initiative.

STRENGTHEN CHINA'S DIGITAL ECONOMY AND TECHNOLOGY INNOVATION

The DSR's outward focus masks several inward objectives, which principally relate to promoting economic growth, technological innovation, and self-sufficiency. Understood this way, the DSR advances Xi's call for "dual circulation," an economic model intended to diversify China's trading partners, reduce its reliance on the United States, and increase the country's self-sufficiency in critical technologies. Under this model, revenue generated abroad by Chinese technology firms drives domestic consumption, employment, GDP growth, and reinvestment to keep pace with capital-rich U.S. technology giants.[48] These dynamics complement Beijing's ambitions to dominate advanced technology manufacturing by 2025, lead in global technology standards by 2035, and become a global superpower by 2050.[49]

ABSORB INDUSTRIAL OVERCAPACITY

Another goal of the DSR is absorbing industrial overcapacity. Beijing's urgency to achieve self-sufficiency and close technology gaps with the United States has led to massive state subsidies, largely through supply-side investments to expand industrial capacity. By 2013, China's industrial policies had produced severe overcapacity, leaving its firms heavily dependent on foreign markets to absorb the surplus.[50] For technology specifically, this created excess supply of legacy semiconductors, fiber-optic cables, and IT equipment.[51] In 2015—the year the DSR launched—overcapacity in China's fiber-optics industry exceeded 50 percent.[52] China's State Council responded by recommending that the state "actively expand the external market."[53] The result was a policy to transform overcapacity at home into geostrategic advantage abroad by enabling Chinese firms to offer artificially low prices to secure foreign market share. The proliferation of cheap Chinese electric vehicles is among the latest examples of this dynamic.

SECURE OVERSEAS MARKETS FOR CHINESE FIRMS

A related but vital objective of the DSR is to help Chinese technology firms secure market share abroad. Overseas expansion embeds Chinese technical standards in key ecosystems and gives Chinese firms valuable field experience to test and iterate products in diverse environments, bestowing a competitive edge. Chinese firms also seek first-mover advantages, understanding that once foreign governments and businesses select foundational digital infrastructure and services, they can lock in customers and leverage for years.

STRENGTHEN BILATERAL TIES AND LEVERAGE

Beyond commercial motives, the DSR also aims to strengthen Beijing's bilateral relations with emerging economies. Studies have found that Beijing's infrastructure and financing arrangements in emerging markets often correlate with closer diplomatic and foreign policy alignment.[54] The DSR reinforces China's self-image as a champion of the Global South. Beijing has shrewdly played on historical grievances among many emerging markets that believe they were "left behind" in past eras of technological advancement, while promoting itself as a champion of development-friendly technology.[55]

Beijing also plays on shared anxieties in many Global South markets about dependence on U.S.-centric global ICT infrastructure, promoting the DSR as an alternative. For example, in 2013, Brazil's secretary of telecommunications described how the country's "communication routes with the world are mainly through the United States ... [t]his creates a vulnerability in Brazilian communications."[56]

In sum, the DSR has advanced overlapping goals for Chinese companies and the state that have evolved with the initiative itself.

Kenyan President William Ruto (L) and Chinese Vice Premier Ding Xuexiang (R) attend a high-level meeting on Belt and Road cooperation during the Forum on China-Africa Cooperation in September 2024. Such engagements illustrate how China uses the Digital Silk Road to advance commercial projects and position China as a preferred technology partner for emerging markets. (Wu Hao/Pool/AFP via Getty Images)

The Digital Silk Road Today

This section examines the growing importance and evolving nature of the DSR, which has become increasingly central to China's overseas ambitions. As China faces backlash against BRI-linked debt distress abroad and mounting economic challenges at home, Beijing has focused on more profitable, scalable technology projects with foreign partners and turned to its private technology firms to implement them. As a result, the lines between the BRI and DSR have increasingly blurred.

DSR REBRANDED: "SMALL YET SMART"

Chinese officials have emphasized a new phase of "small and beautiful" or "small yet smart" projects abroad: financially viable deals in profitable, scalable sectors like cloud computing, financial technology, and AI IoT.[57] This tactical rebranding reflects both backlash over BRI-linked debt and leverage abroad and rising economic pressure at home. In his 2021 speech at the Belt and Road Symposium, Xi Jinping first signaled the emphasis on "small yet smart" to transition away from the big-ticket projects of the BRI's first decade toward less capital-intensive digital infrastructure and services.[58]

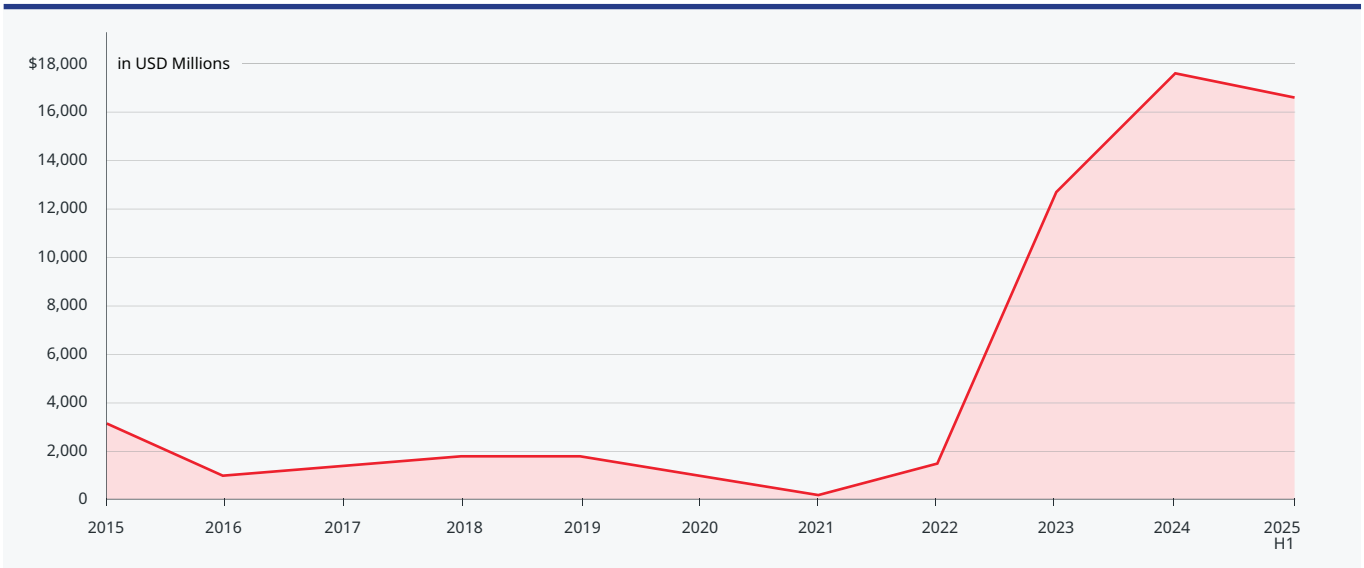
Although China's BRI investments have become "smarter," they have not grown smaller as private entities assume a greater role. The average deal size of BRI and DSR projects grew from $672 million in 2024 to a record $1.2 billion in the first half of 2025.[59] These figures are two to three times higher than typical levels over the past decade.[60]

Remarks by Xi underscore how Beijing has elevated the DSR and reoriented the BRI to technology. In October 2023, Xi opened the Third Belt and Road Forum, where he announced that the BRI had entered an era of "high-quality development," placing technological innovation at the heart of this agenda.[61] Less than a month later, China held the first Belt and Road Conference focused specifically on technology.[62]

Chinese officials have emphasized a new phase of "small and beautiful" or "small yet smart" projects abroad: financially viable deals in profitable, scalable sectors like cloud computing, financial technology, and AI IoT.

Following the high-level push for "small yet smart" projects, state and private DSR investments surged, growing by 794 percent in 2022 compared to the previous year, and by another 905 percent in 2023.[63] Trade data mirror this growing importance of technology: In the first half of 2024, China's trade in digital services reached $200 billion and cross-border e-commerce topped $169 billion—both historic highs.[64]

FIGURE 2: CHINESE TECHNOLOGY INVESTMENTS IN BELT AND ROAD INITIATIVE PARTNER COUNTRIES[65]



*Digital Silk Road investments have reached record highs, reflecting Beijing's shift toward more scalable and profitable technology projects.**

*Data estimates are sourced from the Green Finance & Development Center. Figures presented are approximate and carry a margin of error; the visualization is intended for illustrative purposes only.

ENTERPRISE LED, GOVERNMENT GUIDED

Beijing increasingly relies on private Chinese companies to shoulder the cost of DSR investments.[66] This shift stems from both domestic fiscal pressures and a recognition that overtly touting Chinese government support was increasingly unhelpful in securing bids as Washington and its allies escalated their global campaign against Chinese technology products (detailed in the next section).

The result is what Beijing calls an "enterprise-led, government-guided" model.[67] Under this model, capital-rich firms—typically large Chinese technology companies—are expected to lead. The state offers policy guidance, diplomatic support, and coordination, while firms like Huawei, Alibaba, and Tencent shoulder the execution and financial risk.[68] Beijing seeks projects that can self-sustain through private investment and commercial viability rather than state support.[69] Investment data confirm this shift: In 2020, nearly all major BRI and DSR investors were Chinese state-owned enterprises (SOEs); Alibaba, the largest non-SOE investor that year, accounted for just 1.3 percent of total outbound BRI and DSR investment. By 2023, however, private enterprises such as CATL and ByteDance dominated these investments, accounting for nearly 60 percent.[70]

The DSR has moved from a peripheral component of the BRI to one of its central drivers.

While Beijing has reined in financial support for large-scale overseas infrastructure, this slowdown does not reflect a "collapse" in lending, as some analysts have suggested.[71] While the Export-Import Bank of China (China Exim Bank) and China Development Bank (CDB) reduced their BRI and DSR lending by 86 percent between 2016 and 2024, Chinese commercial banks covered their retreat.[72] The People's Bank of China and its subsidiaries have emerged as key financiers: In 2013, they accounted for just 6 percent of China's overseas lending, compared to over 80 percent from state-backed China Exim Bank and CDB. By 2021, that share had flipped: the People's Bank of China was responsible for 54 percent, while China Exim Bank's and CDB's combined shares had fallen to below 25 percent.[73]

The shift away from large-scale state support also changes where Chinese firms place their bets. With commercial viability assuming greater importance, Chinese tech firms are increasingly channeling their investments to emerging markets with relatively high demand, low regulation, and rapid rates of adoption.[74] Emerging markets in the Middle East and Southeast Asia now absorb the lion's share of new BRI projects, while Africa and Latin America receive far fewer.[75] In 2024, the Middle East and Southeast Asia drew $39 billion and $25 billion, respectively, in Chinese financing and construction.[76] For new cloud and AI projects, Chinese firms are concentrating the majority of their investments in these two regions.[77]

The DSR has moved from a peripheral component of the BRI to one of its central drivers. In place of railways and coal plants financed with multibillion-dollar loans, the BRI's next chapter will be marked by a proliferation of data centers in Jakarta, cloud zones in Kuala Lumpur, and joint AI labs in Riyadh—all emblematic of a DSR recalibrated for both economic pressure at home and strategic ambition abroad.

DOWNPLAYING THE DIGITAL SILK ROAD

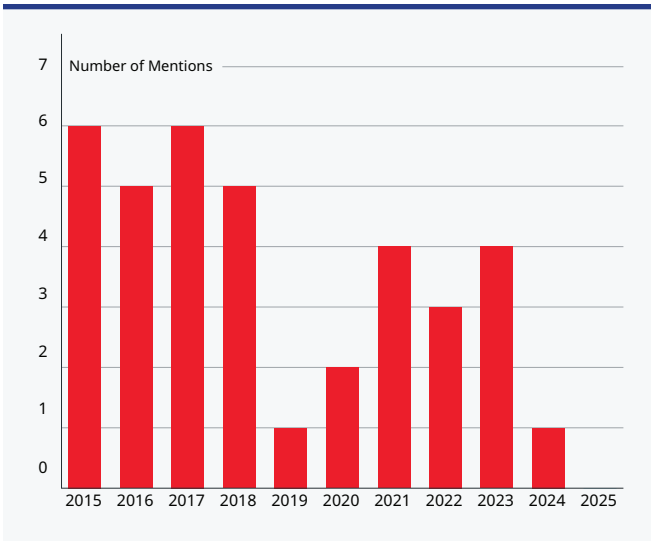
In recent years, the DSR has undergone a paradoxical evolution. Even as China's overseas technology investments have surged to record levels, the formal DSR brand has receded. Only a few years after its launch, the initiative came under pressure as U.S. and allied governments restricted Chinese technology exports and seized on the DSR label as evidence of state involvement in digital infrastructure.[78] In response, Beijing dialed back explicit references, following a pattern seen with other initiatives, such as Made in China 2025.[79] In these cases, Chinese initiatives have shed their branding even as the underlying activity persists—and even accelerates.

The same pattern holds for the DSR. Even as high-level officials increasingly tout the importance of technology to China's foreign engagement, references to the DSR in official policy documents have declined. Since 2022, the term "DSR" has appeared less frequently in China's domestic policy documents and international agreements. Analysis by the authors found that mentions of the DSR in central policy documents decreased significantly from the initiative's early years. Even the years surrounding the COVID-19 pandemic, which saw digital connectivity assume new importance, did not see increased official references to the DSR.

DSR references have also declined in intergovernmental agreements. At least 146 countries have signed memoranda of understanding (MoUs) to join the BRI, but only 16 have signed similar agreements for the DSR.[81] Moreover, there have been no new government-to-government MoUs explicitly tied to the DSR since 2020.[82]

However, it would be a mistake to conflate sparse DSR agreements with a limited Chinese digital footprint

FIGURE 3: MENTIONS OF THE DIGITAL SILK ROAD IN PEOPLE'S REPUBLIC OF CHINA CENTRAL POLICY DOCUMENTS (2015–2025)[80]



This figure shows the frequency of official references to the Digital Silk Road in the Chinese government's central policy documents over time, highlighting the term's decline from 2015–2018 peaks—even as China's overseas technology activity has continued to grow.

*Analysis ends in September 2025.

abroad. Instead, the Chinese government now typically pursues technology partnerships and MoUs outside the official DSR masthead. As of November 2023, China had signed intergovernmental science and technology cooperation agreements with over 80 countries, e-commerce cooperation with 30 countries, and digital economy investment cooperation with 18 countries and regions.[83] As of 2022, the total number of countries with investments or projects by Chinese technology and telecommunications firms is at least 165, including close U.S. allies like the United Kingdom.[84]

The decline in formal branding should not be mistaken for retreat. Even as the DSR label fades, its aims increasingly suffuse China's broader economic and technology partnerships around the world.

Key Actors and Authorities

The DSR's amorphous and evolving nature can make it difficult to identify its key public and private sector actors, along with the tools they use to promote China's technology diffusion abroad. This section attempts to clarify these key actors and authorities.

While the BRI is centrally coordinated by the National Development and Reform Commission, the DSR operates more organically. Leading Chinese technology companies largely power the DSR, often acting with significant autonomy in their overseas projects. Indeed, most DSR projects are not directly financed by the state.[85] However, this does not mean the state is absent. Beijing plays a critical enabling and guiding role—setting strategic direction, providing high-level diplomatic support, and shaping regulatory and financial environments that support China's global technology diffusion. Again, the DSR is more state *enabled* than state directed.

Three key actors have shaped the DSR's expansion: central government bodies, state policy banks, and private companies.[86] Central government ministries provide top-level guidance and diplomatic support. Policy banks like China Exim Bank and CDB provide financing when strategic interests are at stake, particularly in high-priority sectors or regions. Companies serve as the DSR's primary implementers, deploying digital infrastructure and technology platforms worldwide.

CENTRAL GOVERNMENT

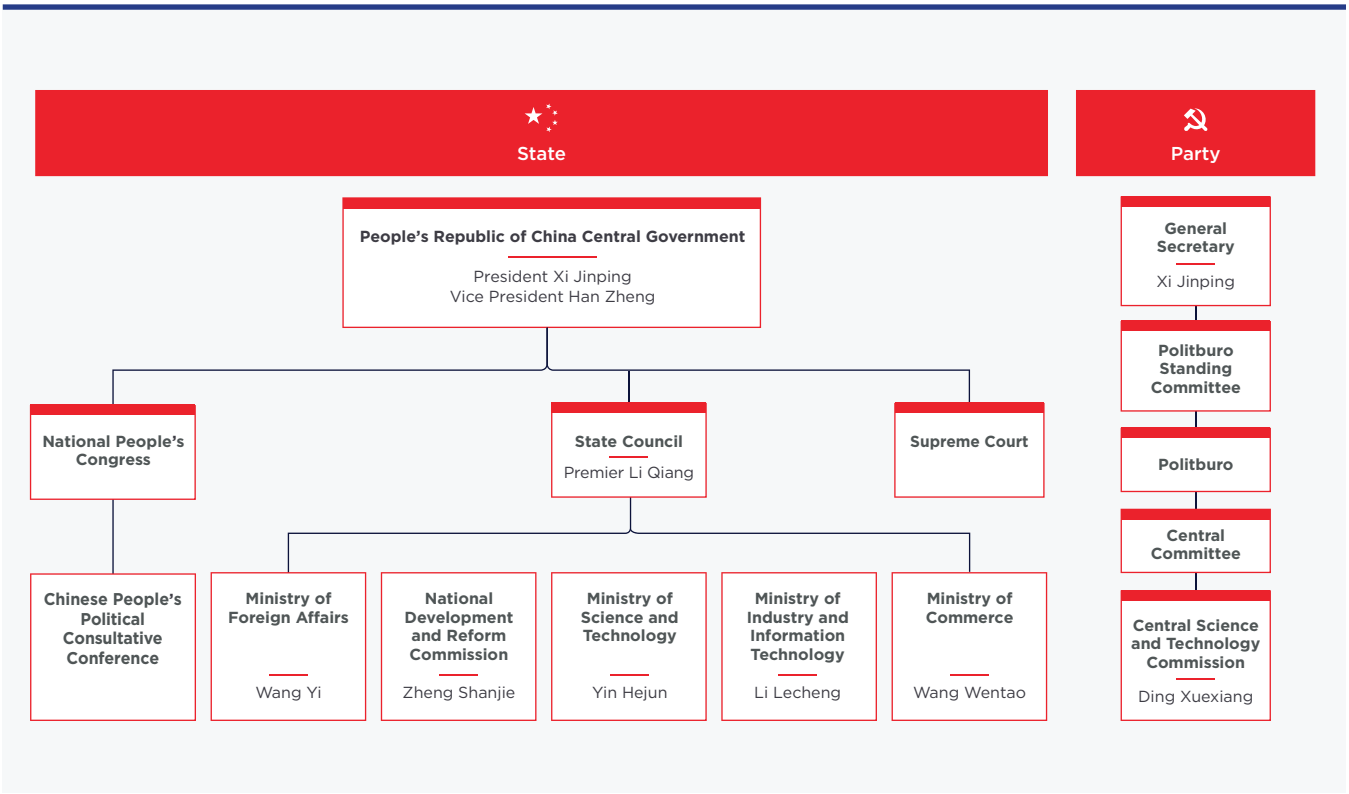
Along with the State Council, five primary ministries provide formal policy guidance for the DSR: the National Development and Reform Commission (NDRC); Ministry of Foreign Affairs (MOFA); Ministry of Commerce, Ministry of Industry and Information Technology; and Ministry of Science and Technology.[87] Although each entity plays a role in China's global technology diffusion, between 2023 and 2025, only the State Council, NDRC, and MOFA have published policy documents explicitly mentioning the DSR, suggesting that they have formal responsibility for its vision and implementation.

The Chinese government exerts less control over firms' overseas activity than outside observers have often assumed.[88] Beijing plays a guiding role consistent with the "government-guided, enterprise-led" model outlined in recent policy documents. While private firms drive the DSR's implementation, they do so within an ecosystem shaped by national frameworks. The state issues guiding documents that offer high-level direction, but private firms and policy banks have flexibility to interpret and implement that direction. The central government also creates government-to-government agreements that establish high-level priorities for bilateral economic and technology cooperation that companies pursue through business-to-business strategic partnerships or joint ventures.

STATE POLICY AND COMMERCIAL BANKS

The two main policy banks that have historically supported the DSR are China Exim Bank and CDB, which both operate under China's State Council. China Exim

FIGURE 4: KEY MINISTRIES SHAPING THE DIGITAL SILK ROAD[91]



This figure outlines the organizational structure of China's central government, highlighting the State Council and its five ministries historically involved in the Digital Silk Road's policy guidance.

The Chinese Communist Party (CCP) has transferred many responsibilities of the Ministry of Science and Technology to the Central Science and Technology Commission, which was established in 2023 under the governance of the CCP's Central Committee.[92]

Bank's focus is supporting and promoting Chinese exports through long-term export credits and concessional loans. The CDB raises funds for large-scale infrastructure projects, most of which are domestic.[89] China Exim Bank provides more overseas loans than the CDB, but the latter typically makes substantially larger commitments.[90]

China Exim Bank and CDB are also core shareholders of the Silk Road Fund, which was established in 2014 to provide long-term equity for strategic BRI and DSR projects and support higher-risk ventures that policy banks may avoid.[94] Commercial banks like the Bank of China, China Construction Bank, and Industrial and Commercial Bank of China also provide loans.[95] Sinosure (China Export and Credit Insurance Corporation) de-risks loans by insuring lenders against political or commercial default.[96]

China's development financing dwarfs the United States'. According to China Exim Bank's 2023 annual report, Chinese export credit agencies provided $39 billion, roughly 14 times the $2.7 billion of U.S. export credit financing in 2022.[97] In the past, most of China's development financing went to physical exports and infrastructure. According to the International Institute for Strategic Studies, between 2015 and 2022, only about 10 percent of DSR projects received direct state-backed loans.[98]

China's development financing dwarfs the United States'.

That has begun to shift as both China Exim Bank and CDB have received increased support for Xi's "small yet smart" BRI projects. Shortly after the 2023 Belt and Road Forum, Xi directed both policy banks to establish a $48 billion financing window to implement the new "high-quality" phase of the BRI.[99] The nearly $100 billion in new financing for "high-quality" projects suggests that China Exim Bank and CDB will assume a larger role in funding digital and tech infrastructure going forward.

Nevertheless, policy banks like China Exim Bank and CDB tend to focus on large, strategic digital

FIGURE 5: CHINA'S OVERSEAS FINANCING INSTITUTIONS[93]

Agency	Role	Tools	Resources
China Export-Import Bank (China Exim Bank)	China's official export credit agency	▪ Export credits for Chinese firms ▪ Buyer's credits for foreign purchasers ▪ Concessional and nonconcessional loans ▪ Syndicated financing with commercial lenders	▪ ~$857 billion in total assets; 4 overseas offices and roughly 560 employees
China Development Bank (CDB)	China's development policy bank charged with advancing national industrial goals domestically and overseas	▪ Medium- and long-term financing to support China's national development strategies ▪ Direct equity investments in foreign infrastructure projects	▪ ~$2.6 trillion in total assets; 11 overseas offices and more than 12,000 employees
State-owned commercial banks (e.g., People's Bank of China, Industrial and Commercial Bank of China)	Chinese commercial banks cofinance projects with Chinese policy banks, although they represent just a fraction of such lending	▪ Syndicated loans alongside Chinese policy banks ▪ Foreign currency clearing and offshore RMB financing ▪ Technical assistance for policy banks to structure complex project finance deals ▪ Short-term bridge loans ahead of longer-term financing	▪ Over $20 trillion in assets, just a fraction of which supports overseas infrastructure lending
Sinosure (China Export and Credit Insurance Corporation)	State insurance body that de-risks Chinese overseas investments	▪ Insurance for Chinese banks against borrower default on overseas loans ▪ Political risk insurance	▪ ~$27 billion in total assets; 2 overseas offices and roughly 2,550 employees
Silk Road Fund	China's sovereign investment fund created to support BRI and DSR projects	▪ Medium- to long-term equity investments ▪ Funds, loans, and debt financing ▪ Joint investment funds with domestic or foreign financial institutions	▪ ~$26 billion in investments as of March 2025; ~$66 billion in total assets
Asian Infrastructure Investment Bank (AIIB)	Multilateral development bank tied to the BRI, established as China's alternative to the U.S.-led World Bank and International Monetary Fund At the June 2025 AIIB Summit, Chinese Premier Li Qiang pressed AIIB members to provide "technology-enabled" infrastructure and "strengthen alignment with [the] BRI."	▪ Concessional and nonconcessional loans to member states ▪ Equity investments in projects ▪ Grants and technical assistance for early-stage project development ▪ Insurance guarantees to de-risk private investment	▪ $8.4 billion in reported 2024 project financing, primarily in Asia; ~$61 billion in total assets ▪ ~700 employees from 78 countries
New Development Bank (formerly BRICS Development Bank)	Multilateral development bank created by BRICS countries to finance sustainable infrastructure in emerging markets	▪ Concessional and nonconcessional loans ▪ Local currency loans to protect against foreign exchange fluctuation ▪ Project-specific technical assistance and equity investments	▪ ~$30 billion in approved loans; approximately 330 employees across five continents

This table provides an overview of China's development finance institutions, in rough order of importance. These include Chinese policy banks (China Exim Bank and CDB), state-owned commercial banks, and China's official loan insurer, Sinosure. The Silk Road Fund and two multilateral development banks with state backing, the AIIB and the New Development Bank, also finance select digital infrastructure and technology projects, albeit at a lower scale.

infrastructure projects that might be difficult for a single firm to finance alone, such as satellite systems or subsea cables.[100] Many Chinese tech exports, such as surveillance platforms or data centers, are also commercially viable given strong emerging market demand and can often proceed without significant state backing.

PRIVATE AND STATE-OWNED FIRMS

Chinese companies have become the principal drivers of the DSR. In the past, Chinese companies chose to adopt the DSR label—or not—based on their commercial interests.[101] For instance, when Huawei won a bid to build the C-Lion1 undersea cable connecting Finland and Germany, a 2017 press release touted the effort as building a "direct Digital Silk Road."[102] Huawei's public embrace of the DSR brand reflected a different commercial and political environment in the initiative's early years, before Washington ramped up its global campaign against Chinese technologies; it is hard to imagine Huawei issuing a similar press release in 2025.

The trend toward an enterprise-led approach has accelerated as state financing for external projects has declined. Concessional lending from China's state policy banks has dropped nearly 90 percent from its 2016 peak, and Beijing has pushed its leading firms—including Huawei, Alibaba, and Tencent—to lead outbound expansion.[103] State support still plays a role—especially in large infrastructure projects—but the primary engine is corporate. With that said, the Chinese government owns "golden shares" or "special management shares" in several leading Chinese firms, including local units of Alibaba, Tencent, and ByteDance. Under this structure, the state holds a minority stake (often only 1 percent) in strategic units but is granted special rights over key business decisions.[104]

In sum, there is no unified structure or primary implementing body of the DSR within China. The state-enabled diffusion of Chinese technology invariably touches on a spectrum of government-owned, government-affiliated, and mostly private entities. Unlike the BRI, the DSR has enjoyed a lighter government footprint in terms of direct financial support and formal branding. That does not mean the Chinese government plays no role; indeed, high-level policy guidance and political directives help guide state organs from banks to SOEs to advance Beijing's ambition for "small yet smart" and "high-quality" digital infrastructure and technology projects abroad. In fact, Beijing's greatest role in advancing the DSR may not come from direct financing of projects abroad, but rather from the support it provides for Chinese companies at home and the often-obscured tactics it uses to secure deals on the ground. Part IV reviews this broader range of support—specifically, how the central government, state policy banks, and Chinese firms drive technology diffusion around the world.

Beijing's greatest role in advancing the DSR may not come from direct financing of projects abroad, but rather from the support it provides for Chinese companies at home and the often-obscured tactics it uses to secure deals on the ground.

FIGURE 6: CHINA'S LEADING TECHNOLOGY FIRMS[105]

Company	Year Established	Structure	Data Centers and Cloud	AI	Telecom	Subsea Cables	Smart Cities	LEO Satellites
Tencent (腾讯公司)	1998	Publicly traded, state holds golden shares	✓	✓			✓	
Alibaba (阿里巴巴)	1999	Publicly traded, state holds golden shares	✓	✓			✓	
ByteDance (字节跳动)	2012	Publicly traded, state holds golden shares	✓	✓				
Huawei (华为)	1987	Private (employee owned)	✓	✓	✓		✓	✓
China Mobile (中国移动)	1997	State-owned enterprise (SOE)	✓		✓	✓	✓	✓
Baidu (百度)	2000	Publicly traded, state holds golden shares	✓	✓			✓	
ZTE (中兴通讯)	1985	State-owned enterprise (via controlling stake held by SOE shareholders)	✓		✓	✓	✓	✓
Hikvision (海康威视)	2001	State-owned enterprise (majority held by a central SOE)		✓			✓	
Dahua (大华)	2001	Semiprivate, state owns 12 percent		✓			✓	
SenseTime (商汤科技)	2014	Partly state owned, but publicly traded	✓	✓			✓	
China Unicom (中国联通)	2009	State-owned enterprise	✓		✓	✓	✓	✓
CloudWalk Technology (云从科技)	2015	Private, but founded with state financing		✓			✓	
HMN Tech (华海通信技术有限)	2008	Private				✓		
SpaceSail (千帆星座)	2024	State-owned enterprise, created with financing from Shanghai government						✓

This table summarizes the ownership models and sectoral focus of major Chinese technology firms active in the DSR, organized by market capitalization. Companies span a range of ownership structures—from private firms like Huawei to state-owned enterprises such as China Mobile.

IV.

How China Competes

How China Competes

Part III described the largely private-sector-led, state-enabled nature of the DSR, whose key actors and tools span several Chinese government entities and leading companies. Nevertheless, the DSR—broadly defined—uses several common tools to enable China's technology diffusion abroad with support at virtually every stage, from a technology's domestic development to its global diffusion. These tools include:

- Industrial policy
- Overseas project financing
- Strategic bundling
- Nonmarket incentives
- Commercial diplomacy
- International standards setting
- Tech upskilling

This section will review these tools to shed light on how the DSR helps Chinese tech compete abroad.

Industrial Policy

A 2025 report from the U.S. Trade Representative describes how China pursues several industrial plans in strategic, high-tech industries to enable "domination by Chinese companies, both in China and globally."[106] Beijing's industrial subsidies stand at levels unmatched by any advanced economy or emerging market.[107] This support enables the rapid global expansion of Chinese firms by allowing them to enter less commercially viable markets and gain a foothold.[108]

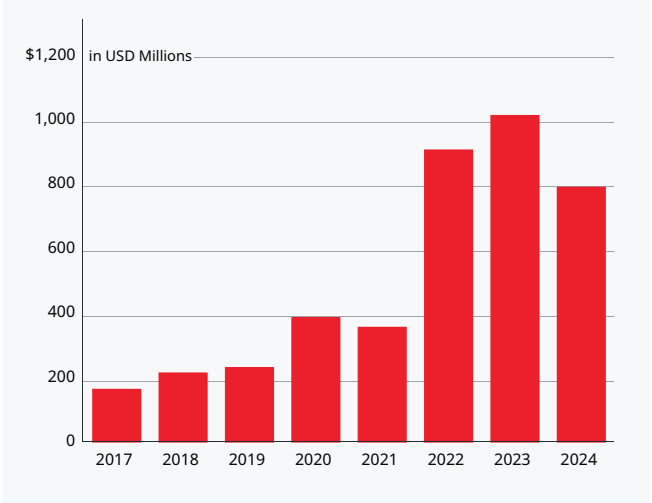
Arguably, China's most notable industrial policy for technology was Made in China 2025, Beijing's flagship initiative to transition the country from a low-cost manufacturer into a high-tech powerhouse.[109] Since the initiative's launch in 2015, Beijing has committed roughly $320 billion to mature sectors like semiconductors, industrial robotics, and biotechnology.[110] The launch of both Made in China and the DSR in 2015 underscore Beijing's twin technology ambitions at home and abroad. These ambitions work synergistically: Large-scale state support through Made in China, paired with China's massive domestic market, helps Chinese companies close innovation gaps, boost industrial capacity, and scale quickly and below cost.[111]

Huawei illustrates how state support enables Chinese firms to underprice competitors abroad. Huawei's support included zero-interest loans, waived restrictions on financing under $3 million, and two $1 billion credit lines as early as 2000.[112] Between 2008 and 2018, Huawei reportedly received $75 billion in government support, allowing it to undercut competitors and rapidly gain market share.[113] At times, those subsidies have enabled Huawei and ZTE to price bids at least 30 percent below Western competitors.[114] The scale of support has only grown. In 2024, Huawei secured nearly $800 million in direct government grants—triple the level in 2019.[115]

State investment also powers China's production of advanced AI semiconductors, the essential hardware underpinning many Chinese technology exports. According to the Semiconductor Industry Association, Huawei's chip production received $30 billion in state support in 2021 and 2022.[116] Although Huawei has historically lacked the capacity to export AI chips at scale, recent developments signal a shift. In July 2025, reports emerged that Huawei had worked to sell its Ascend AI 910B chips to prospective customers in Saudi Arabia, the United Arab Emirates (UAE), Thailand, and Malaysia.[117] Until July 2025, Huawei had withheld its Ascend 910B chips from export due to tight supply, prioritizing domestic customers that had been cut off from U.S. alternatives. But with Huawei's release of the more advanced Ascend 910C chip, the company is directing its 910B

The launch of both Made in China and the DSR in 2015 underscore Beijing's twin technology ambitions at home and abroad.

FIGURE 7: HUAWEI'S GOVERNMENT GRANTS[118]



This figure illustrates the surge in China's annual government grants to Huawei. State support for China's tech national champions reinforces their global competitiveness by subsidizing operations, financing research and development, and enabling aggressive pricing abroad.

stock abroad.[119] China's industrial policy has already enabled it to dominate the export of legacy chips; in time, it may achieve the same for AI chips short of the cutting edge but still valuable for most emerging market needs.

Beyond central government subsidies, Chinese provincial and city governments compete fiercely to build AI, biotechnology, and robotics hubs to attract high-tech champions.[120] Sub-national government support for AI illustrates this dynamic: dozens of provinces offer subsidized cloud credits and venture capital to attract AI start-ups.[121] Cities award contracts to AI and smart city firms to build public sector technologies, helping firms scale. In Hangzhou, the municipal government partnered with Alibaba Cloud to develop City Brain, a platform that leverages AI to ease traffic congestion and improve emergency response times.[122] These projects create a positive feedback loop of steady funding, data, and real-world application opportunities.[123] This model turns Chinese cities into test beds, allowing firms to perfect their offerings at home and then enter global markets with a competitive edge.

Subsidies, tax incentives, local pilots, and other support mechanisms provide Chinese firms with a runway to refine products before going global. By the time they enter foreign markets, many Chinese firms have already achieved scale, efficiency, and technical maturity, enabling the outward diffusion of increasingly high-quality, low-cost offerings across the globe. As those technologies encountered a rising wall of restrictions in developed markets, they flooded emerging ones.

Overseas Financing

State subsidies at home often combine with project financing abroad to hand Chinese companies even greater advantages against U.S. and allied competitors. These loans frequently come with favorable terms, such as low interest rates and generous grace periods for repayment.

As noted previously, total support from Chinese export credit agencies was 14 times the U.S. equivalent in 2022.[124] Crucially, loans from Chinese policy banks are typically "tied" loans, meaning that funds must be used to procure goods and services from Chinese firms.[125] China Exim Bank's loans typically carry requirements that at least 50 percent of the goods purchased with the loan must be procured from Chinese vendors.[126] Beijing calls these provisions "Iron Triangle" loans.[127] Although the Chinese government has since removed the relevant page, CDB's website once outlined how these Iron Triangle loans help Chinese enterprises "expand abroad" by helping overseas buyers purchase Chinese equipment, creating a positive cycle of corporate revenue and overseas expansion.[128]

In late 2021, China Exim Bank also began offering "loans for strategic emerging industries" to support a broad range of activities, including fixed asset investment, mergers, and even "daily operations."[129] By 2023, China Exim Bank had made roughly $303 billion in loans across more than 130 countries, while CDB had financed more than 1,300 BRI and DSR projects.[130] By offering complete and immediate financing, Chinese policy banks accelerate Chinese tech diffusion.

Huawei's global growth is illustrative. From 1997 to 2019, Chinese banks lent $14.8 billion for 99 Huawei projects worldwide. China Exim Bank financed 56 of these loans, while CDB financed 25.[131] Chinese export financing allowed the company to "go global" and become the behemoth it is today.

Total support from Chinese export credit agencies was 14 times the U.S. equivalent in 2022.

Chinese banks now finance next-generation projects in overseas markets, including AI-powered surveillance systems, cloud data centers, and satellite and space infrastructure. In West Africa, China Exim Bank offered a $200 million buyer credit for Ghana's Safe City to finance 8,400 AI-enabled surveillance cameras, two data centers, and an analytics platform.[132] In Kenya, a $200 million concessional loan from China Exim Bank helped build a national cloud facility, ICT network, public safety center, and government enterprise services.[133] At a 2024 meeting with African leaders, Xi committed $50 billion in loans for joint satellite and space exploration projects from 2025 to 2027.[134]

Overseas financing is fundamental to how Chinese tech firms compete abroad by allowing them to offer lower prices and enter less commercially attractive markets; combined with bundled equipment and services, their offerings become even more alluring.

Strategic Bundling

Chinese tech firms have become adept at offering bundled packages of financing, hardware, software, maintenance, and even operations that few competitors can match. Instead of single products, firms such as Huawei, ZTE, and Alibaba often provide end-to-end systems—what some have called a "digital ecosystem in

a box."[135] This dramatically simplifies procurement for foreign entities, which need only engage with a single Chinese company. A Jakarta business owner interviewed for this report put it well: China goes out of its way so that local partners can "press the easy button."[136] By contrast, securing a similar package from the United States and its allies would require engaging several companies and agencies, each with its own rules, procedures, and timelines. As China learned how to make strategic deals easier for foreign partners, Washington's bureaucracy and poor coordination have often made it harder.

The latest iteration of China's strategic bundling is its new "AI-in-a-box" offerings. Huawei and other firms bundle their AI chips, models, and software into self-contained, on-premise systems designed for immediate deployment.[137] Huawei has already partnered with more than a dozen Chinese AI start-ups to codevelop these solutions, including iFlytek, whose founder described the product as "ready to use, right out of the box."[138] Analysts estimate that the market for these all-in-one units could reach $62 billion by 2027, driven by strong global demand for turnkey AI solutions.[139]

Comprehensive packaging also helps China export smart or "safe" cities. In Ecuador, Chinese contractors helped create the national ECU-911 emergency response and video surveillance network. The system was built entirely by Chinese companies and financed by loans from Chinese state policy banks. The project now boasts 16 regional command centers linked to over 4,000 high-definition cameras, thermal imaging units, night-vision drones, and an AI-powered video analytics engine that routes evidence straight to prosecutors.[140] "The help from China is immense, and we only have words of gratitude," said former Ecuadorian president Rafael Correa.[141]

As China learned how to make strategic deals easier for foreign partners, Washington's bureaucracy and poor coordination have often made it harder.

Comprehensive packaging is not always a boon. Recipient cities do not always need the full package that Chinese vendors provide, and some installations have turned into "white elephant" investments—systems

In Quito, Ecuador, Chinese firms built and financed the city's ECU-911 command center. The project exemplifies China's strategy of exporting bundled "safe city" packages—complete systems of hardware, software, financing, and operations. (Juan Cevallos/AFP via Getty Images)

that see little use and impose unsustainable costs.[142] According to Brazilian industry experts interviewed for this project, several municipalities overcommitted to operational fees for Chinese digital projects they cannot sustain. In these cases, Chinese suppliers usually keep baseline prices intact but renegotiate contracts to add additional services such as traffic optimization, flood monitoring, and smart sewage sensors.[143] Huawei, in particular, leverages relationships with government buyers established through earlier telecom contracts to offer higher-value services like smart cities and cloud platforms.[144] These practices deepen technical dependence, reinforce ecosystem lock-in, and secure long-term revenue for Chinese vendors.[145]

Nonmarket Incentives

Nonmarket incentives provide another asymmetric advantage that allows China to secure strategic technology bids abroad. Chinese firms have been repeatedly caught offering nonmarket incentives—such as bribes, kickbacks, luxury gifts, and other inducements—to outmaneuver foreign competitors. AidData's 2022 global inventory of over 20,000 Chinese development projects found that 35 percent of BRI contracts were associated with serious violations, most commonly corruption and fraud.[146] The World Bank has also barred specific Chinese contractors from its projects over corruption. As of August 2025, 373 Chinese contractors and individuals appeared on the World Bank's Listing of Ineligible Firms and Individuals.[147]

These practices are widespread in Africa. In one survey, up to 87 percent of Chinese firms operating on the continent admitted to paying bribes to obtain operating licenses.[148] In Kenya, a prominent lawyer publicly alleged that Chinese firms "routinely offer kickbacks amounting to 10–30 percent of a contract's total value" to sway tender decisions.[149] The U.S. Trade Representative concurred in a 2024 report, stating, "U.S. firms have had very limited success bidding on Kenyan government tenders, with corruption being a significant concern."[150] In Indonesia, several interviewees noted that it is common for public officials to maintain side businesses—an arrangement that can blur the line between public duty and private interest. This environment creates openings for Chinese firms to secure favorable outcomes in formal processes, such as a successful bid or adjudication, through informal means.[151]

These tactics are not confined to emerging markets. In March 2025, Belgian prosecutors found that Huawei lobbyists had "regularly and very discretely" financed travel, gifts, and direct payments to at least 15 current or former members of the European Parliament to influence procurement and regulatory decisions that favored Huawei's cloud and 5G offerings.[152]

Unlike Chinese firms, Western companies are bound by the Organisation for Economic Co-operation and Development's Anti-Bribery Convention and the U.S. Foreign Corrupt Practices Act (FCPA). Chinese firms, unbound by similar rules, can sweeten already attractive state-subsidized deals with illicit payments and services on the side. Such practices give Chinese firms another advantage over U.S. and allied companies, especially in emerging markets with weak anticorruption frameworks. To mitigate this disadvantage, President Trump issued a controversial executive order in February 2025 pausing FCPA enforcement.[153]

Commercial Diplomacy

China's commercial diplomacy includes state efforts to support its firms overseas. The central government draws on several tools, such as trade promotion, market access support, and direct political and diplomatic engagement to identify and secure strategic deals. Beijing has perfected commercial diplomacy as an instrument of statecraft, pairing proactive diplomatic engagement with various forms of state-backed support and bundled packages from the private sector. Of course, Beijing uses carrots as well as sticks. Beijing wields incentives generously, but it has also threatened to withhold aid or financing when governments moved to exclude Chinese vendors from their networks.[154]

Today, China fields the world's largest diplomatic network. According to the Lowy Institute, Beijing surpassed Washington in 2019 and now maintains 276 embassies and consulates worldwide.[155] Meanwhile, both the size of the U.S. Foreign Service and U.S. spending on diplomacy have effectively flatlined.[156] A Kenyan business advisor interviewed for this report noted that U.S. companies "are missing out big time…the U.S. government isn't at the table in the way the Chinese government is."[157]

Beijing has perfected commercial diplomacy as an instrument of statecraft, pairing proactive diplomatic engagement with various forms of state-backed support and bundled packages from the private sector.

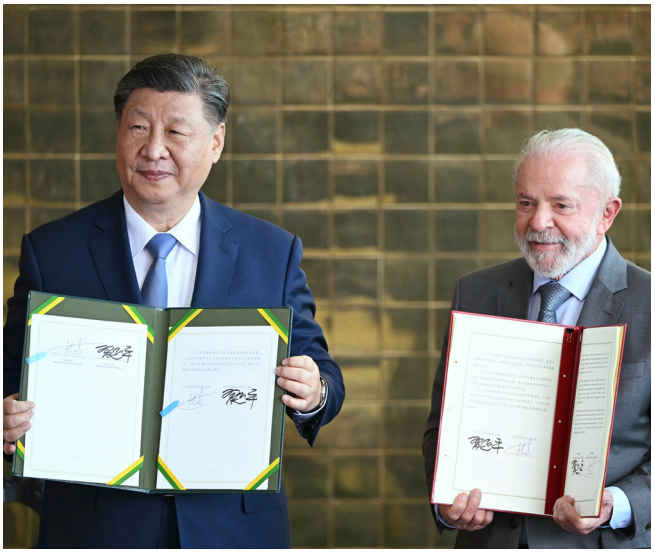
Size is only part of the difference; training and mission focus also matter. China's MOFA advertises an "urgent need for a group of outstanding science and engineering talents who are committed to the diplomatic cause."[158] In China, diplomats are specifically tested and recruited for their knowledge of science and technology and stationed abroad by China's Ministry of Science and Technology as part of its mandate to identify investment opportunities for Chinese firms.[159]

Many Chinese embassies and major consulates have a standalone Science and Technology Section (科技处), sometimes called the S&T Counsellor's Office. It is estimated that China's Ministry of Science and Technology deploys over 140 science and technology diplomats to China's S&T sections in more than 52 countries.[160] Chinese S&T diplomats have a mandate to track overseas science and technology trends, scout opportunities for Chinese investment, and expand channels for global research and development (R&D) collaboration.[161] Frontline diplomats also work hand in glove with firms, so that when a host government seeks a new data center or satellite internet provider, the local Chinese mission can quickly line up financing, technical experts, and political support.

In China, diplomats are specifically tested and recruited for their knowledge of science and technology.

In addition, top Chinese leaders provide high-level diplomatic support to advance major tech deals. This support often takes the form of government-to-government MoUs or joint statements designed to facilitate flagship investments. Huawei, for instance, regularly inks major agreements on the sidelines of Chinese presidential visits.[162]

Xi's November 2024 visit to Brasília illustrates this high-level political facilitation for technology deals. During the visit, China and Brazil signed nearly 40 cooperation agreements and pledged to identify greater synergies between the BRI and Brazil's development priorities.[163] Among them was an MoU between Brazil's state telecom company, Telebras, and Shanghai-owned SpaceSail, an LEO satellite internet provider seeking to challenge Starlink's dominance in the Brazilian market.[164] Brazil even offered up one of its military bases, the Alcântara Launch Center, to facilitate SpaceSail's equatorial launches.[165] These agreements underscore how high-level diplomacy can close strategic deals under the DSR.



Chinese Communist Party General Secretary Xi Jinping and Brazilian President Luiz Inácio Lula da Silva display bilateral agreements during a November 2024 state visit in Brasília. Xi's visit produced nearly 40 cooperation agreements, including a deal between Brazil's state telecom company and Chinese low Earth orbit satellite provider SpaceSail—illustrating how high-level diplomacy facilitates strategic technology partnerships under the DSR. (Evaristo SA/AFP via Getty Images)

By contrast, U.S. embassies often lack dedicated science and technology sections. Most American diplomats—especially in the senior foreign service—have limited technical depth, which means that opportunities to shape AI regulations or engage on issues like data localization often go unnoticed or under-resourced.[166] Part VI of this report explores gaps in U.S. commercial diplomacy in greater detail.

International Standards Setting

China has prioritized international standards setting as a strategic lever to influence how global technologies are designed, deployed, and governed. Standards make up the technical rulebook that instructs global firms on how products must operate and interconnect—the "connective tissue between technology and commerce."[167] In a 2021 CCP Central Committee document, Beijing set an ambition to lead global standards setting by 2035, naming AI as an explicit priority.[168]

Global technology standards are negotiated in committees at bodies such as the International Telecommunication Union and the 3rd Generation Partnership Project (3GPP). Beijing's strategy relies on outsized participation at these bodies: Chinese delegations fill committee seats, chair working groups, and arrive with pre-drafted text, giving them heightened influence over the final wording of standards.[169]

In 2022, Huawei alone filed more than 5,000 standards contributions and currently leads the world in declared 5G standard-essential patents.[170] Huawei's footprint dwarfs any single U.S. player. Qualcomm—the most active U.S. contributor—submitted fewer than 2,000 3GPP papers in 2022, less than half of Huawei's output. (Admittedly, Qualcomm prioritizes quality over quantity in its submissions.)[171] Qualcomm only holds 120 leadership roles across standards bodies, a mere quarter of Huawei's count.[172] When the proposals of Chinese firms prevail, their equipment often becomes the low-friction choice for global markets, providing Beijing with long-term ecosystem advantages.

If Beijing's proposed standards become the default, Chinese technologies will plug and play, while competitors face higher costs to achieve interoperability. Moreover, when a company's patented technology is written into a standard, rival manufacturers must either redesign their products or pay the patent holder a royalty. Default standards can have disproportionate effects in emerging markets, which often lack the resources or expertise to customize or adapt competing technologies. For them, Chinese systems offer turnkey solutions ready to deploy out of the box. The lower switching costs and streamlined integration make Chinese offerings the path of least resistance, driving adoption and deepening dependencies.

Tech Upskilling

Both the Chinese government and Chinese firms invest heavily in technology upskilling programs abroad. These programs not only build technical capacity but familiarity with Chinese platforms and tools. Over time, skilling programs can facilitate technological lock-in: Future entrepreneurs, officials, and IT professionals are more likely to select Chinese products they know.

Chinese firms have operationalized this strategy for years. Huawei's "Seeds for the Future" program has reportedly established over 2,600 ICT academies in more than 150 countries.[173] The company began holding 5G training sessions for Saudi officials as early as 2019 and now trains tens of thousands of ICT professionals globally.[174] Alibaba's cloud unit also hosts tech and digital skilling programs worldwide; the company claims to have trained over 60,000 students and professionals just between 2023 and 2025.[175] In Kenya, Huawei even helped coauthor the country's tech skilling playbook.[176] Officials in Indonesia interviewed for this report described hundreds, if not thousands, of young professionals traveling to China for all-expenses-paid trips to learn about Huawei's technology ecosystem.[177] Although U.S. firms like Microsoft, Cisco, and Google also offer upskilling programs abroad, they are typically smaller in scale and rarely match the free or heavily subsidized offerings of Chinese counterparts.[178]

The Chinese government also helps support upskilling by funding vocational training programs. Since 2016, China has established at least 33 "Luban Workshops" in more than two dozen countries.[179] These institutions provide instruction in fields ranging from AI to robotics, promoting technologies that China aims to export. The educational assistance is typically provided at no cost to students and, in some cases, even includes covered trips to China.[180] Teachers and alumni report that students who complete the workshops come away sold on the value of Chinese technology and, by association, develop a more favorable view of China.[181] The workshops, along with corporate training, can subtly push technologists in emerging markets toward adopting Chinese technologies.

***

In short, China wields a range of diverse and overlapping tools—from direct subsidies to indirect technology upskilling—to support its firms at virtually every stage of international expansion. To effectively counter the DSR, U.S. policymakers will need to make a more coordinated and sustained effort to support U.S. firms abroad and offer meaningful alternatives to countries adopting Chinese technologies.

V.

Domains of Competition

Domains of Competition

The United States and China compete to shape digital ecosystems across both strategic emerging markets and technology domains. U.S. and allied policymakers cannot contest China's DSR in all emerging markets, nor should they seek to counter the diffusion of all China-linked digital infrastructure and technologies. This is neither realistic nor desirable. Instead, policymakers must proceed from a sober assessment of which domains deserve prioritization.

Given limited resources, policymakers should prioritize domains with (1) an outsized effect on an emerging market's digital trajectory, (2) significant consequences to U.S. and allied interests and values, and (3) a reasonable opportunity for the United States and its allies to either match Chinese offerings or prevail outright.

Determining whether a particular domain has an outsized effect entails many factors, such as whether it requires a major long-term investment or partnership with a foreign technology company; whether it entails significant switching costs, suggesting longer-term "lock-in" dynamics; and whether it cedes control over sensitive, interconnected data and systems with implications for cybersecurity, economic and political coercion, disinformation, and techno-authoritarianism. Foundational digital infrastructure certainly falls within this category, along with digital services in the public sector that could reinforce or weaken democratic governance.

The effect of an emerging market's digital trajectory on U.S. interests and values overlaps significantly with the country's broader geostrategic importance to Washington. Countries that host significant U.S. military presence, such as the Philippines, must ensure the integrity of connected networks. Countries with disproportionate influence on regional and even international politics, such as Brazil and South Africa, also implicate U.S. and allied interests given the countries' influence in key international forums. Rapidly growing markets, such as Saudi Arabia, also represent an opportunity for the United States and its allies to deny Chinese technology firms lucrative opportunities for overseas expansion to reinvest in R&D and close technology gaps. Developing democracies, such as Kenya and Indonesia, deserve attention from Washington, lest Chinese-linked surveillance technologies undermine hard-won progress and discredit their example.

Finally, policymakers should prioritize emerging markets and technology domains where the United States and its allies have a reasonable opportunity to either match Chinese offerings or prevail outright. Limited—and even declining—federal resources to promote U.S. and allied technology abroad require prioritization to maximize impact. Doing more with less requires focusing on areas where first-mover advantages remain possible, versus more capital-intensive efforts to dislodge established Chinese vendors that enjoy the benefits of existing contracts, network effects, and technological lock-in. In domains such as electric vehicles, Chinese companies like BYD have all but cornered emerging markets, producing 60 percent of the world's electric vehicles and 80 percent of the batteries powering them.[182] In 4G and 5G, Huawei has similarly secured many emerging markets, leaving U.S. and allied vendors little choice but to prepare for the next telecommunications transition.

To be sure, even these criteria would produce a list of technology domains too long to detail comprehensively. This report suggests six priority domains that meet the above criteria and consistently surfaced in the authors' field visits to Indonesia, Kenya, Brazil, and Saudi Arabia:

1. Subsea cables
2. Next-generation telecommunications
3. LEO satellites
4. Data centers and cloud services
5. Artificial intelligence
6. Smart cities

Together, these six domains form the critical digital infrastructure and services that will decisively shape an emerging market's technology trajectory. The list is neither fixed nor exhaustive; other domains such as e-commerce, financial technology (fintech), semiconductors, and biotechnology deserve scrutiny but, in the authors' judgment, not more so than the six areas listed here.

The reasons vary. Domains such as biotechnology remain nascent in most emerging markets and could be ripe for research in the coming years. E-commerce and fintech are growing and influential in emerging markets, and the proliferation of Chinese offerings, including AliPay, WePay, and others, undoubtedly poses risks for data security and lockout for U.S. and allied firms. Still, the ability of a Chinese company to develop a detailed profile of a consumer in Indonesia does not create the same level of risk as surrendering an entire country's telecommunications network or a government data center. Access to semiconductors is, of course, foundational for any country's digital ecosystem, but not all countries require their own design, fabrication, and packaging capacity, as they do access to telecommunications, cloud services, and AI. Policymakers should still

pay attention, however, to emerging market dependence on Chinese-linked supply chains for semiconductors, as Beijing already has considerable leverage with 39 percent of global capacity for legacy chips.[183]

For each of the six priority domains, this section surveys its role and importance in a country's broader digital ecosystem, assesses the relative state of the U.S.-China competition, and offers examples of how that competition has unfolded in key emerging markets.

Subsea Cables

Subsea cables are the vital arteries of global telecommunications, carrying more than 99 percent of global dataflows within and across continents through fiber-optic cables beneath the waves.[184] No existing technology can match their bandwidth. Every day, subsea cables carry sensitive government communications, $10 trillion in transactions, and terabytes of personal and commercial data.[185] They are critical, contested, and vulnerable.

Subsea cables remain the fastest, most reliable, and most cost-effective way to convey vast quantities of data, making them essential for high-bandwidth technologies such as 5G, IoT, cloud services, and AI. Accelerating demand for these technologies in emerging markets, combined with growing interest in foreign capitals in building a more resilient telecommunications infrastructure, has led to surging demand for subsea cable infrastructure around the world.

Since 2015, the number of active and planned subsea cables worldwide has more than doubled from 299 to 650.[186] As of January 2025, active subsea cables totaled nearly 1.5 million kilometers in length—enough to circle the earth 37 times.[187] These systems range from smaller cables under 200 kilometers, which often connect different islands within a country, to systems of up to 20,000 kilometers that link continents.[188]

Four firms dominate the construction and maintenance of subsea cables, three of which are headquartered in the United States or its close allies: SubCom (United States); Nippon Electric Company, or NEC (Japan); and Alcatel Submarine Networks (France). The fourth and newest entrant is HMN Technologies, formerly Huawei Marine Networks. Since its founding in 2008, HMN Tech has become the fastest-growing builder of subsea cables in the world.[189] Between 2020 and 2024, it built nearly one in five new cables.[190]

Despite HMN Tech's rapid growth, the company has deployed just 7 percent of the total subsea cable infrastructure worldwide.[191] Analysis from TeleGeography projects that HMN Tech's global market share may shrink to just

Technicians moor the Marea subsea cable near Sopelana, Spain. Financed by Microsoft and Meta, the 6,600-km link from Virginia to Bilbao illustrates how U.S. tech firms have become key drivers of subsea cable infrastructure to expand reliable, high-speed connectivity abroad. (Ander Gillenea/AFP via Getty Images)

5 percent in the coming years, likely as a result of U.S. and allied efforts to limit its expansion.[192] Compounding Beijing's challenge, U.S. tech companies such as Amazon, Meta, Microsoft, and Google have emerged as major financiers of subsea cable infrastructure to help expand the reliable, high-speed digital connectivity abroad required for their services, and they now own or lease almost half of all subsea cable bandwidth.[193] U.S. tech companies have largely done this without support from Washington, which has only recently become more engaged in identifying and supporting strategic subsea cable projects. Part VI of this report reviews these efforts in greater detail.

Subsea cables implicate several direct security interests for the United States and its allies. As lifelines for the modern information economy, subsea cables represent a concentrated and exposed choke point for malign actors to exploit. Emerging markets often lack resilience in their subsea cable infrastructure, often relying on a handful of systems for their national connectivity, significantly exacerbating the risk. Malign actors could also compromise subsea cable landing points for espionage and data exfiltration. The risks of compromising the cable itself remain low, however, as operators would likely receive swift notice of a breach. Subsea cable data are also typically encrypted, requiring substantial—if not prohibitively difficult—decryption efforts, although cost-effective methods to do so may yet arise. Separate from concerns about espionage and exfiltration, adversaries could also cut off subsea cables entirely in a conflict to cripple a country's economy and interconnected security and defense capabilities. These obvious risks underscore the urgency of trusted vendors to build, operate, and repair these systems.[194]

Since its founding, HMN Tech has become the fastest-growing builder of subsea cables in the world. Between 2020 and 2024, it built nearly one in five new cables.

Globally, the United States and its allies are generally well positioned to prevail in the race to deploy subsea cable infrastructure around the world. Three of the four primary vendors—which command an overwhelming share of global subsea cable infrastructure—are domiciled in the United States, Japan, and France. The United States' leverage over the global financial system also gives it power to influence the risk-averse, multiparty consortia that typically finance these systems. The case of the Sea-We-Me-6 cable, detailed in Part VI, underscores how the combination of sanctions and inducements from Washington and its allies succeeded at dislodging HMN Tech from a key project. Washington has also begun to more proactively flex its tools of economic statecraft, such as the DFC and the U.S. Trade and Development Agency (USTDA), with significant opportunity to do more. Major headwinds relate principally to the relatively anemic U.S. and allied fleet of repair ships and ongoing coordination challenges in identifying and countering HMN Tech–led subsea cable projects before the company secures key bids. In addition, China's territorial claims over key subsea cable routes could allow it to delay the permitting required to lay or repair cable infrastructure. China also dominates critical upstream inputs for fiber-optic cables such as gallium and germanium.[195]

Next-Generation Telecommunications

If subsea cables form the global information highways between countries, terrestrial networks are the vital connectors within countries. They enable everything from phone calls to text messages to high-bandwidth internet access. Telecommunications networks encompass subsea cables, but they also include transmitters, receivers, and channels—wired connections like fiber-optic cables and wireless connections using electromagnetic waves such as radio frequencies—that together move information between users, countries, and continents. Unlike many other technologies, telecommunications are highly regulated at the national and international levels. International bodies set standards for each generation of wireless technology—4G, 5G, and soon 6G. The networks themselves are typically operated by state-owned or state-linked utilities. They are expensive, long-term investments, and as such, the choice of vendor can lock a country into a decade or more of path dependency.

The United States and its allies have compelling interests in ensuring that Chinese firms do not dominate global telecommunications infrastructure in key security partners. Telecom networks can carry sensitive digital activity, from government communications to prized corporate intellectual property (IP). Chinese-equipped networks therefore expand the reach of Beijing's operations for espionage, pre-positioning, and data exfiltration. Extensive Chinese-equipped networks also limit the United States' capacity to deepen economic, military, and intelligence partnerships and hand Beijing leverage over lower-income nations, which often lack the resources to pivot to more secure alternatives. Despite these risks,

telecommunications remain the DSR's most enduring success, especially in emerging markets. Today, Huawei is the world's largest supplier of telecom equipment and operates in more than 170 countries.

Five firms dominate the global construction of telecom networks. Huawei controls 31 percent of the global telecom equipment market—roughly double the share of its closest competitors Nokia (15 percent) and Ericsson (13 percent). ZTE follows with an 11 percent share, and Samsung holds 4 percent.[196] Combined, Huawei and ZTE account for more than 40 percent of the global market—which includes China's large domestic market—and their lead is only growing.[197] Meanwhile, the United States has no telecom champion making large-scale, end-to-end 5G deployments abroad, with firms like Qualcomm and Cisco instead providing specific components and services within global networks.[198]

Without a compelling alternative, the United States has struggled to blunt China's momentum. Instead, it has advocated, with limited success, for the adoption of allied alternatives—mostly from Nokia and Ericsson. Washington has also sought to rally a coalition of allies around shared concerns for trusted, "clean" networks, discussed in further detail in Part VI. These efforts arrested the momentum of Chinese telecommunications companies in many wealthy markets, but as of 2025, only 17 countries had fully banned Huawei or ZTE from their 5G networks.[200] Major economies, including Italy and Spain, continue to allow Chinesecompanies to operate as key vendors in their networks.[201] Even where bans are in place, implementation is uneven, and in many cases, countries have exempted existing Huawei contracts while barring it only from future procurement.[202]

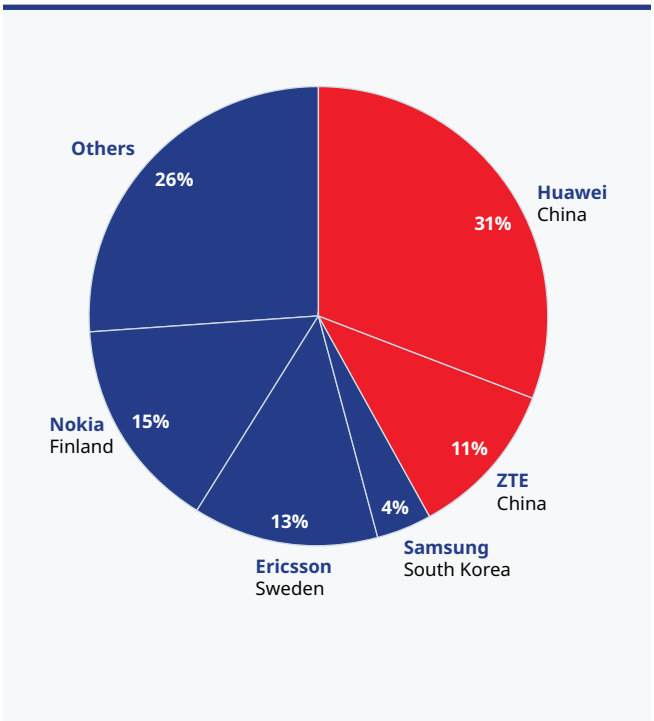
Restrictions in advanced economies have also pushed Chinese vendors to expand their efforts in emerging ones. In a late 2024 earnings call, Ericsson's CEO warned of "sharply increased competition" from Chinese vendors in Latin America, as well as Europe, and anticipated losing further deals to Huawei and ZTE on price.[203] Outside the United States and wealthier allies and partners, Chinese telecom firms remain deeply embedded in global networks.

Washington's main counteroffer—Open Radio Access Networks (Open RAN)—has yet to fill the gap, although it remains in an early phase. Unlike traditional networks, Open RAN uses standardized interfaces to allow a variety of vendors to supply different components, with the goal of reducing reliance on any one supplier.[204] Open RAN could, in theory, undercut Huawei's end-to-end dominance and offer new entry for U.S. and allied companies.[205] In practice, however, the technology faces significant technical and financial hurdles. Open RAN systems can lag in performance, are more complex to integrate, and lack the economies of scale that vendors with end-to-end offerings enjoy.[206] The 2022 CHIPS and Science Act authorized $1.5 billion to support Open RAN deployments at home and abroad through a new Public Wireless Supply Chain Innovation Fund, but commercial adoption remains slow and federal investments have principally supported domestic buildouts.[207] In July 2025, Congress rescinded $850 million from the fund, dramatically curtailing federal support for Open RAN development and deployment.

While the United States and its allies largely lost the transition to 4G and 5G in key emerging markets like Brazil and Indonesia, nearly half the world remained unconnected to 5G as of 2024, presenting an opportunity for the United States and its allies to leverage development financing to expand trusted connectivity.[208] At the same time, the United States and its allies should begin to shift its focus to 6G.

The early 6G transition is already underway, and standards, IP, and interoperability protocols remain

FIGURE 8: MARKET SHARES OF THE FIVE LARGEST GLOBAL TELECOM EQUIPMENT VENDORS[199]



The global telecom equipment market is increasingly concentrated in the hands of Chinese vendors, giving Beijing long-term leverage over countries' critical digital infrastructure.

undecided. After a surge in 5G investments from 2018 to 2022, the telecom market is now in a lull between cycles: Equipment revenues fell 5 percent in 2023 and another 8 percent in 2024.[209] As Chinese 4G and 5G infrastructure ages in key markets, governments will begin surveying options for their next-generation networks. Although the 6G transition will likely build on existing networks, proactive investment and strategy could help U.S. and allied firms position themselves now to offer secure, high-quality alternatives when countries begin the transition.

China understands the significance of the 6G transition. In 2019, Beijing set up an IMT-2030 Promotion Group to accelerate the country's R&D efforts for 6G wireless.[210] Chinese firms are now filing more 6G-related patents than any other country.[211] Huawei alone is reportedly investing billions annually in 6G research, with trials underway in advanced markets like Shanghai and Shenzhen and commercial offerings expected to roll out in the early 2030s.[212]

Advocates of 6G tout several potential benefits of the upcoming transition, including improved sensing capabilities and deep AI integration.[213] Policymakers should facilitate new capabilities while remaining clear-eyed about industry claims, especially since their most bullish claims about 5G have yet to manifest. That is not to say Washington should ignore 6G, only that it should promote it with a calibrated understanding of the stakes.

Where U.S. and allied vendors cannot match Chinese counterparts on price or deployment scale, they must compete on efficiency, quality, and trust. U.S. and allied firms like Intel, Qualcomm, Cisco, Ericsson, and NVIDIA still lead in core enabling technologies—cloud services, AI, semiconductors, and edge computing—that could become decisive in the 6G era if strategically bundled. One key advantage is real-time inference at the network's edge, which is critical for latency-sensitive applications like autonomous vehicles and industrial IoT. This dynamic plays to the strengths of U.S. companies.[214]

LEO Satellites

Communications satellites present a new frontier in global connectivity and competition. This competition now unfolds across three principal regimes: geostationary Earth orbit, middle Earth orbit, and LEO. In interviews and field research for this report, however, LEO satellites consistently emerged as the principal area of interest because of their potential to transform connectivity in emerging markets. LEO also stood out as a clear U.S. advantage to harness, given its first-mover advantages with the breakout success of Starlink.

LEO satellites operate in large constellations below 2,000 kilometers and travel at nearly 18,000 miles per hour. Their lower altitude enables relatively high-speed, low-latency communications compared with legacy satellite-based internet and bypasses the need for expensive and time-consuming terrestrial infrastructure.[215] These attributes have made LEO systems especially appealing in emerging markets, where deploying fiber-optic cables or radio towers is either impractical or cost-prohibitive.[216]

LEO satellites are poised to become a core layer of global communications. The development of direct-to-device communications means that ordinary smartphones will increasingly connect directly to satellites without the need for intermediating terminals.[217] Soon, mobile devices may toggle seamlessly between terrestrial cell towers and satellite links, making LEO infrastructure essential for uninterrupted global connectivity.[218] LEO satellites will also be essential for powering IoT-enabled smart systems. Their ability to deliver continuous low-latency connectivity in mobile and hard-to-reach environments could make them critical for autonomous vehicles, smart grids, and long-haul logistics networks.[219]

The United States has several compelling interests in maintaining leadership in LEO satellite deployment worldwide. First, LEO satellites are a core component of U.S. defense strategy, enabling resilient low-latency communications; real-time intelligence, surveillance, and reconnaissance; early missile warning; and precision navigation and timing.[220] Superiority in satellite communications can also confer key advantages on the battlefield: In Ukraine, for instance, Starlink has become indispensable for drone operations, artillery coordination, and real-time intelligence.[221]

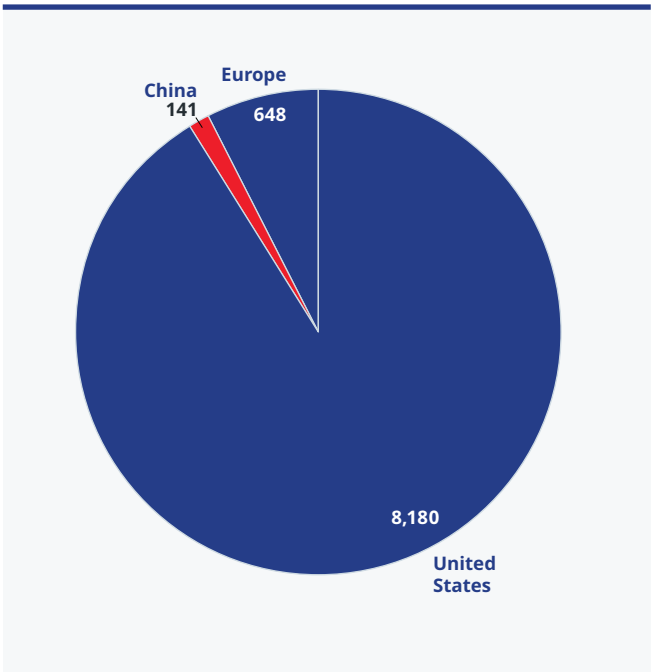
Starlink's value in Ukraine has reshaped Chinese military thinking.[222] People's Liberation Army (PLA) scientists now emphasize the need for LEO dominance and are accelerating satellite launches to prevent SpaceX from monopolizing limited "low-orbit resources."[223] A proposed constellation by PLA engineers would provide internet access, monitor rival networks, and conduct anti-Starlink operations.[224] Meanwhile, the PLA continues to develop counterspace capabilities—including anti-satellite weapons, jammers, and cybertools—to contest U.S. satellite supremacy in the Indo-Pacific.[225] If China were to surpass the United States in LEO capabilities, it could undermine U.S. advantages in intelligence collection, space-based targeting, and global command and control.[226] Maintaining a lead in LEO satellite deployment is therefore essential to ensure that U.S. forces can operate with secure, resilient communications in contested environments.

Securing the global LEO satellite market will bring significant economic benefits. The market could grow a staggering sevenfold over the next decade, rising to $108 billion.[227] Driving growth are the nearly 2.6 billion people—a third of the world's population—who still lack reliable internet access.[228] Starlink has already had to pause new enrollments in some regions as surging demand outpaces current network capacity.[229] Meeting global demand will help U.S. firms secure long-term user bases and limited "low-orbit resources" ahead of competitors.

The United States currently holds a commanding lead and first-mover advantage. Starlink alone operates approximately 7,875 active satellites, roughly two-thirds of all satellites in orbit.[230] The company claims to serve more than 6 million users across 140 countries and territories.[231] By comparison, Chinese firms likely have fewer than 800 satellites in LEO and have struggled to reliably place satellites into orbit.[232] SpaceSail, China's state-owned and leading LEO satellite firm, has a 14 percent failure rate for recent individual satellite launches; Starlink's current failure rate is under 0.5 percent.[233]

This has not deterred Chinese providers from entering the market. China's space program has the second-most satellites in orbit after the United States, although the gap remains wide. That may shift in the coming years: Goldman Sachs estimates that three-fourths of the 70,000 satellites projected to launch globally over the next five years could come from China.[235] Beijing considers itself on track to surpass the United States as the world's leading space power by 2045.[236]

FIGURE 9: TOP COUNTRIES BY LOW EARTH ORBIT SATELLITE DEPLOYMENT[234]



The United States leads the world in active low Earth orbit satellite deployment, operating more than 8,100—driven largely by Starlink—compared to 648 from Europe and approximately 141 from China.

A man lifts a Starlink satellite dish at a house in Niamey, Niger, in January 2025. With 63 percent of Africa's population still lacking internet access, Niger and other countries are turning to Starlink to bridge the continent's digital divide. (Boureima Hama/AFP via Getty Images)

Chinese firms and government actors are also working to lock in future markets through space cooperation agreements, joint ventures, and targeted commercial diplomacy. During a presentation at the 2024 Zhuhai Air Show, a SpaceSail representative presented a map highlighting six priority countries: Brazil, Uzbekistan, Kazakhstan, Pakistan, Malaysia, and Oman.[237] Since then, the company has struck MoUs and strategic partnerships with most of those countries' telecom carriers and established local R&D hubs and subsidiaries to deepen its presence.[238]

At the same time, SpaceSail is capitalizing on growing unease in emerging markets about dependence on Starlink as a long-term partner. In March 2025, Starlink founder Elon Musk threatened to revoke Ukraine's access over a critical minerals dispute, alarming other governments.[239] On the social media platform X, Musk warned that Ukraine's "entire front line would collapse if I turned [Starlink] off."[240] Starlink has also clashed with regulators in South Africa, Malaysia, Brazil, and Kazakhstan, which allege that it has failed to comply

with local regulations.[241] SpaceSail is now courting the same countries where Starlink has faced political backlash and is negotiating access agreements with more than 30 governments.[242]

At the same time, SpaceSail is capitalizing on growing unease in emerging markets about dependence on Starlink as a long-term partner.

LEO satellites are becoming a critical layer of global telecommunications infrastructure. The United States may hold a dominant position, but its lead is neither permanent nor uncontested. China is moving to close the gap with near-term plans to launch thousands of satellites and leveraging targeted diplomacy to lock in future market access.[243] Preserving U.S. leadership will require sustained public investment in resilient constellations and proactive partnerships in contested markets. Failure to act risks forfeiting leadership in a critical layer of global connectivity—and the strategic leverage that comes with it.

Data Centers and Cloud Services

Data centers are facilities that house servers to store, secure, and process data. They include enterprise data centers customized for a particular company or government agency; colocation centers for third parties to rent space for their own servers; cloud, edge, and hyperscale data centers to provide low-latency digital services; and, more recently, AI data centers to train and operate frontier models. The design, purpose, and footprint of each of these data centers may differ, but they all have become foundational digital infrastructure in the 21st century.

Historically, the United States has dominated global data center capacity. According to Synergy Research Group, as of 2024, the United States hosted 51 percent of high-powered data center capacity, measured by the actual megawatts of power used by computing equipment. Europe and China followed with 17 and 16 percent, respectively, with the rest of the world hosting 15 percent.[244]

Although the United States will likely continue to lead the world in total data center capacity in the medium term, both U.S. and Chinese hyperscalers are actively deploying data centers in emerging markets to provide low-latency services at the edge and comply with local privacy and data sovereignty laws. As these hyperscalers expand abroad, they have consolidated a growing share of global data center infrastructure. In 2025, hyperscalers operated 44 percent of global data center capacity, which could rise to 61 percent by 2030. Focusing on relative shares, however, masks a more important trend: total hyperscale data center capacity is on track to rise threefold by the end of the decade.[245] Globally, the data center market could rise from $348 billion in 2024 to $652 billion by 2030.[246]

Several dynamics are driving this surge. Chief among them is the rapid adoption of cloud, AI, and other digital services as emerging markets rapidly digitalize. In Southeast Asia, data center demand could increase threefold by 2030.[247] Many emerging markets are mirroring this trend: Saudi Arabia's data center market could triple by 2030, and Kenya's data center capacity could increase 10-fold by 2026.[248]

Another dynamic is the intensifying competition to train and deploy frontier AI models, which has injected unprecedented capital and ambition into large-scale data center buildouts. The demand flows two ways: from foreign governments and companies that need U.S. export-controlled chips and technology to realize their AI ambitions, and from U.S. companies that see lower-cost foreign markets as an opportunity to complement U.S. infrastructure and bypass domestic land, energy, and permitting bottlenecks. Nowhere is this two-way dynamic more apparent than in the Gulf, where President Trump announced major deals in May 2025 with the UAE and Saudi Arabia to strengthen the AI ecosystems in all three countries through joint partnerships and investment. Although the details of both agreements were still pending as of October 2025, the agreement with Saudi Arabia could allow NVIDIA and AMD to provide hundreds of thousands of cutting-edge AI chips to jump-start the kingdom's new AI champion, Humain.[249] Similarly, the UAE could build the largest AI cluster outside the United States, with plans for a 5 gigawatt campus spearheaded by its AI champion, G42.[250]

All of this points to a period of unprecedented data center construction around the world, creating both opportunity and risk for the United States and its allies. Partner governments that store sensitive data with a Chinese cloud service provider (CSP) like Huawei or Alibaba could be exposed to risks of espionage, data exfiltration, and IP theft.

There is also a risk of long-term lock-in. Companies or agencies that partner with foreign CSPs face high switching costs that, combined with bureaucratic inertia, are often prohibitive. This dependence could

President Trump meets with Crown Prince Mohammed bin Salman in Riyadh in May 2025. The visit featured major deals—including commitments from NVIDIA and Alphabet—that highlighted how Gulf partners are turning to U.S. firms and chips to power their AI ambitions. (Win McNamee/Getty Images)

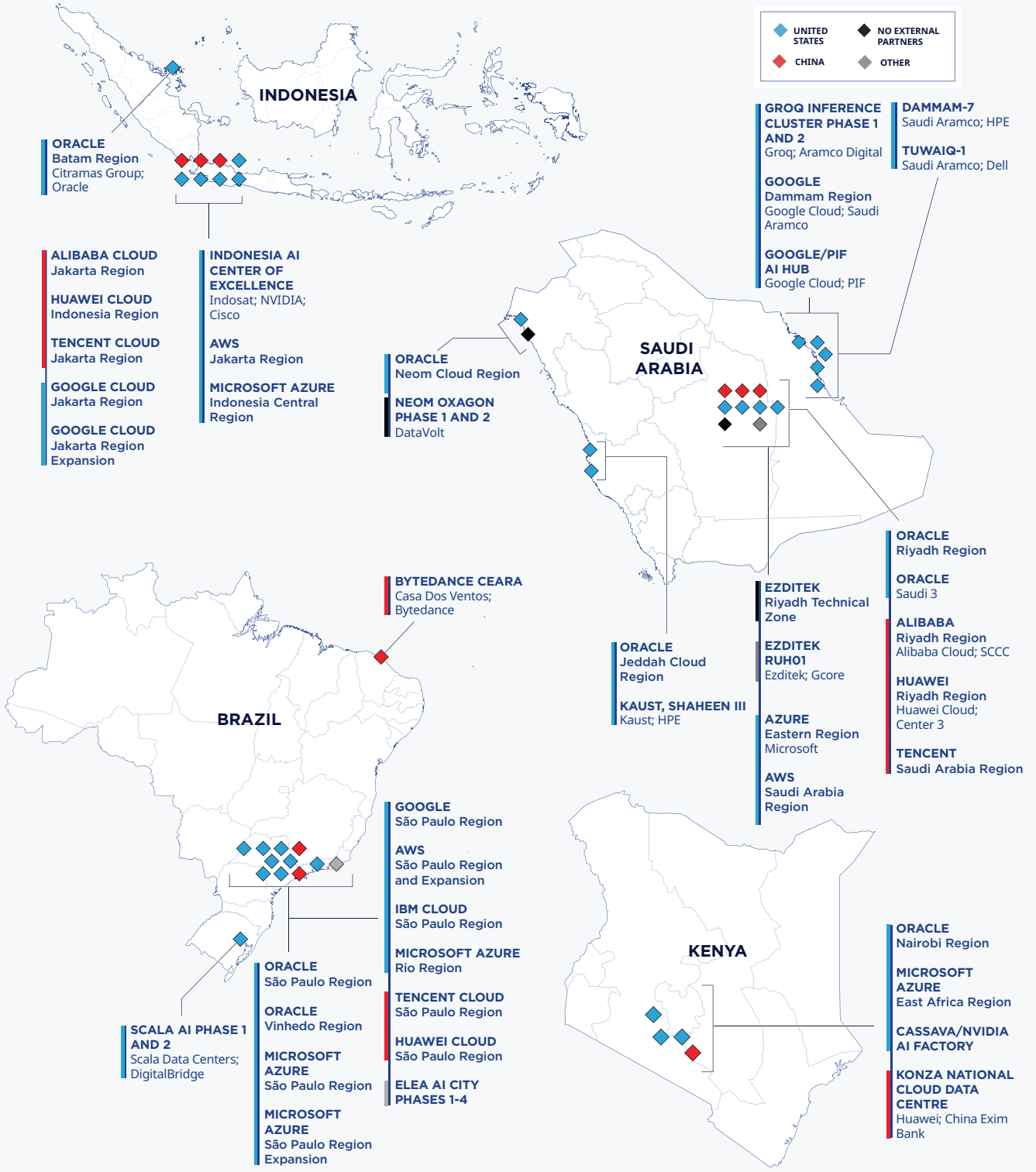
create leverage for the foreign CSP and its home government. In the case of Chinese CSPs, which have little legal recourse to resist Beijing's demands under existing national security and intelligence laws, this creates significant risks that foreign countries could have sensitive government, commercial, and other data used as leverage. This risks a new "data debt" to Beijing akin to the financial debt that it has leveraged against emerging markets following expensive infrastructure projects under the BRI.

Although Chinese hyperscalers have made concerted efforts to expand data center infrastructure abroad, U.S. companies retain a dominant position. AWS, Microsoft Azure, and Google Cloud together accounted for more than 60 percent of the global cloud market as of 2024, while Alibaba Cloud and Tencent Cloud had just 6 percent combined.[251] Admittedly, these figures include the large domestic cloud markets in both the United States and China. Compared with their Chinese counterparts, U.S. cloud service providers retain advantages in performance, premium offerings, and latency because of their broader global network and private internet backbones.[252] The global picture of U.S. cloud dominance, however, fades at the regional level. In Southeast Asia, for instance, Chinese providers command a majority of active cloud regions in Indonesia and Singapore, along with 100 percent of active cloud regions in Thailand and the Philippines.[253]

The picture appears grimmer for China's AI data center ambitions abroad. Chinese technology companies already struggle to access sufficient high-end chips for their domestic AI computing needs and have instead resorted to brute force approaches that amass lower-performing chips in lieu of cutting-edge U.S.-designed offerings. Should U.S. export controls relax, however, China may find it easier to satisfy growing domestic and global demand for its AI services.[254] As of this report's publication, however, there have been no comparable efforts by Chinese companies to replicate overseas AI compute infrastructure buildouts on the scale of the U.S.-Gulf deals announced in May 2025.

In fact, a reported Huawei effort to build AI infrastructure in Malaysia—the first example of Chinese-built AI infrastructure abroad—has all but stalled. Malaysia's deputy minister of communications had announced that the country would deploy 3,000 of Huawei's Ascend graphics processing units in the country, but that official has since retracted their remarks and the government has disavowed the project.[255] In July 2025, reports surfaced that Huawei was actively seeking to sell its

FIGURE 10: U.S. HYPERSCALERS LEAD CLOUD COMPUTING DEPLOYMENT IN KEY EMERGING MARKETS[256]



This figure compares the presence of U.S. and Chinese data centers and cloud services in Kenya, Brazil, Indonesia, and Saudi Arabia. Although U.S. firms dominate global cloud and data center capacity, Chinese providers are expanding in underserved markets and secondary cities.

legacy Ascend 910B chips to the UAE, Saudi Arabia, and Thailand, while reserving its more advanced 910C chips for Chinese companies attempting to compete with U.S. counterparts. Each of these countries has active or expanding partnerships with U.S. AI companies like NVIDIA, suggesting that Huawei is working to avoid becoming boxed out of key compute markets even as it struggles to compete under the sting of U.S. export controls.[257]

U.S. firms may have a dominant position in global cloud and data center deployment, but Chinese competitors have repeatedly shown a willingness to proactively fill gaps in underserved strategic markets, such as Mexico and Nigeria, or to serve second- or third-tier cities beyond large capitals.[258] Although the United States enjoys a 10-fold advantage over China in its total compute capacity, it would be a mistake for policymakers to assume that China cannot overcome existing hurdles to realize its AI infrastructure ambitions abroad—specifically by brute forcing domestic design, packaging, and fabrication capacity for advanced AI chips in the face of U.S. export controls.[259] Should it succeed, it would fundamentally undermine the current U.S. advantage in global data center deployment.

Artificial Intelligence

AI is the newest, most contested, and arguably most important domain of technology competition between the United States and China. In essence, AI is the application of certain technologies and techniques to enable computers to simulate human intelligence. AI can take many forms, although global attention since 2023 has focused overwhelmingly on the rapid progress of large language models (LLMs), which train on vast quantities of data to develop general-purpose capabilities. LLMs include "closed" models that do not publicize their training data or source code and "open" models that do, with gradients in between. Generally, closed models have led the frontier of AI performance according to benchmarks, and these models come almost entirely from U.S. companies, including OpenAI, Google, Anthropic, and xAI. However, the competitive landscape changes short of the frontier, where a proliferating ecosystem of open-source models has pitted Meta's Llama against several compelling Chinese alternatives from DeepSeek, Alibaba, Z.ai, and Moonshot AI.[260]

Beyond LLMs are several narrower AI applications tailored for discrete areas such as drone autonomy, logistics, predictive maintenance, advanced manufacturing, material research science, and government services, including "smart" cities detailed in the next section.[261]

If the United States has secured an early lead in LLMs, China appears to have the edge in narrower AI applications in areas such as industrial robotics and government services.[262] There is active debate about whether general-purpose LLMs will obviate the need for narrower AI models, but until then, U.S. policymakers would be wise to pursue a diversified strategy for global AI diffusion.[263]

U.S. and allied policymakers have several interests in winning the race for global AI diffusion. If subsea cables, data centers, and telecommunications are foundational digital infrastructure in the 21st century, AI is the era's foundational digital technology. The choice of partnering with a U.S. or a Chinese AI company thus carries far-reaching geostrategic implications.

Since 2023, AI models have achieved astonishing improvements in capability. Many experts now predict the arrival of artificial general intelligence within a few years, and with it, new and potentially acute risks in areas such as cybersecurity, bioweapons, and disinformation. If emerging markets develop AI ecosystems aligned with U.S. and allied companies, this will create stronger pathways for policymakers to influence the technology's responsible development and adoption abroad and limit dangerous uses from malign state and nonstate actors.[264]

As with critical digital infrastructure, data security and espionage remain serious risks from the proliferation of untrusted AI models, as they typically require access to significant and often sensitive data. AI adoption also poses similar risks of long-term dependence and lock-in, which grow if an entity hands over its data to fine-tune the AI model's application over time. Even free and low-cost AI services, such as those most popular with consumers, can reap powerful first-mover advantages by becoming the default platform of choice. The internet "browser wars" are instructive: since eclipsing Internet Explorer in 2012, Google Chrome has maintained a dominant share of global browsing despite several free alternatives.[265]

Another risk is that, unlike subsea cables, AI models do not passively convey data; they actively ingest, manage, and curate it. Partnership with a foreign AI company therefore raises concerns about not only dependency and data security, but also disinformation and manipulation. DeepSeek's AI models, for instance, have censored answers about the massacre at Tiananmen Square and the status of Taiwan.[266] In August 2025, *The New York Times* reported that the Chinese company GoLaxy had used DeepSeek to conduct disinformation campaigns in Hong Kong and Taiwan.[267] As AI platforms increasingly assume the role of search engines as curators of the modern internet, their power to shape information according to their biases could grow exponentially.

In the case of China, those biases will reflect a domestic ecosystem inflected by Beijing's authoritarian government, which has already created a vast system of technology-enabled surveillance and social control. Although U.S. AI companies are hardly perfect in this regard, they nevertheless remain bound by U.S. jurisdiction and its constitutional guarantees. U.S. and allied AI products developed in free societies are far more likely to reflect liberal values, making their dissemination around the world an important front in the broader competition between democracy and authoritarianism.[268]

Finally, quality data is an indispensable input for advanced AI training, especially as leading AI companies have effectively scraped most of the world's publicly available information. The diffusion of Chinese AI products around the world therefore confers not only conventional market advantages, but also AI-specific advantages in expanding access to novel data. If data is the new oil, technology companies that corner large markets are effectively securing the new Ghawar Fields of the 21st century AI-enabled economy.

For all these reasons, U.S. and allied policymakers have a direct and growing interest in winning the race to shape AI ecosystems in key emerging markets. With the exception of wealthy countries like Saudi Arabia and the UAE, most emerging markets are not yet in a position to train their own AI models. They lack the capital, hardware, and expertise. Instead, they seek partnerships with foreign AI companies to tailor and integrate models to suit their needs, consistent with local languages and norms. In these cases, foreign governments and companies do not always need top-of-the-line AI models; "good enough" offerings are typically sufficient, as they can deliver most of the same capabilities at lower cost.[269]

This dynamic plays directly to China's longtime advantage in offering lower-cost, tailored packages in emerging markets, as in the transition to 4G and 5G networks. China's emphasis on open-source models as an asymmetric response to U.S. dominance at the AI frontier is well suited to emerging market developers, consumers, and even companies that are more cost sensitive.[270] Moreover, Huawei and ZTE benefit from strategic partnerships with emerging market governments and national champions that they have assiduously cultivated over many years. These partnerships enable ready pathways to bundle new AI services, as they have already done in Kenya and Brazil. Ubiquitous Chinese-made smartphones from Huawei, Xiaomi, and Vivo create another powerful vector to deliver edge AI services to consumers in emerging markets across the Global South.[271]

Nevertheless, U.S. companies enjoy powerful advantages in the global AI competition. U.S. AI companies have a global reputation for technology leadership and innovation, and their models continue to top performance leaderboards.[272] ChatGPT remains, by far, the most downloaded AI platform in the world, with 910 million global downloads as of July 2025, compared to just 125 million for DeepSeek.[273] Even if Chinese AI offerings see exploding demand in emerging markets, they could struggle to meet it as they prioritize domestic needs. DeepSeek reportedly had to limit access to its model because of insufficient computing infrastructure to handle additional demand, a potential downstream effect of U.S. export controls—or a company decision to devote limited compute to internal purposes.[274] Still, Chinese firms are striking strategic partnerships where they can and recognize the importance of early presence in emerging markets. Saudi Aramco adopted DeepSeek's AI model for its data centers.[275] In January 2025, Alibaba announced that it would make its Qwen model available to global developers through an application programming interface, leveraging its data centers in key markets across Southeast Asia, Africa, and the Middle East.[276]

ChatGPT remains, by far, the most downloaded AI platform in the world, with 910 million global downloads as of July 2025, compared to just 125 million for DeepSeek.

The United States and its allies must brace for a longer-term competition to shape AI ecosystems in emerging markets and cannot rely solely on their advantages in data center infrastructure and technological innovation; they require a strategy for AI partnerships with emerging markets that reflects the imperative of cost, cultural competency, and first-mover advantages.

Smart Cities

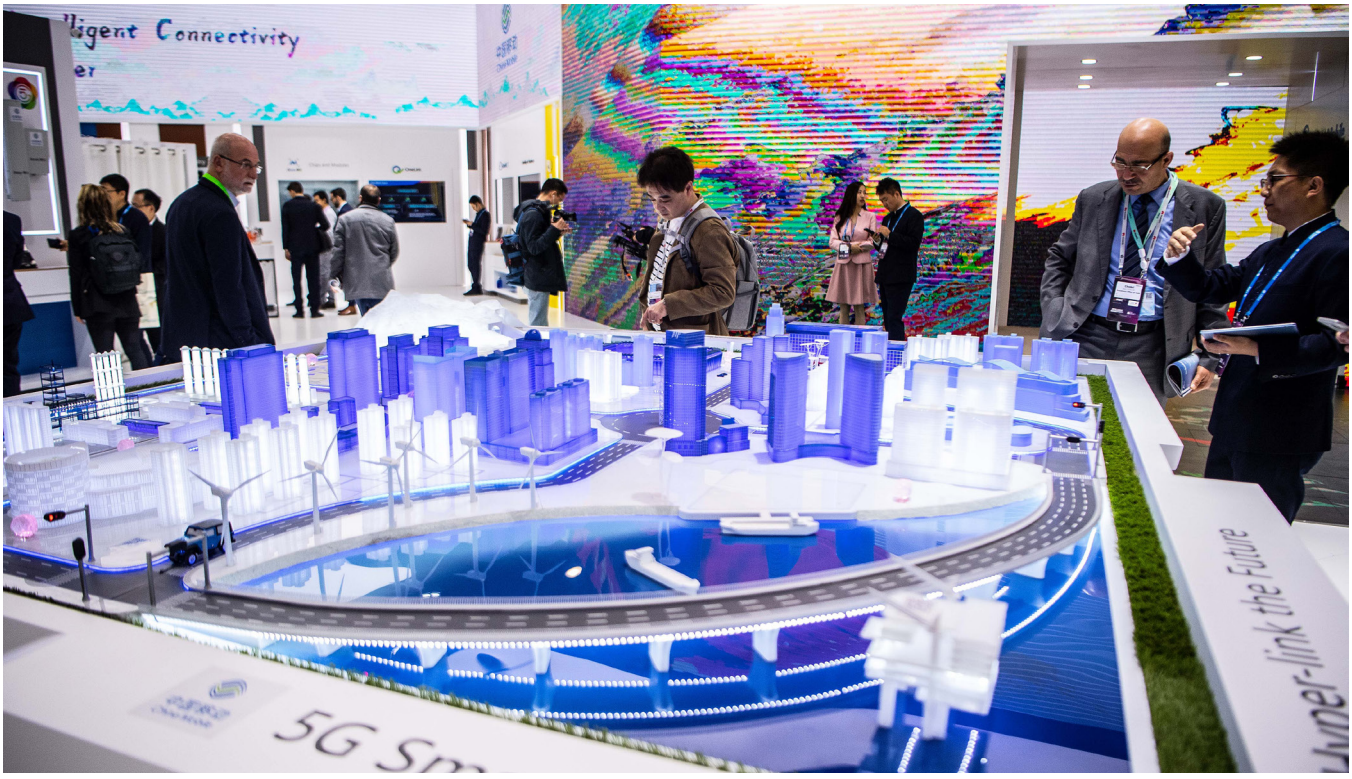
Smart cities are the places where technology and municipal management intersect. In essence, smart cities employ a range of technologies—including IoT, high-definition cameras, edge computing, and customized analytics—to improve traffic, crime, public health, energy efficiency, and more. Although the term *smart city* is often applied loosely, and the sophistication of smart cities can vary widely, governments have embraced the concept as a relatively low-cost means to address important, often underserved, public needs.

U.S. and allied policymakers have an interest in competing in the global smart city market to not only seize economic opportunity but also prevent the entrenchment of digital authoritarianism in emerging democracies. In the wrong hands, smart city technologies can enable predictive policing, mass surveillance, and Orwellian social credit scoring. As AI advances and integrates with smart city platforms, these risks may only grow absent responsible governance and democratically aligned alternatives.

Countries across the globe are embracing smart cities with zeal, and the market is expected to reach nearly $4 billion by 2030.[277] By midcentury, 70 percent of the world's population will live in cities, driving demand for technology-enabled solutions to manage growing urban populations, which increasingly strain current infrastructure, systems, and services. For cash-strapped mayors across the Global South, smart cities hold appeal as relatively low-cost "modern" solutions to reduce traffic, cut crime, improve public health, and burnish a city's reputation for innovation. But reality often falls short of these ambitions. In Kenya, for instance, Huawei claimed that its "Safe City" offerings reduced crime where it was deployed by nearly half in 2015 compared to the prior year, but the country's National Police Service reported a much smaller decline in Nairobi and a small *increase* in Mombasa.[278]

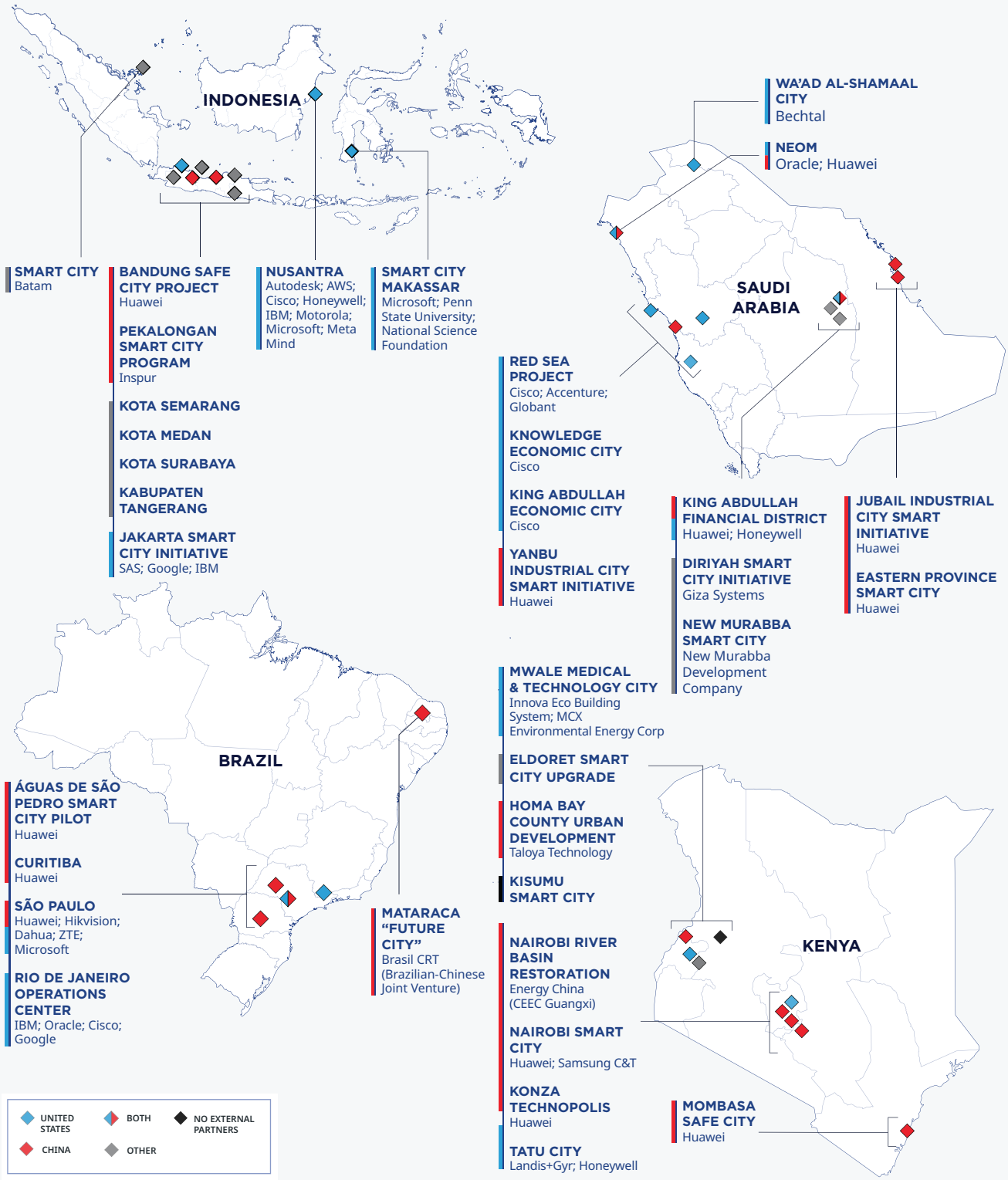
Chinese firms have dominated global smart city exports. Chinese surveillance technology operates in over 80 countries, and Chinese firms have exported smart city products and services to over 100 countries.

To date, Chinese firms have dominated global smart city exports. Chinese surveillance technology operates in over 80 countries, and Chinese firms have exported smart city products and services to over 100 countries.[279] Huawei alone has deployed its smart city services in more than 700 cities, from Barcelona to Singapore.[280] Today, Chinese companies Hikvision and Dahua represent 60 percent of global surveillance camera sales.[281]



Visitors explore a 5G smart city platform at the China Mobile booth during the 2019 Mobile World Congress in Barcelona. Smart city platforms like these are proliferating worldwide, with Chinese firms deploying them in hundreds of cities across more than 100 countries. (David Ramos/ Getty Images)

FIGURE 11: CHINESE FIRMS LEAD SMART CITY DEVELOPMENT IN KEY EMERGING MARKETS[282]



The graphics illustrate Chinese firms' modest lead in deploying smart city projects driven by bundled, state-backed packages and the leveraging of prior government contracts.

High-level political backing has propelled China's smart city expansion. President Xi has repeatedly endorsed smart city initiatives in public speeches, even placing urban internet, cloud computing, and big data infrastructure on par with roads and bridges in national urban planning.[283] Chinese policymakers view smart city construction as a core pillar of the DSR, describing it as a "strategic opportunity" for Chinese firms to expand abroad.[284]

The diffusion of Chinese-equipped smart cities also spreads Beijing's model of social and political control. Unsurprisingly, illiberal regimes are the most likely adopters: 71 percent of countries importing Huawei's Safe City platform are rated "partly free" or "not free" by Freedom House.[285] A 2025 study by the University of Southern California found that Chinese technology transfers directly enable digital repression and entrench authoritarian rule.[286]

Some emerging market governments have awoken to the risks. During Xi's 2018 visit to the Philippines, the two countries signed 29 deals, including a $400 million China Exim Bank–financed plan for Huawei to build a 12,000-camera surveillance system dubbed the "Safe Philippines Project."[287] Philippine legislators later raised alarms over data privacy and cybersecurity, citing Huawei's obligations under Beijing's 2017 National Intelligence Law. Manila scrapped the project in 2022.[288] China's success in the global competition for smart city deployment stems from its firms' ability to offer bundled packages—often backed by state financing—while drawing on prior relationships with key local players such as national telecommunications agencies and firms.

By contrast, the United States and its allies have yet to develop a comprehensive smart city alternative to compete with Chinese offerings, even as global demand grows. Efforts like the U.S.-ASEAN Smart City Partnership are promising, but their future remains tenuous under the Trump administration.[289] With that said, U.S. firms are already more active in the smart city ecosystem than many observers realize, even if they

Chinese firms have exported smart city products and services to over 100 countries. Huawei alone has deployed its smart city services in more than 700 cities, from Barcelona to Singapore.

struggle to match their Chinese counterparts' scale. IBM coined the term "smart city" in the 1990s, and Cisco and Microsoft have since developed and deployed smart city solutions for governments around the world.[290] U.S. development agencies have also supported U.S. firms competing abroad for smart city infrastructure. For example, the USTDA funded a feasibility study for smart city solutions in the planned Indonesian capital of Nusantara.[291] The grant also funded a pilot project to demonstrate technology offerings from seven U.S. companies.[292]

Parsing the smart city market is difficult, as offerings often mix U.S., Chinese, and other foreign vendors within a single platform. In Brazil, municipalities rely on local integrators for procurement, often blending Chinese hardware with software from the United States, France, Israel, or South Korea. In field research conducted for this report, the authors visited a surveillance company based in São Paolo whose cameras are made with Chinese hardware, U.S. chips, and U.S.-sourced AI software.[293] Similarly, French manufacturer Thales DIS has supplied facial recognition software to São Paulo's Civil Police and the Brazilian Federal Police, which was then integrated with Hikvision and Dahua hardware for use in border patrol and urban crime mitigation.[294]

As emerging markets build new urban digital infrastructure, the question is not whether these systems will be adopted, but whose systems will shape the underlying standards and norms. While some governments incorporate Chinese smart city technologies to consolidate

FIGURE 12: RELATIVE U.S. AND CHINESE LEAD ACROSS KEY TECHNOLOGY DOMAINS

Authors' assessment of the relative U.S. and Chinese advantages across the domains of telecommunications, smart cities, subsea cables, AI, cloud, and LEO satellites.

control, many will seek alternatives that emphasize trust, privacy, and security. If the United States wants to promote a more open and democratic digital order, it cannot cede tomorrow's smart cities to Chinese firms.

***

Stepping back, these six domains reveal a complex, interconnected, and escalating contest between the United States and China to shape the future of digital infrastructure and ecosystems in key markets around the world. In some domains, such as subsea cables, data centers, cloud services, and AI, the United States and its allies enjoy a dominant position—for now. In others, such as terrestrial telecommunications and smart cities, China has the edge.

The future of all six domains, however, remains up for grabs. Imaging that one side will "win" them all decisively is unrealistic; in reality, U.S., allied, and Chinese firms will continue to operate alongside each other around the world, often within the same networks and platforms. The goal for the United States and its allies should be to secure sufficiently strong market share to shape the trajectory of emerging nation regulators, developers, enterprises, and consumers—thereby reaping the longer-term ecosystem benefits. The recommendations in Part VIII of this report offer specific ideas to this end.

China's overwhelming success in key domains of this competition, namely telecommunications, finally forced Washington and its allies to recognize the threat and begin mobilizing a response. The next section assesses its effectiveness to date.

VI.

U.S. Efforts to Counter the Digital Silk Road

U.S. Efforts to Counter the Digital Silk Road

The United States and its allies have yet to fully mobilize their considerable advantages to offer the Global South a compelling and coherent alternative to the DSR. With that said, they have taken initial steps over the past decade to reduce the DSR's risks and seize the opportunities of a rapidly expanding global demand for digital infrastructure, services, and technology partnerships broadly.

The launch of the DSR in 2015 came at a time of growing concern in Washington about the diffusion of Chinese telecommunications infrastructure, propelled by a 2012 report from the House Permanent Select Committee on Intelligence about the risks of Huawei and ZTE to domestic telecommunications networks.[295] Even as awareness among U.S. policymakers grew, action from Congress and the Obama administration remained limited.

The First Trump Administration: The Campaign Launches

A serious U.S. campaign to restrict Chinese telecommunications equipment launched during the first Trump administration. In 2017, Congress voted to restrict Huawei and ZTE equipment from federal and defense networks.[296] In 2019, the Trump administration added Huawei to the Entity List, crippling the company's ability to transact with U.S. firms and benefit from U.S. technologies.[297] Congress followed up by passing the Secure and Trusted Communications Networks Act, which banned federal subsidies to compromised telecommunications vendors, and the Federal Communications Commission (FCC) invoked the law to target Huawei and ZTE.[298]

As Washington tightened U.S. restrictions on Huawei and ZTE at home, it increased pressure abroad on its allies and partners to follow suit. Growing U.S. pressure effectively forced foreign vendors to choose between lucrative U.S. government contracts and cheap Chinese telecommunications equipment. The Trump administration pressed its case by arguing that including Chinese telecommunications equipment in core networks threatened U.S. security and intelligence cooperation. The pressure worked for wealthier U.S. partners: Between 2018 and 2022, every member of the Five Eyes alliance moved to restrict Huawei and ZTE from their 5G networks, along with Japan, France, Sweden, and the Netherlands, although the scope and speed of the restrictions varied by country.[299] Germany became the last major European country to restrict Huawei in 2024.[300]

The first Trump administration also worked to build a multilateral, standards-based architecture to emphasize trust and security in 5G networks. A major accomplishment came in 2019 with the Prague Proposal, a set of recommendations to inform how states assess risks in building and operating 5G infrastructure.[301] Such frameworks were highly effective as they gave foreign governments—including top European and Asian allies—a less overtly geopolitical reason to restrict Huawei and ZTE equipment in their networks.

As Washington tightened U.S. restrictions on Huawei and ZTE at home, it increased pressure abroad on its allies and partners to follow suit.

Another prominent effort during the first Trump administration was the Clean Network initiative. Launched by the State Department in 2020, the initiative sought to define and disseminate standards for secure, trusted digital infrastructure and services. The initiative began with 5G networks but later expanded to include applications, app stores, cloud services, and fiber-optic

FIGURE 13: THE TRUMP ADMINISTRATION'S CLEAN NETWORK INITIATIVE[302]

CLEAN PATH

Seeks to prevent China-linked carriers from providing internal telecommunications services to and from the United States.

CLEAN CARRIER

Seeks to remove untrusted China-linked applications from U.S. mobile app stores.

CLEAN STORE

Seeks to block untrusted China-linked applications from U.S. mobile app stores.

CLEAN APPS

Seeks to prevent "trusted" U.S. and foreign apps from being pre-downloaded, or available for download.

CLEAN CLOUD

Seeks to block Chinese cloud services providers such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent from storing or processing the sensitive information of U.S. citizens and businesses.

cables—although telecommunications received the majority of government attention and resources. This was Washington's first effort to package multiple domains (5G, apps, cloud) into a coherent, branded initiative and launch a diplomatic campaign to enlist partners. With that said, disagreements within the Trump administration about the feasibility of the initiative limited its effectiveness beyond 5G.[303]

The second major accomplishment in the first Trump administration was the creation of the DFC in 2018. Unlike traditional development bodies, the DFC makes market-based investments in private sector entities to generate a return for American taxpayers while advancing humanitarian, economic development, and national security goals. The DFC has a total investment cap of $60 billion and a suite of tools to attract private capital, including the ability to make equity investments and offer debt financing, feasibility studies, and political risk insurance.[304]

A smaller but important development during this period was the State Department's creation in 2018 of Regional China Officers (RCOs), who serve as forward-deployed specialists to help diplomatic posts understand and counter China's influence on the ground.[305] As of October 25, the department had roughly 20 RCOs deployed globally, along with a four-person Office of China Coordination (known as "China House") at its headquarters in Washington.[306]

Former Secretary of State Mike Pompeo announces in April 2020 that all 5G network traffic entering and exiting U.S. diplomatic facilities must follow a "Clean Path." The announcement marked the start of a diplomatic campaign urging allies and partners to join the Clean Network Initiative and exclude Chinese 5G carriers from their networks. (Andrew Harnik/Pool/AFP via Getty Images)

Another often-overlooked success came in 2019, when the Trump administration pushed for reforms to EXIM. Unlike the DFC, EXIM is an export credit agency with a mandate to support U.S. exports and jobs, which it does through financial tools to level the playing field for American firms competing against subsidized peers from China and elsewhere.[307] EXIM has a $135 billion lending limit and tools that include direct loans, loan guarantees, and insurance to safeguard higher-risk purchases of U.S. exports. In 2019, EXIM created a new China and Transformational Exports Program (CTEP) to prioritize investments that counter Beijing's subsidies and support advanced technologies like AI and semiconductors. EXIM is now required to reserve at least 20 percent of its total support for CTEP investments.

Despite progress, EXIM faces several challenges. To be eligible for support through CTEP, at least 51 percent of the exported content must be American-made—far higher than the 20 to 30 percent domestic content requirements in competitor export credit agencies. Securing a waiver requires extensive justifications that can deter participation.[308] A requirement that any EXIM-supported goods must travel on U.S.-flag vessels also hinders participation.[309] Compounding the problem, EXIM is required to limit defaults across its total lending portfolio to less than 2 percent, fueling a risk-averse investment culture anathema to cutting-edge technologies.

The first Trump administration also sought to pursue a more integrated approach to technology statecraft within the U.S. government. The administration launched the Digital Connectivity and Cybersecurity Partnership (DCCP) in 2018 as a "whole-of-government global initiative to promote an open, interoperable, reliable, and secure internet."[310] The DCCP brought together eight federal agencies to help foreign partners adopt better cybersecurity, privacy, and regulatory approaches to promote open and secure digital infrastructure and technologies.[311] Congress formally authorized the DCCP in 2023.[312]

Congress further contributed in 2019 by creating a $300 million Countering PRC Influence Fund (CPIF) at the State Department to "expand partnerships and counter Chinese pressure globally."[313] Under the CPIF, U.S. diplomatic posts have broad flexibility to submit proposals for approval based on local conditions. Congress

funded the CPIF every subsequent year, even increasing funds to $400 million in the fiscal year 2024 funding bill.[314] The CPIF has offered the State Department a rare and agile mechanism to match Chinese-funded projects on the ground, although critics have pointed out that the fund struggles from a lack of strategic focus, spreading funds at the expense of concentrated impact, and tenuous connections for some projects to genuine counter-PRC efforts. Although the initial fund did not mention technology as an explicit focus, over time, CPIF funding has supported cyber capacity building and initiatives to promote Open RAN in emerging markets.[315]

Toward the end of the first Trump administration, the FCC moved to block the Pacific Light Cable Network, a subsea cable system between the United States and Hong Kong. This action signaled an increasingly assertive stance by the FCC against Chinese-linked digital infrastructure; the FCC has since blocked all such cables with landing points in China within its jurisdiction.[316]

The CPIF has offered the State Department a rare and agile mechanism to match Chinese-funded projects on the ground, although critics have pointed out that the fund struggles from a lack of strategic focus.

Stepping back, the first Trump administration oversaw a flurry of activity that provided an informal playbook for countering the DSR. This playbook combined new legal authorities from Congress to limit Chinese technology firms' access to U.S. and allied markets; policy tools like export controls to further squeeze those firms' access to U.S. and allied technologies; strategic investments to promote secure technologies abroad and outcompete Chinese alternatives; and diplomacy through multilateral standards setting, norm shaping, and dealmaking.

Although coordination within government and with foreign partners improved, the tools and resources remained undeveloped, under-resourced, and largely ad hoc. Still, the administration deserves credit for reversing Huawei's momentum in many developed markets across Europe, Asia, and North America and embracing a more holistic view of the threat posed by China-linked digital infrastructure, along with the necessity of a more comprehensive and agile response. Crucially, U.S. actions during this time cast a global pall over Chinese technology companies, forcing capitals and companies around the world to factor in the security and geopolitical risk of transacting with them in greater measure.

The Biden Administration: The Campaign Escalates

President Joe Biden's administration built on its predecessor's playbook with significant new restrictions on Chinese technology products, along with new resources, institutions, and coordination both at home and abroad.

Although the full spate of new restrictions against Chinese technology products during this period is beyond the scope of this report, the following are the most relevant: In October 2022, the Biden administration announced significant export controls on advanced AI chips to China, which it tightened a year later to close loopholes and add critical semiconductor fabrication equipment. In its final days, the Biden administration also released the so-called AI Diffusion Rule, which divided the world into three tiers that determined the number of advanced AI chips that countries could import. The second Trump administration rescinded the rule, promising to replace it with a "simpler" version. As of October 2025, the new rule remained pending.

The Biden administration did not limit new restrictions to chips. During this period, the FCC blocked authorization to import communications equipment from Huawei, ZTE, Hytera, Hikvision, and Dahua,

SNAPSHOT OF SUCCESS: PALAU

The first Trump administration offered an early model for partnering with key allies to promote secure digital infrastructure in third countries. The small Pacific Island nation of Palau provided an early case. With only one subsea cable connecting the island to the world, Palau faced significant risk from disruptions to the cable due to geopolitical or natural crises. At the time, HMN Tech was actively pursuing bids to expand subsea cable infrastructure in the Pacific.[317] In response, the United States partnered with Australia and Japan to assemble a $30 million investment to make sure the new ECHO subsea cable connecting the United States to Singapore included a landing point in Palau.[318] The U.S. government pitched in about $4.6 million, Australia contributed $10 million, and Japan provided a financing package.[319] The case underscored the potential of the United States and its partners to jointly deploy capital to win strategic digital infrastructure bids. At the same time, the dearth of comparable successes since then underscores the difficulty of replicating this coordination across governments.

significantly limiting new sales to the U.S. market.[320] The administration also leveraged authorities under the International Emergency Economic Powers Act to effectively ban Chinese-made electric vehicles—including their import from U.S. partners and allies—and laid the groundwork for similar action against Chinese-made drones.[321]

As Washington tightened access to the U.S. market for Chinese technology products, it expanded the institutions and resources to promote U.S. and allied alternatives. Passage of the CHIPS and Science Act in 2021 allocated $500 million over five years for the International Technology Security and Innovation Fund (ITSI), administered by the State Department, to promote secure telecommunications networks and resilient ICT and semiconductor supply chains abroad.[322] The law also provided $1.5 billion for a new Public Wireless Supply Chain Innovation Fund to scale viable U.S. and allied alternatives to China-linked telecommunications networks, such as Open RAN. (The fund was rescinded in July 2025 under the One Big Beautiful Bill Act.)[323]

Alongside new funding, the State Department created new bureaucratic capacity to elevate technology diplomacy. This culminated in the launch of a new Bureau of Cyberspace and Digital Policy (CDP) in April 2022.[324] Since its launch, CDP has played an essential role in elevating technology diplomacy within the federal government while signaling its importance to allies and partners, some of whom have since created comparable bureaus of their own. In January 2023, the State Department also established the Office of the Special Envoy for Critical and Emerging Technology (S/TECH), which the Trump administration has since shuttered as part of its departmental streamlining.[325]

Vital to any U.S. technology promotion efforts abroad are *f*rontline diplomats. The overwhelming majority of America's frontline diplomats are U.S. Foreign Service Officers, who support U.S. technology diffusion by helping to shape favorable policy and regulatory environments, negotiate bilateral trade and technology agreements, and monitor local developments to inform policy back in Washington. In 2022, the State Department took a major step by offering a new course for diplomats on Cyberspace and Digital Policy Tradecraft.[326] Still, few U.S. diplomats—and even fewer ambassadors and senior officials—have deep technology expertise. This lack of expertise means that frontline opportunities to secure key technology bids and shape emerging AI or data policies can go unnoticed or suffer from a lack of adequate staffing, resources, or depth to engage effectively. The July 2025 termination of several technology experts in S/TECH exacerbated the shortage.[327]

The State Department's elevation of technology diplomacy is overdue and unfinished. The CDP faces ongoing challenges, such as clarifying roles and responsibilities across the department—and the federal government broadly—given the crosscutting nature of cyber and technology issues.[328] Still, the elevation of the CDP as a bureau facilitated higher-level support, attention, and bureaucratic cut-through within the State Department; it has also moved Washington closer to a whole-of-government approach to cyber and digital diplomacy, although significant room for improvement remains.

Few U.S. diplomats have deep technology expertise. This lack of expertise means that frontline opportunities to secure key technology bids and shape emerging AI or data policies can go unnoticed or suffer from a lack of adequate staffing, resources, or depth to engage effectively.

The U.S. Department of Defense also began to recognize the need to support emerging technologies and critical supply chains, with semiconductor vulnerabilities prompting a broader focus on chokepoints that could undermine U.S. military capabilities and national security. In 2022, the department stood up the Office of Strategic Capital (OSC) to invest and attract capital, in partnership with the private sector, to help commercialize and scale national security–critical technologies both at home and abroad. To that end, the OSC can offer loans, loan guarantees, and technical assistance, with an initial $984 million authorized lending limit.[329] Although the OSC's initial Investment Strategy emphasizes investment in the domestic technology ecosystem, it has no statutory limitation against investing abroad. Indeed, the strategy explicitly notes the importance of strengthening the collective industrial base and competitiveness of U.S. allies and partners.[330]

The U.S. government's toolbox to counter the DSR includes a number of other agencies, programs, and initiatives. Although detailing them all is beyond the scope of this report, Figure 14 offers a high-level overview of the key U.S. agencies, along with their respective roles, tools, and resources.

FIGURE 14: AMERICA'S TOOLKIT TO COUNTER THE DIGITAL SILK ROAD[331]

Agency	Role & Tools	Resources
STATE DEPARTMENT		
Bureau of Cyberspace and Digital Policy (CDP)	Leads cyber and digital policy coordination within the State Department. *Tools:* ▪ In-house technical and policy expertise. ▪ Cyber diplomacy and technology training for foreign and civil service officers. ▪ Bilateral and multilateral cyber and digital policy dialogues. ▪ Capacity building and training on cyber attribution and responsible state behavior.	▪ No stand-alone funding; CDP's activities receive funding from the State Department's Diplomatic Programs account, which is appropriated under State, Foreign Operations, and Related Programs bill (SFOPS); in FY 2024, the State Department allocated $24 million to CDP.
Bureau of Economic and Business Affairs (EB) **Office of Development Finance** (ODF) **Infrastructure Assistance Network** (ITAN) **Transaction Advisory Fund,** managed by ODF	Leads economic policy engagement and diplomacy within the State Department. *Tools:* ▪ In-house expertise on international infrastructure financing. ▪ Capacity building for partner countries to improve their project evaluation processes. ▪ Coordination of U.S. assistance for infrastructure. ▪ Rapid response technical assistance for strategic transactions, including information and communications technology (ICT) projects. ▪ Feasibility studies, environmental and social impact studies, legal and technical reviews.	▪ No stand-alone funding; EB's activities receive funding from the State Department's annual Diplomatic Programs account, which is appropriated under SFOPS.
Countering PRC Influence Fund (CPIF)	Flexible grants for projects to counter China's global influence, with projects submitted by diplomatic posts for approval. Although there is no explicit mention of technology as a strategic focus, CPIF has supported efforts to counter the DSR—for instance, through cyber capacity building and promoting Open RAN.	▪ $325 million (FY23). ▪ Congress directed the State Department to protect $155 million for CPIF following its July 2025 rescission of bilateral economic assistance.
U.S. Foreign Service Economic Officers	Leads the State Department's efforts to "expand trade, investment, transportation, and telecommunications links." Officers advocate for free, open, interoperable, and secure digital ecosystems, liaise with foreign industry and government partners, and report on relevant policy developments abroad.	▪ ~1,500 economic officers operating in more than 190 countries and across the interagency (as of December 2020).
International Technology Security and Innovation Fund (ITSI)	Flexible grants to partner countries to promote secure ICT and chip supply chains abroad. The State Department has flexibility to allocate funding to other agencies, such as the DFC. Within the State Department, the ITSI is jointly led by the CDP, EB, and Bureau of International Security and Nonproliferation. As of October 2025, the State Department had allocated ITSI funds to at least eight countries: Costa Rica, India, Indonesia, Kenya, Mexico, Panama, the Philippines, and Vietnam.	▪ $500 million ($100 million per year through 2027).
Partnership for Global Infrastructure and Investment (PGI)	G7+ initiative to advance high-quality infrastructure in emerging markets, implicitly as a counter to the BRI and DSR. PGI enables government-to-government and government-to-business coordination across the G7, while harnessing collective capital, tools, and leverage over multilateral development banks.	▪ $60 billion mobilized (out of $600 billion committed). ▪ No dedicated U.S. funding; resources come from interagency transfers and private sector commitments.
Digital Connectivity and Cybersecurity Partnership (DCCP)	Whole-of-government effort to advance an open, interoperable, and secure internet. *Tools:* ▪ Technical assistance to partner governments. ▪ Policy and regulatory engagement. ▪ Coordination across the interagency.	▪ Congressionally authorized but lacks dedicated funding; DCCP activities receive support through SFOPS appropriations.

Agency	Role & Tools	Resources
Regional China Officers (RCOs)	Specialists placed across the department's six geographic bureaus to help assess and counter China's global influence, with substantive expertise on China. Network of RCOs can surface regional and global insights.	▪ ~20 officers (October 2025).
DEPARTMENT OF COMMERCE		
American AI Exports Program	Created by a July 2025 executive order, this program reviews, approves, and aligns federal resources to support "full-stack AI technology" export packages from industry.	▪ Funded by the Department of Commerce.
Bureau of Industry and Security (BIS)	Protects U.S. technology leadership through Export Administration Regulations, which can include bans, licensing requirements, end-use controls, and more for U.S.-origin and U.S.-linked products.	▪ $191 million (FY23).
International Trade Administration (ITA)	Strengthens global competitiveness of U.S. industry. Within the ITA, Global Markets leads the U.S. Commercial Service, a global network of trade professionals operating across 80 international markets that promotes U.S. exports, advances U.S. business interests, and attracts inbound investment. *Tools:* ▪ Customized research about a foreign market's structure, trends, practices, and key stakeholders. ▪ Various services match U.S. firms with potential foreign partners, conduct background checks on those partners, assess a U.S. firm's product viability abroad, and leverage overseas trade shows.	▪ $613 million (FY23). ▪ ~2,200 staff, ~675 of whom work in the U.S. Commercial Service. Of these, ~225 are deployed abroad.
National Institute for Standards and Technology (NIST)	NIST serves as the U.S. government's technical lead for voluntary international standards setting. Other countries adopt these standards for their own governance. Examples include NIST's Cybersecurity Framework and AI Risk Management Framework. NIST's Standardization Center of Excellence also supports U.S. engagement in international standardization for critical and emerging technologies.	▪ $172M for Standards Coordination and Special Programs (FY23), which includes international engagement. ▪ ~570 technical staff who participate in over 300 standards setting organizations.
DEPARTMENT OF DEFENSE		
Office of Strategic Capital (OSC)	Invests and attracts capital to commercialize and scale national security–critical technologies to strengthen the collective competitiveness of the United States and its allies and partners through loans, loan guarantees, and technical assistance.	▪ $984 million authorized lending limit (through FY26).
INDEPENDENT AGENCIES		
Millennium Challenge Corporation (MCC)	Independent U.S. government international development agency that enters five-year "compacts" with emerging markets that pair large-scale grants with progress in good governance and economic reform. The MCC focuses on seven core sectors: (1) agriculture; (2) education; (3) energy; (4) health; (5) land and property rights; (6) roads and transportation infrastructure; and (7) water, sanitation, and irrigation.	▪ $930 million (FY23; although reporting in July 2025 suggested the Trump administration may cancel more than half of the MCC's programs).

Agency	Role & Tools	Resources
U.S. International Development Finance Corporation (DFC)	The U.S. government's development finance institution with a twin mandate to advance U.S. foreign policy interests and economic development in emerging markets. *Tools:* ■ Debt financing through direct loans and guarantees of up to $1 billion over 25 years. ■ Equity investments, which are vital for early-stage companies and projects. ■ Investment in emerging market private equity funds. ■ Grants for feasibility studies and technical assistance to assess a project's commercial viability. ■ Political risk insurance to cover up to $1 billion of losses, as well as reinsurance to boost its underwriting capacity.	■ $60 billion cap on lending authority. ■ $983 million, including $243 million for administrative expenses.
U.S. Trade and Development Agency (USTDA)	Independent agency that supports U.S. jobs and exports for critical infrastructure projects in emerging markets, generating an average of $231 in U.S. exports for every dollar of its programs. *Tools:* ■ Feasibility studies and technical assistance to build a pipeline of bankable projects. ■ Pilot projects to adopt U.S. equipment and technology overseas to enable future scaling. ■ Training grants for local partners to offset incentives from foreign competitors that can allow them to outcompete U.S. firms. ■ Reverse trade missions that bring foreign government and business leaders to the United States to meet U.S. partners and observe offerings firsthand. ■ Industry conferences and workshops to connect U.S. and foreign firms. ■ U.S. Global Procurement Initiative to train public officials in emerging markets about procurement practices that account for a project's full life-cycle costs.	■ $87 million in FY24 ■ ~80 employees.
Export-Import Bank of the United States (EXIM)	The U.S. government's export credit agency with a mandate to support exports and jobs and level the playing field for U.S. firms. At least 20 percent of EXIM's total support must go to the China and Transformational Exports Program, which is focused on countering Beijing's subsidies and support for advanced technologies like AI, biotechnology, quantum computing, and semiconductors. *Tools:* ■ Export credit insurance to mitigate commercial and political risks for foreign sales. ■ Working capital loan guarantees to help U.S. businesses finance purchases of labor and materials for exports. ■ Financing trusted foreign purchases of U.S. goods and services through direct loans, guarantees, and insurance for their purchaser.	■ $135 billion lending cap.
U.S. Agency for International Development (USAID)	In early 2025, the Trump administration shuttered USAID. Previously, USAID provided feasibility studies, digital ecosystem country assessments, capacity building, market access support for U.S. firms, and funding to promote digital literacy, freedom, skilling, and infrastructure in emerging markets. In July 2024, USAID had outlined a 10-year Digital Policy to integrate cyber and digital issues into its work.	

Leveraging Allies and Partners

Another key initiative that emerged during the Biden administration was the Partnership on Global Infrastructure and Investment (PGI), launched in June 2023. PGI is a G7+ effort to counter the BRI by mobilizing $600 billion in global infrastructure investments, although the United States has only mobilized $60 billion to date.[332] Secure ICT is one of the PGI's four "priority pillars" for investment.[333] In November 2023, the United States hosted the PGI Indo-Pacific Economic Framework for Prosperity Forum, which resulted in several commitments to expand digital infrastructure in the Indo-Pacific, including a $600 million investment from KKR in Singtel, one of Singapore's largest data center operators, and new cloud partnerships between Google and the governments of Malaysia and Thailand. Through the PGI, the USTDA also announced feasibility studies to deploy Open RAN in Indonesia and launch the MYUS subsea cable to connect Malaysia to the United States.[334]

The Biden administration also integrated technology cooperation in key bilateral and plurilateral relationships. It especially embraced the Quad, a diplomatic partnership between the United States, Japan, India, and Australia, to promote secure and trusted technology in third countries. The Quad combines a focus on the Indo-Pacific region with formidable financial, technological, and relational assets across the four members, united by distrust of a rising China. The Quad has placed particular emphasis on promoting secure alternatives to China-linked digital infrastructure by promoting Open RAN and subsea cables, boosting cybersecurity, and enhancing cooperation on strategic technologies.

Since the Quad's launch, notable outcomes include formal partnerships on cybersecurity and subsea cables, joint principles for secure software and cybersecurity in critical infrastructure, and $20 million for an Open RAN deployment in Palau.[335] Members of the Quad also committed to deploy $50 billion in infrastructure assistance and investment in the region by 2027, but they remain far short of that goal as of September 2025.[336] A new Quad Investors Network launched in May 2023 aims to catalyze investment from member nations in critical and emerging technologies, but it also has yet to demonstrate significant progress.[337] The United States committed $5 million for a new CABLES program through its Quad partnership to provide technical assistance and capacity to boost subsea cable security.[338]

At the bilateral level, the Biden administration used technology dialogues to strengthen ties and promote trusted digital infrastructure and services, among other

(From 3rd L to R) Tanzanian Vice President Philip Isdor Mpango, Democratic Republic of the Congo President Felix Tshisekedi, U.S. president Joe Biden, Angolan President João Lourenço, and Zambian President Hakainde Hichilema attend the Lobito Corridor Trans-Africa Summit in December 2024. The railway project, a flagship of the G7's Partnership on Global Infrastructure and Investment, exemplifies Washington's most integrated effort yet to offer a strategic alternative to China's Belt and Road Initiative and the Digital Silk Road. (Andrew Caballero-Reynolds/AFP via Getty Images)

goals. The U.S.-India Initiative on Critical and Emerging Technology, for instance, laid the foundation for cooperation on secure subsea cable systems as alternatives to China-linked networks. The second Trump administration has since rebranded it as Transforming Relations Utilizing Strategic Technologies, and significant potential remains for both countries to expand cooperation in

SNAPSHOT OF SUCCESS: LOBITO CORRIDOR

The PGI's biggest—albeit tentative—success to date has been the Lobito Corridor, an 800-kilometer railway connecting Angola, Zambia, and the Democratic Republic of the Congo to increase critical mineral exports and create investment opportunities for the United States and its allies. The effort brought together multiple U.S. agencies, including the DFC, EXIM, and USAID, to mobilize $4 billion in U.S. public and private investment, reaching $6 billion with investments from other G7 countries.[339] The Lobito Corridor is perhaps the closest Washington has come to a more strategically integrated model of foreign assistance to counter China's BRI and DSR, and it offers a potentially promising model for a comprehensive approach that combines federal agencies, tools, investments, and engagement with allies. At the same time, follow-through from Washington remains essential to realizing the corridor's high ambitious.

countering the DSR—for instance, by supporting Indian-style digital public infrastructure in third countries across the Indo-Pacific and beyond.

During the Biden administration, Washington also became more aggressive in blocking specific China-linked digital infrastructure projects using carrots, sticks, and coordination with allies. In 2022, the Biden administration successfully dislodged HMN Tech from a $600 million project to construct the Sea-We-Me-6 cable connecting Singapore to France. The company had won the bid in part due to generous subsidies from Beijing. According to Reuters, the Biden administration combined credible threats with concrete incentives. On the one hand, it warned the consortium financing the cable that it planned to put HMN Tech on the Entity List, crippling its future ability to transact with U.S. firms. (It later followed through.) At the same time, it offered inducements in the form of $3.8 million in USTDA grants to foreign telecommunications companies to sweeten the deal. The consortium ultimately replaced HMN Tech with the U.S.-based SubCom.[340]

Looking back at the Biden administration, several trend lines come into focus. Export controls and other restrictions on Chinese technology firms continued to tighten, severely restricting the ability of Chinese firms to access the U.S. market and sensitive technologies. At the same time, stricter export controls on advanced AI chips and fabrication equipment required—and at times tested—the cooperation of U.S. allies such as the Netherlands and Japan. The Biden administration's restrictive measures, including the AI Diffusion Rule, also fueled doubts in key capitals and boardrooms about the reliability of long-term U.S. technology partnerships.

At the same time, the Biden administration deserves credit for creating new diplomatic capacity, investing modest but real resources through initiatives like the ITSI Fund, and proactively blocking risky Chinese infrastructure projects. With that said, most of the Biden administration's efforts could not match ambitious rhetoric with concrete, large-scale investments to truly compete with Beijing. Underscoring this, Washington has thus far failed to follow up on its success in Costa Rica with scalable offerings to meet its 5G aspirations.

All of this points to a larger and ongoing challenge, which is that Washington has found it much easier—for fiscal, political, and bureaucratic reasons—to impose unilateral restrictions on Chinese technologies rather than develop coherent and well-resourced tools to promote U.S. and allied alternatives.

Enduring Challenges

Stepping back, it is clear that the United States already has considerable tools to both counter the spread of Chinese digital infrastructure and technologies in emerging markets and promote secure and trusted alternatives. These tools apply across a continuum of engagement, from shaping entire technology ecosystems through standards setting, policy and regulatory advocacy, and workforce skilling to project identification, development, contracting, and financing. The enduring challenge remains coordination and, above all, dedicated, stable funding in the face of large-scale state support from China.

Broadly speaking, the United States has preferred to engage at the ecosystem level with efforts to promote fair, open, rules-based, and rights-respecting laws and regulations consistent with its liberal, free-market approach. The United States has generally shown less appetite for large-scale, project-specific engagement, partly due to concerns over corporate favoritism and fairness, as well as a limited resources to support such projects. China has taken the opposite tack: focusing heavily on winning specific bids and cultivating key relationships versus higher-level policy and regulatory advocacy. Both approaches have their advantages, but China's method has clearly succeeded at securing strategic projects and the longer-term lock-in they can enable.

SNAPSHOT OF SUCCESS: COSTA RICA

The United States achieved a notable success in Costa Rica, which has long served as a beachhead for Beijing in Central and Latin America.[341] Huawei largely built Costa Rica's 3G and 4G networks with the state utility, Instituto Costarricense de Electricidad (ICE). Two crippling ransomware attacks in the spring of 2022 by Conti, a Russia-linked ransomware group, brought the country's cybersecurity vulnerability to the fore, providing Washington an opening. In response, the Biden administration provided a $25 million grant to establish a new Cybersecurity Operations Center in the country, followed by a $300 million credit for ICE to buy secure 5G equipment to replace its Huawei gear.[342] In August 2023, Costa Rican president Rodrigo Chaves Robles signed a decree that effectively banned Huawei from participating in its 5G auction.[343] The United States and Costa Rica then announced a strategic partnership to promote open, secure, and reliable digital infrastructure, outlining far-reaching cooperation from cloud to cybersecurity to AI.[344]

The second Trump administration continued this momentum when Secretary of State Marco Rubio visited Costa Rica during his first official trip abroad and celebrated the country's telecommunications transition as Costa Rica's trade minister praised America's support for the country's "telecom sovereignty."[345] However, the administration's early move to suspend foreign assistance, combined with broader cuts and reorganization at the State Department, slowed U.S. funds to Costa Rica, causing frustration in San José about Washington's lack of follow-through.

This shift is welcome and overdue. However, the transition toward a more coherent U.S. approach to the global technology competition remains nascent, under-resourced, and lacking broader strategic vision. The proliferation of agencies with their own initiatives, authorities, and funding streams has some merit in that it provides the U.S. government different tools and expertise for different contexts. At the same time, it has the effect of spreading limited resources thin, diluting impact, and allowing parochial bureaucratic interests instead of strategic priorities to drive funding decisions. This ultimately undermines opportunities for coordination, consolidation, and economies of scale. In practice, this means that programs and diplomatic posts sometimes invoke China as a pretext for funding efforts they would otherwise have pursued, for instance, through CPIF.

Limited flexible funding for technology projects overseas also means that programs, diplomatic posts, and even other agencies compete intensely for resources, which can lead to the diversion of limited resources for projects disconnected from strategic objectives. All of this points to considerable opportunity to improve U.S. resources and tools to counter the DSR in terms of scale, coordination, and strategic focus.

Over the past 10 years, the United States has begun to shift its approach to balance its higher-level ecosystem engagement with more proactive, project-specific commercial diplomacy—largely in response to the success of China's BRI and DSR and the erosion of U.S. and allied market share in key sectors and markets. The second Trump administration continued this shift with its July 2025 executive order on Promoting the Export of the American AI Technology Stack. That order established a new American AI Exports Program within the Department of Commerce and empowered it to solicit and approve industry proposals for full-stack AI technology packages—an implicit counter to the bundled packages from Chinese companies that have succeeded in emerging markets. The order also empowered the Economic Diplomacy Action Group, chaired by the State Department, to align relevant federal resources to support these packages.[346]

In July 2025, President Trump signed the executive order on Promoting the Export of the American AI Technology Stack. The order established the American AI Exports Program in the Department of Commerce to promote full-stack U.S. AI technology packages abroad. (Chip Somodevilla/Getty Images)

VII.

Allied Efforts to Counter the Digital Silk Road

Allied Efforts to Counter the Digital Silk Road

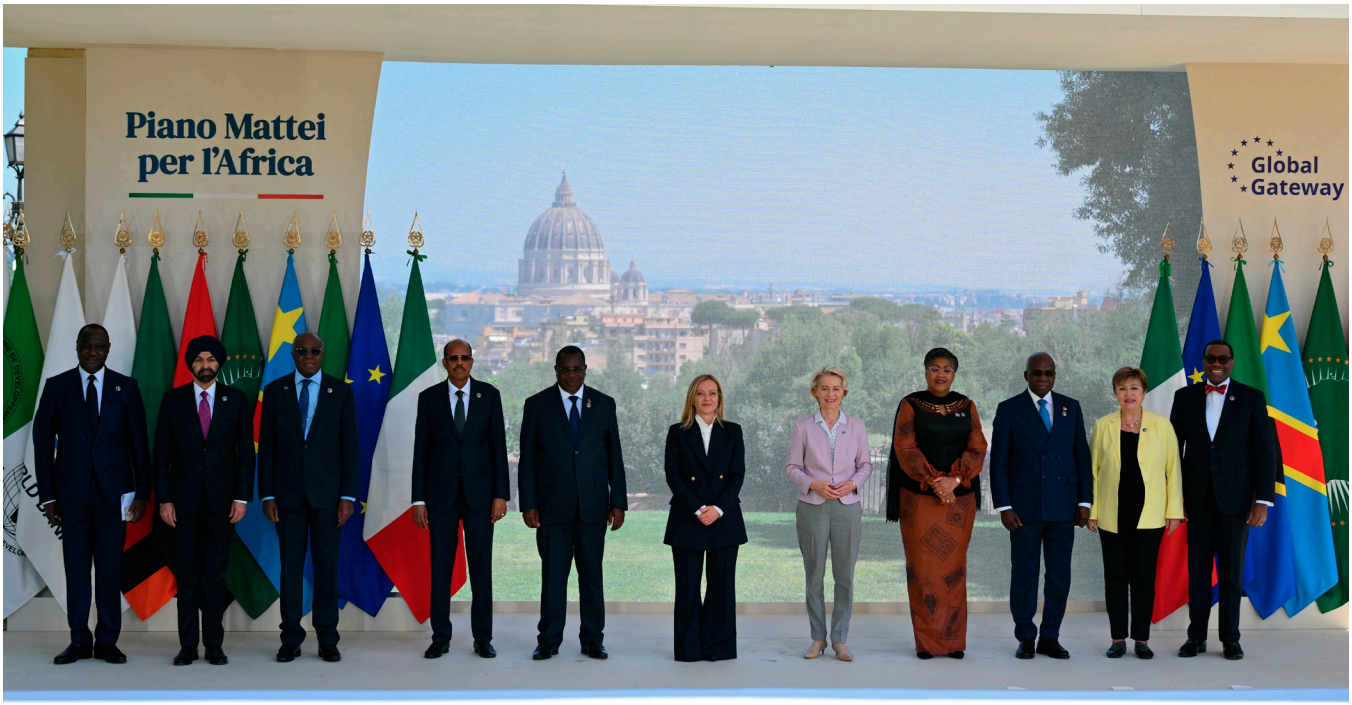
If scale determines the next phase of geopolitical competition, as it has in past contests, China's fourfold population, technological prowess, and twofold manufacturing capacity give it a formidable edge.[347] The United States cannot match China's scale on its own, but it can surely do so by working with its unrivaled network of allies and partners, which offers leadership in advanced technologies, financing, and political reach in regions where Washington has limited influence. The following section highlights the tools, authorities, and successes of key allies and partners that Washington should prioritize for cooperation in countering the DSR.

European Union

The European Union, with its 450 million residents and nearly $20 trillion GDP, is a formidable but underutilized partner in efforts to counter the DSR.[348] The first Trump administration's aggressive campaign against Huawei and ZTE combined with growing anxieties in European capitals about how China-linked infrastructure could divide the European bloc, pose security risks, and undermine industry champions like Ericsson and Nokia.

The EU began elevating digital policy and infrastructure engagement abroad accordingly. It launched the Partnership on Digital Transformation with the African Union in 2019 to promote connectivity, digital skilling, and regulatory reforms across the continent with a focus on secure, trusted digital infrastructure and services.[349] The same year, it also launched the Policy and Regulation Initiative for Digital Africa, a roughly $12 million dialogue with an emphasis on reforms for spectrum harmonization, digital transformation, and internet governance.[350] It also created the Digital for Development Hub to promote a "human-centric" vision of digital policy and governance around the world, largely through dialogues and technical assistance with specific regions abroad.[351]

The EU's signature effort came in 2021 with the launch of Global Gateway, which committed $350 billion to promote "smart, clean, and secure" infrastructure worldwide, including digital infrastructure. European Commission President Ursula von der Leyen subtly framed the effort as a counter to the BRI and DSR, declaring that it sought to "create links and not dependencies."[352] Global Gateway is a framework, not a dedicated fund, that seeks to mobilize "Team Europe"—the EU, its member states, and European multilateral development banks—to deploy funding



European and African leaders gather in Rome for the June 2025 Mattei Plan and Global Gateway summit. The meeting highlighted Global Gateway's role as the European Union's flagship $350 billion effort to offer "smart, clean, and secure" infrastructure as a strategic alternative to China's Digital Silk Road. (Alberto Pizzoli/AFP via Getty Images)

between 2021 and 2027. The effort initially focused on Africa with a roughly $175 billion package built on five pillars, including "accelerating the digital transition."[353] Signature projects include expanding subsea and terrestrial fiber buildouts, green data centers, satellite-based connectivity, and efforts to promote digital governance.[354]

The European Union, with its 450 million residents and nearly $20 trillion GDP, is a formidable but underutilized partner in efforts to counter the DSR.

Global Gateway later extended to Asia, Latin America, and the Caribbean with approximately $53 billion in additional funding.[355] This included efforts to support the 5G rollout in Costa Rica, extend connectivity to 85 percent of Colombians, boost cybersecurity in the Dominican Republic, and boost the AI ecosystem in Argentina.[356] In June 2025, the EU and India announced a partnership to promote digital services, such as digital public infrastructure, in third countries.[357]

The EU's approach combines significant investments with a heavy emphasis on sustainability, inclusion, privacy, and digital governance. The emphasis on values offers a sharp contrast with opaque BRI and DSR investments. It also creates potential tensions with the United States, which has at times bristled at Europe's efforts to diffuse its regulations for privacy and digital markets—the so-called Brussels effect—which Washington views as targeting American tech companies. Other challenges include the lack of dedicated funding for Global Gateway, which relies on the commitments of member states and European multilateral development banks, as well as perennial coordination issues for any EU-based initiative that requires member consensus. Alignment and redundancy with PGI remain another challenge, given the presence of three EU members in the G7.

Japan

Japan brings considerable assets to help counter the DSR. It is a top provider of subsea cables through NEC, and Japanese companies such as Rakuten and NEC are active in Open RAN deployments. NTT is also a global leader in smart city projects.[358] The country has a reputation for high-quality infrastructure projects and enjoys strong diplomatic relations with countries across the Indo-Pacific. Tokyo is also an active provider of grants, financing, and capacity building in the Indo-Pacific through its Official Development Assistance, managed by the Japan International Cooperation Agency.

The last decade has seen important shifts in Japan's development assistance. In 2015, Japan launched the Partnership for Quality Infrastructure as an alternative to BRI projects in the region, with $110 billion focused on Asia. The emphasis on high quality and sustainability, like the EU's Global Gateway, was an implicit alternative to BRI projects that often came with low initial costs, only to lock countries into longer-term debt and vendor dependencies. This period also saw a shift in Japan's foreign policy and development assistance in response to a deteriorating security environment and rising Chinese economic influence in the region through the BRI.[359] In 2016, Prime Minister Shinzo Abe announced the Free and Open Indo-Pacific Initiative (FOIP), which emphasized a rules-based international order, peace and stability, and economic prosperity through connectivity, including through ICT.[360]

Nevertheless, during an April 2021 visit between President Biden and Prime Minister Yoshihide Suga, the leaders announced a new U.S.-Japan Global Connectivity Partnership, in which the two countries committed to $4.5 billion in funding to strengthen digital competitiveness with investments in AI, 5G, semiconductor supply chains, and more.[361] An explicit focus of the partnerships is strengthening cooperation in third countries across the Indo-Pacific, Africa, and Latin America.[362]

As China's assertiveness in the Indo-Pacific grew, Tokyo began to shift its development assistance to better align with national and security interests. In 2023, Japan reformed its Development Cooperation Charter to make national interests an explicit objective of Official Development Assistance.[363] Japan also reformed the FOIP to include an "offer-based" approach whereby the country can proactively suggest projects in partner markets, mirroring a common tactic for BRI projects.[364] Using this approach, Japan helped finance Cambodia's national data center and diversify a telecommunications network dominated by Chinese vendors.[365]

More broadly, Japan continues to fund Open RAN deployments, cybersecurity capacity building, and digital governance consistent with its vision for a free, open, and rules-based Indo-Pacific as an implicit counter to the DSR. Japan's reputation for quality and reliability, paired with strong diplomatic relations in the region, makes it a powerful partner.

Australia

Australia has also emerged as a critical partner in efforts to counter the DSR, especially in the South Pacific.

Canberra announced the "Pacific Step-up" strategy in 2016 to significantly increase its engagement in the region, including through long-term investments.[366] In 2018, the Australian government provided approximately $92.5 million to build a new Coral Sea Cable connecting the Solomon Islands and Papua New Guinea, following news that they had reached an agreement with Huawei to build it.[367] The government also financed a new Cyber Security Center in Papua New Guinea to cultivate local talent. The government announced a new Australian Infrastructure Financing Facility for the Pacific (AIFFP) the same year to bring Pacific governments and industry together to design and deliver secure, "high-impact" projects through a mix of grants and loans.[368] As of June 2024, the initiative had delivered around $1.3 billion for 28 infrastructure projects, including the strengthening of telecommunications infrastructure—mostly subsea cables—in Tonga, Palau, Timor-Leste, Kiribati, Nauru, and the Federated States of Micronesia.[369] Canberra's focus on physical infrastructure, combined with flexible mechanisms such as AIFFP, has allowed it to offer tangible and competitive alternatives to Chinese-linked digital infrastructure in a part of the world that is too often overlooked.

Canberra's focus on physical infrastructure has allowed it to offer tangible and competitive alternatives to Chinese-linked digital infrastructure in a part of the world that is too often overlooked.

One of Australia's most important contributions over this period was driving the creation of the Trilateral Infrastructure Partnership (TIP) in 2018 between Japan, Australia, and the United States.[370] The joint effort seeks to align the project prioritization, screening, and investment of the Japan Bank for International Cooperation, the U.S. DFC, and the Australian Department of Foreign Affairs and Trade and Export Finance Australia. In essence, TIP seeks to drive joint, strategically informed investments in infrastructure projects, including digital infrastructure.[371] Since its launch, TIP has helped bring the three countries together to finance a subsea cable spur to Palau and a $95 million cable for East Micronesia.[372] In 2023, the three countries also collaborated to help Telstra, a leading Australian telecommunications company, acquire Digicel Pacific, a smaller provider serving the six Pacific nations of Papua New Guinea, Fiji, Samoa, Tonga, Vanuatu and Nauru. When Digicel Pacific went up for sale, the three nations pooled around $1.5 billion in financing to prevent its acquisition from China Telecom, complemented by loan guarantees from the DFC and Japan Bank for International Cooperation.[373]

***

Stepping back, several key U.S. allies and partners have moved toward a more security-oriented approach to development assistance in response to an increasingly assertive China. They have elevated digital infrastructure and services as a focus of external engagement and assistance. They have made strong public commitments to deploy significant capital, recognizing the gap with the BRI and DSR. They have also begun tapping bilateral and multilateral mechanisms to deploy this capital to secure strategic bids and counter the DSR.

As a result, the United States and its partners have achieved notable successes in the South Pacific, West Africa, and Central America. Still, ambitious rhetoric has outstripped committed resources, coordination remains ad hoc, and now, aspirations to deepen partnerships to promote cybersecurity, secure digital infrastructure, Open RAN, and more compete with tariffs and trade policy on the agenda. The result is considerable untapped potential to leverage the collective expertise, influence, and resources of the United States and its partners to finally offer key emerging markets a compelling alternative. Each country may struggle to match Beijing's lavish subsidies and support on their own; but they can surely do so together.

VIII.

Recommendations

Recommendations

To better counter the DSR and promote trusted U.S. and allied technologies, this report offers the following recommendations.

Strategy and Coordination

Craft a Global Technology Competition Strategy. Washington still lacks an overarching strategy to counter the DSR and promote secure and trusted alternatives, even as digital infrastructure and emerging technologies become more important and China's promotion efforts expand in emerging markets.

The White House should direct the State Department, led by the undersecretary for economic growth, energy, and the environment and the CDP, to develop a detailed strategy within a year with three primary outcomes.

First, the strategy should prioritize countries for U.S. engagement based on their importance to U.S. security and economic interests, the presence of U.S. technology firms, and their geostrategic importance.[374] Specific criteria could include the following:

SECURITY

Formal commitments

- Treaty alliance with the United States (e.g., NATO, bilateral mutual defense)
- Nonbinding defense agreement (e.g., major non-NATO ally, Defense Cooperation Agreement, Enhanced Defense Cooperation Agreement)

Operational presence

- U.S. and/or allied military bases
- Joint exercises, intelligence sharing, cyber cooperation
- Geostrategic location
- Proximity to geographic chokepoints (e.g., Strait of Malacca)

ECONOMY

Digital market

- Size, growth, and digital service adoption rate

Resources and infrastructure

- Critical minerals for tech supply chains

Investment and regulation

- Regulatory environment for digital trade and services
- Investment climate

Competitive positioning

- Penetration of Chinese tech firms
- Resilience to Chinese economic coercion
- Existing U.S. and allied tech presence

POLITICS

Governance and alignment

- Democracy or resilient emerging democracy
- Risk of democratic backsliding

Strategic influence

- Influence in regional bodies (e.g., ASEAN, Community of Latin American and Caribbean States, Gulf Cooperation Council)

Political will

- Open window to deepen U.S. cooperation
- Backlash against China (e.g., related to debt, sovereignty, territorial claims)

Second, the strategy should prioritize the most strategically vital domains of digital infrastructure, such as the six outlined in this report, with (1) an outsized effect on an emerging market's digital trajectory, (2) significant consequences to U.S. and allied interests and values, and (3) a reasonable opportunity for the United States and its allies to either match Chinese offerings or prevail outright.

Finally, the strategy should identify and align U.S. investments and other tools with these key areas and geographies accordingly. The list of priority countries and technology areas should not be long to avoid diluting impact. The July 2025 executive order on Promoting the Export of the American AI Technology Stack represented an overdue step in this direction for AI, as it called for the State Department to develop a unified strategy "to promote the export of American AI technologies and standards."[375] The administration should build on this effort for other strategic domains and, ideally, fold this effort into a broader strategy for the global technology competition.

Past efforts to direct federal agencies toward a more unified approach, such as the DCCP, either aimed too narrowly or simply rebranded existing programs. The

State Department's 2024 International Cyberspace and Digital Policy Strategy was a welcome step, but it focused on promoting "digital solidarity" through capacity building, governance, and responsible state behavior.[376] Efforts to identify priority geographies and domains of the technology competition did not always come with disciplined investment of limited resources. Indeed, the overall lack of resources remains an acute—and growing—challenge.

In developing the strategy, the administration may choose to keep its prioritization of key countries and domains private to limit diplomatic and industry pushback. However, fear of offense cannot be a reason to avoid difficult decisions about how best to target limited resources based on strategic interests.

The State Department should lead the strategy's development but consult all relevant agencies, such as the Commerce Department and the DFC. The State Department should also leverage its position as chair of the DFC Board to ensure alignment.

Establish a Strategic Competition Council. Digital infrastructure and emerging technologies are but one domain of the broader strategic competition with adversaries such as China. In fact, the crosscutting nature of technology often makes it difficult to disaggregate from other priorities such as physical infrastructure, security, and health. The challenges of countering the diffusion of Chinese technologies specifically are often true for U.S. efforts to counter Chinese influence broadly. Too often, these efforts suffer from different agencies pursuing their own mandates with their own strategies, resources, and tools. Truly integrated efforts are rare.

To address this, the White House should create an interagency Strategic Competition Council to elevate and better coordinate U.S. efforts to counter Chinese influence in strategic markets and sectors abroad, with an emphasis on digital infrastructure and emerging technologies. The council would include all relevant federal agencies and convene at least biannually to review implementation of the Global Technology Competition Strategy described earlier and identify redundant or ineffective U.S. investments and engagement. It should also contract with a private sector entity to maintain a dashboard tracking all U.S. investments and initiatives in priority countries. The Trump administration made progress in July 2025 by empowering the Economic Diplomacy Action Group to implement its executive order on global AI promotion, but it should raise its sights beyond AI.

Although working-level interagency convenings already occur ad hoc for specific projects, such as the Lobito Corridor, a White House–led Strategic Competition Council would ensure sustained, high-level prioritization across the government versus the current episodic approach, which may achieve tactical successes without advancing a broader strategic vision.

Strategic Investment

Establish a new U.S. Partnership Agency by consolidating the DFC, EXIM, USTDA, PGI, and the ITA's Global Markets and Industry & Analysis functions. Congress should pass legislation to streamline these agencies, offices, and initiatives into a single entity to align their disparate tools under a unified leadership and strategic vision to limit redundancy, maximize limited resources, and facilitate engagement by foreign governments and companies now forced to navigate a tangle of federal bureaucracy.

The U.S. government has no shortage of tools to identify, secure, and finance strategic digital infrastructure and emerging technology projects abroad. However, these tools suffer from a lack of coordination and strategic focus. As Figure 14 indicates, the ability to fund feasibility studies for digital infrastructure and technology projects resides across the State Department, DFC, and USTDA. Financing and insurance mechanisms cross the DFC and EXIM. The USTDA and ITA both offer tools to help with legal and contract-related issues to close projects. Virtually all of them offer related technical assistance. The State Department, DFC, and U.S. Commercial Service deploy officers abroad to identify, cultivate, and close strategic foreign opportunities.

Although the status quo allows for a diversity of perspectives and approaches, on balance, the costs of poor coordination, redundant investments, and diffuse impact outweigh the benefits. At the same time, consolidation should not become a pretext for slashing resources, beyond efficiencies from streamlining. This moment demands more investment in proactive commercial engagement, not less.

Alternatively, the White House and Congress should reform the DFC and EXIM for the global technology competition. The DFC and EXIM reauthorization is an opportunity to unleash both agencies' potential to promote strategic technologies and digital infrastructure abroad.

DFC—For all its promise, the DFC struggles with a lack of focus as it spreads limited financial and human resources across the globe for priorities including critical minerals, energy, farming, and financial inclusion. In part, this is often because other agencies press the DFC to make short-term, one-off investments ahead of summits and other major convenings untethered from strategic objectives. At the same time, digital infrastructure and services are not an explicit DFC focus area, and as such, related investments remain a fraction of its overall portfolio. Congress should quadruple the DFC's total lending authority to $240 billion and designate emerging technologies and digital infrastructure an explicit priority, with the specific technologies determined by the new Global Technology Competition Strategy.[377] In addition, Congress should maintain oversight of DFC investments to ensure strategic alignment and guarantee sufficient resources for expert personnel, including lawyers to vet and close transactions in a timely manner. Congress should also loosen restrictions that often block the DFC from supporting digital infrastructure projects that may incidentally benefit high-income countries. Finally, Congress should modernize how the DFC accounts for equity investments, allowing fewer dollars to go further, consistent with the Enhancing American Competitiveness Act.[378] For its part, the DFC should create an executive-level position for a chief strategic technology officer.

EXIM—Policymakers should require EXIM to allocate at least half its lending support to projects that counter China and promote advanced technologies through CTEP, far more than the current 20 percent requirement. Investments should focus on technology areas identified in the new strategy. It should also relax U.S. shipping and content requirements for CTEP investments—for instance, by permitting allied vessels and content to count—while doubling EXIM's default cap to at least 4 percent. Finally, the Trump administration should foster a more investment-driven culture to help EXIM move at the speed of business, not bureaucracy.

For both the DFC and EXIM, Congress should increase compensation for employees to attract more investment professionals and better compete with private sector opportunities.

Both approaches require strengthening and streamlining coordination with the private sector—for instance, through a new American Partnership Advisory Council—to create a shared understanding of emerging market dynamics and opportunities, as well as tools and resources available between business and government.

Review and potentially expand the ITSI Fund, administered by the State Department, which promotes secure telecommunications networks and resilient ICT and semiconductor supply chains abroad.[379] ITSI currently has $500 million in funding over five years. Before expanding funds, Congress should assess past ITSI investments for strategic impact. If Congress expands funding, it should maintain robust oversight over ITSI investments to guard against dilution of funds and diversion to nonstrategic projects. The White House and State Department should ensure that ITSI investments align with the new Global Technology Competition Strategy.

Expand and reform the Countering PRC Influence Fund. The State Department uses the CPIF to expand partnerships and counter Chinese pressure globally.[380] Congress should revise the CPIF's authorizing language to make countering the DSR an explicit priority and scale it to at least $1 billion, increasing further based on performance.[381] Congress should also designate a significant share of CPIF funds for rapid, agile investments in strategic opportunities, as determined by the undersecretary for energy, economic growth, and the environment. The undersecretary could also transfer funds to different interagency partners, such as the DFC, which may be better positioned for implementation.

Expand the USTDA's Global Procurement Initiative. The Global Procurement Initiative improves the capacity of foreign public officials to account for the full life cycle of costs, such as security, reliability, and maintenance, when making significant procurement decisions. This is not only in foreign partners' best interests, but also directly counters the tendency of Beijing-subsidized projects to provide a lower initial bid to create longer-term dependency. The USTDA initiative remains relatively small with significant opportunities for expansion.

Leverage U.S. influence over multilateral development banks to raise standards for all ICT projects. Washington should leverage its financial contributions to multilateral development banks, such as the World Bank and Inter-American Development Bank, to raise procurement standards to further emphasize quality, trust, and security, drawing where appropriate on insights from the USTDA's Global Procurement Initiative. In addition, Washington could push these banks to condition investments in emerging market ICT projects on meeting the new Digital Trust and Secure Standard or its equivalent. When ICT projects fall short, the United States should

better coordinate with allies and partners to block approval. In the past, the World Bank helped finance the acquisition of Chinese and Russian facial recognition surveillance technologies in the Brazilian state of Rio Grande do Norte.[382]

Identify and prepare for critical procurement decisions for digital infrastructure and services in priority emerging markets. The silver lining of Huawei and ZTE's success in winning the emerging market transition to 4G and 5G networks is that, in several countries, Chinese-built telecommunications networks are aging. The State Department should direct embassies to identify the life cycle of digital infrastructure, determine future procurement junctures when such infrastructure will require modernization or replacement, and work now to prepare U.S. and allied alternatives, such as Open RAN, 6G, and satellite-based connectivity. The same is true for critical transitions of major government agencies and private companies to cloud services and AI. Embassies should better anticipate and shape these decisions, which often require earlier notification and engagement from U.S. and allied companies.

Technology Diplomacy

Pilot a cohort of Foreign Technology Officers. Responsibility within the U.S. diplomatic corps for technology policy engagement abroad currently lies with economic officers who have broad responsibility for areas ranging from trade to energy and the environment. As a result, expertise in and attention for technology developments abroad often compete with other responsibilities. A pilot class of Foreign Technology Officers would receive extensive training in critical and emerging technology policy and deploy to priority posts abroad—ideally, those identified in the new Global Technology Competition Strategy.

Expand training for Cyberspace and Digital Policy Statecraft at the Foreign Service Institute. Established in 2024, this class is routinely oversubscribed. The State Department should increase course offerings to meet demand and require this training for RCOs. Personnel reductions at the department in 2025 have reportedly included staff responsible for this course; the administration should refill these roles expeditiously.

Appoint more ambassadors with leadership experience in the technology sector. Few U.S. diplomats, and especially ambassadors and senior Foreign Service Officers, have deep backgrounds in technology. The Biden administration's appointment of Meg Whitman as U.S. ambassador to Kenya is instructive. Ambassador Whitman drew on her previous experience as the CEO of Hewlett-Packard to elevate technology policy with Kenyan president William Ruto, facilitate connections with leaders in Silicon Valley, and spearhead a "tech road show" of senior Kenyan government officials to meet with leaders in Silicon Valley and other U.S. technology hubs. It is no coincidence that Microsoft and G42 announced a historic $1 billion investment in Kenya during her tenure. The administration should seek to appoint more ambassadors, ideally to the priority countries identified in the Global Technology Competition Strategy, with experience comparable to former ambassador Whitman.

Expand the number of U.S. Commercial Service Officers and DFC employees deployed abroad to increase support for U.S. technology companies to identify and secure strategic opportunities in emerging markets. The Commercial Service is a 2,200-person global network of trade specialists that focuses specifically on helping U.S. businesses successfully identify, enter, and navigate foreign markets to boost exports and support jobs back home.[383] Although most staff reside in the United States, about 225 of its members are deployed abroad across 80 countries.[384] These scant numbers mean that the Commercial Service struggles to meet demand from U.S. technology companies and potential foreign partners. The DFC has four officers for all of Asia. A U.S. Government Accountability Office report found that between 2016 and 2020, an average of just 900 U.S. personnel focused on economic and commercial diplomacy were deployed abroad.[385] Few of them have real expertise in technology.

Focus the Department of Defense's Office of Strategic Capital. OSC has a broad mandate to identify and support emerging technologies and digital infrastructure, both at home and abroad, with national security implications. This creates obvious potential for redundancy with civilian agencies, such as the DFC and State Department. The White House should ensure that OSC focuses on providing the interagency with analysis about which emerging markets deserve prioritization from the Department of Defense's perspective; otherwise, OSC should focus investments on U.S. and allied defense-relevant technologies overlooked by current

market incentives. The Defense Department is not best positioned to foster long-term strategic technology partnerships abroad, as its participation may unnerve commercial partners leery of its explicit national security mandate.

Leverage NATO member-state investment funds. Canada, Denmark, Italy, Norway, Türkiye—and perhaps soon, the United States—have sovereign wealth funds. Norway's fund is the largest in the world, with $1.8 trillion in assets.[386] NATO should convene a summit to explore opportunities for member-state sovereign wealth funds and other investment funds to support digital ecosystems in priority emerging markets—for instance, through internal reforms that require high standards of trust and security for digital infrastructure projects, incentives for co-investments with the public sector consistent with the national interest, or strengthening in-house technology expertise.

Technology Partnerships

At a time of fiscal pressure and budget cuts, Washington should pursue partnerships to leverage foreign capital and connections to emerging markets that offer robust protections for sensitive American technologies like AI.

Create a mechanism for countries to request strategic technology partnerships with the United States. Many countries still view the United States as the best partner for high-quality technology offerings. Put simply, the United States has what the world wants, from advanced chips to cloud computing to research and education. Washington should leverage this demand by creating pathways for foreign governments to request strategic technology partnerships with the United States that match their specific needs with America's tech offerings. Washington could lay out clear, broadly consistent criteria—as it did with the now-rescinded AI Diffusion Rule—as a condition for these partnerships, such as robust IP and cybersecurity protections, divestment from China-linked digital infrastructure and surveillance technologies, purchase commitments for U.S. goods and services, and even investment in the United States. In exchange, Washington would fast-track approvals and support from bodies like the new U.S. Partnership Agency (or the DFC, EXIM, and USTDA) and expand technology trade missions, research collaboration, and talent exchange. Washington should incentivize but not require cooperation from the U.S. private sector in these arrangements, for example, by whitelisting trusted technology firms and granting them bidding preference and expedited approvals under these partnerships.

Strengthen and focus the American AI Exports Program on key emerging markets. The July 2025 executive order on Promoting the Export of the American AI Technology Stack requires that industry proposals for a full-stack AI technology export package "identify specific target countries or regional blocs for export engagement."[387] Given limited capacity to review proposals, and limited federal resources to support them, the administration should focus the program on priority emerging markets. Congress should also ensure that the Department of Commerce has sufficient resources and expertise to review proposals in a timely manner.

The Economic Diplomacy Action Group empowered under the July 2025 executive order should undertake a comprehensive review of all relevant federal tools and resources—as outlined in Figure 14—to identify opportunities to streamline application procedures, requirements, and review timelines to facilitate industry participation and expedite federal support for AI export packages. Consolidating many of these tools into a new American Partnerships Agency, as outlined in an earlier recommendation, would facilitate this.

Elevate smart cities in the AI Exports Program. The Trump administration's new AI Exports Program will review industry proposals to export a "full-stack AI technology package" that must include "AI applications for specific use cases."[388] In developing the program, the administration should clarify that it will prioritize AI-enabled smart city applications that respect democratic values to jump-start the development of integrated, rights-respecting U.S. offerings able to compete with China's techno-authoritarian alternatives.

Focus coordination with allies and partners in strategic regions to maximize impact. There is opportunity for the United States to work more closely with technology-leading allies and partners to identify select "swing states" and strategic technology areas and then align investments and engagement to the maximum extent possible. All too often, the United States and its allies spread around limited investments according to their own pet priorities and programs, occasionally including them under a joint initiative that is coordinated from the outset in name only.

- *Africa and the Middle East: Leverage the European Union's Global Gateway and the UAE.* The EU's Global Gateway has already made considerable investments in subsea cables, data centers, telecommunications, and other infrastructure in sub-Saharan Africa, drawing on its historical connections to the continent. Projects include green hydrogen plants in Morocco, digital skilling in Nigeria, broadband connectivity in the Democratic Republic of the Congo, and mobile connectivity in Tanzania.[389] The United States and the EU should identify priority markets in sub-Saharan Africa and the Middle East and create a working group to coordinate strategic investments in digital infrastructure and emerging technologies.

  The UAE has extensive and growing diplomatic and commercial relations in the Middle East and sub-Saharan Africa, and Emirati companies like G42 have forged promising partnerships with U.S. companies to expand their presence in third countries such as Kenya. Emirati officials and companies can help de-risk, accelerate, and finance projects in emerging markets, clearing the way for U.S. participation. Washington should encourage partnerships similar to the $1 billion Microsoft-G42 investment in Kenya, provided they meet similar conditions for security, human rights, and IP protection. At the same time, the UAE is an imperfect partner given its close ties to China and spotty record on human rights; therefore, Washington should proceed with cautious optimism.

- *Central and Latin America: Leverage the European Union's Global Gateway.* As in Africa, the EU's Global Gateway has made considerable investments in digital infrastructure in countries such as 5G networks in Costa Rica, electric vehicle and battery production in Mexico, and green hydrogen and broadband connectivity in Colombia.[390] Washington and Brussels should focus investments in priority "swing states" and technology areas and coordinate investments and engagement accordingly.

- *Indo-Pacific: Leverage the Quad and the TIP.* Washington should identify and align common priority countries in the Indo-Pacific for engagement between the Quad and TIP. It should seek to replicate the success of cooperative efforts to dislodge HMN Tech from subsea cable projects in the region for other critical digital infrastructure projects, such as 5G/Open RAN and data centers, drawing on the formidable combination of direct investment, technical assistance, and diplomatic pressure that Washington, Canberra, and Tokyo can bring to bear. Washington should also uplift India's Digital Public Infrastructure to counter China's diffusing "smart city" surveillance technologies.

Create a U.S. Partnership Portal for both U.S. and foreign companies, universities, and research institutions to harness existing U.S. government tools and resources. Today, a U.S. company or potential foreign counterpart seeking clarity on U.S. government resources may interact with myriad U.S. personnel from the State Department, Commerce Department, DFC, EXIM, USTDA, and MCC, to name just a few. The White House should create a single point of entry—ideally, within the proposed U.S. Partnership Agency—where U.S. companies and foreign counterparts could access all the relevant resources and personnel instead of navigating the labyrinthine bureaucracy on their own.

Revive Digital Ecosystem Country Assessments. Before its closure, USAID conducted in-depth assessments of an emerging market's digital ecosystem to identify risks, gaps, and opportunities for U.S. government and private sector engagement.[391] These assessments are vital to targeting U.S. public and private sector engagement effectively. The White House should revive this tool and locate it within the new U.S. Partnership Agency or the State Department's CDP.

IX.

Conclusion

Conclusion

A decade after the DSR's launch, the initiative is at once less visible and more important than ever. Under Western pressure and growing skepticism, the DSR has receded as a high-profile, state-affiliated campaign. References in official policy documents have declined, and Chinese officials and companies rarely tout ties to the DSR in public statements. At the same time, the DSR's underlying ambition—harnessing technology to strengthen Beijing's ties to the world—has never been more vital to China's economic and foreign policy ambitions.

Rapid digitalization across the world has created historic opportunity for Chinese companies, especially in emerging markets. Rapid advances in AI, LEO satellites, and other technologies have raised the geopolitical stakes for technology leadership. Officials in both Beijing and Washington recognize the importance of not only developing cutting-edge technologies but diffusing them across the globe.

Rising opportunity drives the DSR, but so does necessity. High youth unemployment, declining foreign investment, and longer-term structural issues within China's economy have combined with rising export controls, investment restrictions, product bans, and broad-based tariffs to create significant headwinds for its tech sector at the very moment technology has moved to the center of Beijing's broader ambitions and the U.S.-China competition. Recognizing this, Beijing has doubled down on a full spectrum of state support to help its technology companies innovate, iterate, and build at home so they can compete and scale abroad. Cut off from many wealthier markets, Chinese technology companies have redoubled their efforts in emerging ones as a source of revenue to reinvest and keep pace with Western counterparts. In short, Beijing may no longer tout these efforts as building the DSR, but it expands nonetheless.

The United States and its allies have awoken, slowly, to the DSR's intertwined commercial, security, and governance threats. They have intensified efforts to counter it, from launching the PGI through the G7 to match Beijing's state subsidies to leveraging the Quad and the TIP to block Chinese-linked subsea cable and telecommunications infrastructure in the Pacific. In Washington, administrations of both parties have begun overdue reforms to the offices, authorities, and tools required to offer the world an alternative. The U.S. State Department has elevated technology as a priority; the DFC and USTDA have increased support and coordination for ICT infrastructure; and EXIM has new authorities to promote strategic technology exports focused on countering China. This is welcome, overdue, and woefully insufficient. Dedicated, stable funding to close the gap with China's generous state support remains scant as the Trump administration pares back foreign assistance and the expert personnel.

More broadly, Washington continues to over-rely on protective tools, principally through increased controls on investments and exports of sensitive technologies.[392] If Washington has shown great appetite for protecting American technology—with good reason—it has yet to produce an equally ambitious agenda to promote it.

It has little time to waste. To consider the stakes of the accelerating U.S.-China technology competition, imagine a world in which Beijing underwrote the global financial system over the past century instead of the United States. Consider a new century in which the nexus of digital infrastructure and dataflows runs through the CCP, instead of the world's democracies. Picture emerging democracies suffocated by advanced technologies for mass surveillance and social control perfected in China's totalitarian test bed.

The stakes may be great in the unfolding technology competition around the world, but so is America's hand. The United States now occupies a dominant position in AI, cloud services, and LEO satellites.[393] All the top hyperscalers and frontier AI companies are American. Three of the top four subsea cable companies are from the United States and its allies.[394]

Despite these advantages, success in the global technology competition is far from assured. From chips to telecommunications to biotechnology, China has consistently closed gaps that were once thought insurmountable. All of this invites the question: How should America and its allies use this potentially fleeting moment of technological advantage to secure key markets abroad, break the grip of China's DSR, and draw the world toward a more free, open, and secure digital future?

More immediately, as the Trump administration considers a replacement for the AI Diffusion Rule, it should raise its sights and offer the world not only a framework to access cutting-edge AI chips, but advanced technologies more broadly to draw them into America's technology ecosystem. The administration should also recognize that it cannot credibly persuade emerging markets to care about exposure to Beijing's leverage through its DSR as it exploits its own economic leverage over friends and allies with volatile tariff policy. Long-term technology partnerships require a broader foundation of bilateral trust and stability that recent trade and tariff policies risk undermining.

At home, the United States must also double down on the bedrock of its global appeal as a technology partner: cutting-edge innovation. The world wants American technology because it is often the best, born of an unrivaled ecosystem that combines top global talent and research institutions, dynamic capital markets, strong IP protections, and an entrepreneurial culture. No plan or program from Washington can replace the allure of American innovation as a driver of global demand, although it can certainly undermine it.

At the same time, the lesson of the 5G race is that market forces alone cannot assure the global spread of U.S. and allied tech in key emerging markets—especially as China redoubles state support for strategic technologies. Lower-cost Chinese technology offerings, backed by generous state support, often prevail over more expensive, secure alternatives. The answer is not to mirror Beijing's government-driven approach, but to level up Washington's statecraft for a new era of great power technology competition.

1. "Xi Urges Continuous Efforts to Promote High-Quality BRI Development," Xinhua News Agency, November 21, 2021, http://en.cidca.gov.cn/2021-11/21/c_685270.htm.

2. Mark Kennedy, "Reauthorizing DFC in Lame Duck Period Avoids Disrupting an Important Foreign Policy Tool," Wilson Center, November 20, 2024, https://www.wilsoncenter.org/article/reauthorizing-dfc-lame-duck-period-avoids-disrupting-important-foreign-policy-tool.

3. Enhancing American Competitiveness Act of 2023, S. 3005, 118th Congress (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3005.

4. "The U.S. Department of State International Technology Security and Innovation Fund," U.S. Department of State, accessed September 11, 2025, https://www.state.gov/the-u-s-department-of-state-international-technology-security-and-innovation-fund/.

5. *Review of the Fiscal Year 2024 United States Agency for International Development Budget: Hearing before the U.S. Senate Committee on Foreign Relations*, 118th Congress, April 26, 2023, https://www.govinfo.gov/content/pkg/CHRG-118shrg53434/html/CHRG-118shrg53434.htm.

6. "The Fund's Value," Norges Bank Investment Management, August 21, 2019, https://www.nbim.no/en/.

7. "What Is a DECA?" Digital Development, accessed September 11, 2025, https://www.digitaldevelopment.org/about/what-is-deca/.

8. Vivek Chilukuri and Ruby Scanlon, "Countering the Digital Silk Road: Indonesia," Center for a New American Security, March 20, 2025, https://www.cnas.org/publications/reports/countering-the-digital-silk-road-indonesia.

9. "Saudi Data & AI Authority and Vision 2030," Saudi Data & AI Authority, accessed September 11, 2025, https://sdaia.gov.sa/en/SDAIA/SdaiaStrategies/Pages/sdaiaAnd2030Vision.aspx.

10. Jane Munga, "A New Chapter in U.S.-Kenya Relations Links Silicon Valley and Silicon Savannah," Carnegie Endowment for International Peace, June 13, 2024, https://carnegieendowment.org/emissary/2024/06/kenya-us-tech-cooperation-silicon-savannah?lang=en.

11. Richard Fontaine and Gibbs McKinley, "Global Swing States and the New Great Power Competition," Center for a New American Security, June 26, 2025, https://www.cnas.org/publications/reports/global-swing-states-and-the-new-great-power-competition.

12. "Microsoft Corporation," Bull Fincher, accessed September 11, 2025, https://bullfincher.io/companies/microsoft-corporation/revenue-by-geography; "Alphabet Global Revenue by Region (2024)," Voronoi, April 30, 2025, https://www.voronoiapp.com/markets/-Alphabet-Global-Revenue-by-Region-2024-4902.

13. Jonathan E. Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities,'" Center for Strategic and International Studies, November 4, 2019, https://www.csis.org/analysis/watching-huaweis-safe-cities.

14. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (Summer 2019): 42–79, https://doi.org/10.1162/isec_a_00351.

15. Chilukuri and Scanlon, "Countering the Digital Silk Road: Indonesia"; Ruby Scanlon and Bill Drexel, "Countering the Digital Silk Road: Brazil," Center for a New American Security, April 24, 2025, https://www.cnas.org/publications/reports/countering-the-digital-silk-road-brazil; and Vivek Chilukuri and Ruby Scanlon, "Countering the Digital Silk Road: Kenya," Center for a New American Security, July 22, 2025, https://www.cnas.org/publications/reports/countering-the-digital-silk-road-kenya.

16. "Mobile Network Usage in Latin America: Current Data Traffic and Forecasts to 2030," GMSA Intelligence, October 7, 2024, https://www.gsma.com/about-us/regions/latin-america/wp-content/uploads/2024/10/Mobile-network-usage-in-Latin-America-ENG-version-3-FINAL.pdf.

17. Gabriela Valente, "Brazil Bets Big on AI Infrastructure," Ion Analytics, June 6, 2025, https://ionanalytics.com/insights/infralogic/brazil-bets-big-on-ai-infrastructure.

18. "Middle East Data Center Market Landscape 2024–2029: Increase in Usage of Inexhaustible Green Energy Sources, 5G Deployments & Edge Facilities Gaining Momentum," Global Newswire, June 20, 2024, https://www.globenewswire.com/news-release/2024/06/20/2901479/0/en/Middle-East-Data-Center-Market-Landscape-2024-2029-Increase-in-Usage-of-Inexhaustible-Green-Energy-Sources-5G-Deployments-Edge-Facilities-Gaining-Momentum.html.

19. Sapna Chadha, "How Southeast Asia Can Become a $1 Trillion Digital Economy," World Economic Forum, December 12, 2023, https://www.weforum.org/stories/2023/12/how-southeast-asia-can-become-trillion-digital-economy/.

20. Declan Walsh and Hannah Reyes Morales, "The World Is Becoming More African," *The New York Times*, October 28, 2023, https://www.nytimes.com/interactive/2023/10/28/world/africa/africa-youth-population.html; "Africa's Digital Economy to Reach $712bn by 2050," CNBC Africa, June 9, 2022, https://www.cnbcafrica.com/media/6307527595112/africas-digital-economy-to-reach-712bn-by-2050/.

21. "Why Africa, Why Kenya?—Ambassador Whitman AmCham Summit Keynote," U.S. Embassy Kenya, March 29, 2023, https://ke.usembassy.gov/why-africa-why-kenya/.

22. Geoffrey Gertz and Miles M. Evers, "Geoeconomic Competition: Will State Capitalism Win?" *The Washington*

Quarterly 43, no. 2 (2020): 117–136, https://doi.org/10.1080/0163660X.2020.1770962.

23. Joan Tilouine, "In Addis Ababa, the African Union Headquarters Spied on by Beijing," *Le Monde Afrique*, January 26, 2018, http://www.lemonde.fr//afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

24. Sebastian Moss, "Australia: Huawei's Papua New Guinea Data Center Security 'Openly Broken,' Making Potential Spying Easy," Data Center Dynamics, August 12, 2020, https://www.datacenterdynamics.com/en/news/australia-huaweis-papua-new-guinea-data-center-security-openly-broken-making-potential-spying-easy/.

25. Interviews with H and J, October 16, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

26 Luiz F. Bittencourt et al., "The Internet of Things, Fog and Cloud Continuum: Integration and Challenges," Cornell University, September 26, 2018, https://arxiv.org/abs/1809.09972.

27. "Mapping Huawei's Smart Cities Creep," Privacy International, https://privacyinternational.org/long-read/4689/mapping-huaweis-smart-cities-creep.

28. Jonathan Hillman, "U.S. at Risk of Losing Cloud Computing Edge to China," Politico, August 26, 2021, https://www.politico.com/newsletters/politico-china-watcher/2021/08/26/us-at-risk-of-losing-cloud-computing-edge-to-china-494105.

29. "Hikvision Global," Hikvision, https://www.hikvision.com/en/.

30. Reynold Cheung, "Huawei's 2024 Performance—Trading Billions in Profit for a Shot at Technological Sovereignty," CTOL Digital Solutions, March 31, 2025, https://www.ctol.digital/news/huawei-2024-profit-trade-for-tech-sovereignty/; Celia Chen and Jane Zhang, "Huawei Sees 'Complicated' Year Ahead Despite Posting Record Group Sales of US$121 Billion on Strong Domestic Sales of Smartphones," *South China Morning Post*, March 31, 2020, https://www.scmp.com/tech/big-tech/article/3077723/huawei-reports-solid-business-smartphones-drive-group-sales-us121; Hauwei, "2024 Annual Report."

31. Huawei, "EU Ranks Huawei as the World's 2nd Highest Investor in R&D," press release, December 20, 2021, http://huawei.com/en/news/2021/12/european-commission-huawei-investor.

32. "Research and Development Margin for Apple Inc.," FinBox, 2025, https://finbox.com/NASDAQGS:AAPL/explorer/rd_exp_margin/; "How Does Google's R&D Spending Growth Compare to Revenue Growth in 2024?" AI Invest, March 29, 2025, https://www.ainvest.com/chat/share/googles-spending-growth-compare-revenue-growth-2024-bb4796/; "Research and Development Margin for Microsoft Corporation," FinBox, 2025, https://finbox.com/NASDAQGS:MSFT/explorer/rd_exp/.

33. Charlotte Trueman, "Huawei Unveils Ascend 920 AI Chip, Will Start Shipping 910C to Chinese Customers From May—Report," Data Center Dynamics, April 22, 2025, https://www.datacenterdynamics.com/en/news/huawei-unveils-ascend-920-ai-chip-will-start-shipping-910c-to-chinese-customers-from-may-report.

34. "Top 100 Global Innovation Leaders," FDI Intelligence, June 19, 2023, https://www.fdiintelligence.com/content/7d894243-9c09-5a30-960f-7fe3567c3063.

35. Amy Hawkins, "Beijing's Big Brother Tech Needs African Faces," *Foreign Policy*, July 24, 2018, https://archive.is/20230804021912/https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

36. Shan Jie, "China Exports Facial ID Technology to Zimbabwe," *Global Times*, April 12, 2018, https://archive.is/NTZ5N#selection-1295.0-1299.95.

37. Hawkins, "Beijing's Big Brother Tech Needs African Faces."

38. Yana Gorokhovskaia and Cathryn Grothe, "The Mounting Damage of Flawed Elections and Armed Conflict," Freedom House, 2024, https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict.

39. Tony Roberts and Marjoke Oosterom, "Digital Authoritarianism: A Systematic Literature Review," *Information Technology for Development*, November 24, 2024, https://doi.org/10.1080/02681102.2024.2425352.

40. "The New Big Brother: China and Digital Authoritarianism," U.S. Senate Committee on Foreign Relations, July 21, 2020, https://www.govinfo.gov/content/pkg/CPRT-116SPRT42356/html/CPRT-116SPRT42356.htm.

41. Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State," Center for Security and Emerging Technology, October 2020, https://cset.georgetown.edu/publication/designing-alternatives-to-chinas-repressive-surveillance-state/.

42. Angus Berwick, "A New Venezuelan ID, Created with China's ZTE, Tracks Citizen Behavior," Reuters, November 14, 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.

43. Abid Hussain, "Pakistan Tests Secret China-Like 'Firewall' to Tighten Online Surveillance," Al Jazeera, November 26, 2024, https://www.aljazeera.com/news/2024/11/26/pakistan-tests-china-like-digital-firewall-to-tighten-online-surveillance.

44. David Gordon and Meia Nouwens, "Introduction," in *The Digital Silk Road: China's Technological Rise and the*

Geopolitics of Cyberspace, ed. David Gordon and Meia Nouwens (New York: Routledge, 2022); Michael Bennon and Francis Fukuyama, "China's Road to Ruin: The Real Toll of Beijing's Belt and Road," *Foreign Affairs*, August 22, 2023, https://www.foreignaffairs.com/china/belt-road-initiative-xi-imf.

45. Gordon and Nouwens, "Introduction."

46. Anna Gross et al., "How the US Is Pushing China out of the Internet's Plumbing," *Financial Times*, June 13 2023, https://ig.ft.com/subsea-cables/; "Infographic: Amazon and Microsoft Stay Ahead in Global Cloud Market," Statista, accessed February 27, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

47. Marcus Willett, "China's Investment in Digital Technologies and the Digital Great Game," in Gordon and Nouwens, *The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace*, 28.

48. Hung Tran, "Dual Circulation in China: A Progress Report," Atlantic Council, October 24, 2022, https://www.atlanticcouncil.org/blogs/econographics/dual-circulation-in-china-a-progress-report/.

49. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Co., 2015); "Made in China 2025," State Council of the People's Republic of China, trans. Center for Security and Emerging Technology, May 8, 2025, https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

50. Hong Shen, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication* 12 (2018): 2383–2701, https://ijoc.org/index.php/ijoc/article/view/8405; Mamta Babkar, "China Stimulated Its Economy Like Crazy after the Financial Crisis ... and Now the Nightmare Is Beginning," *Business Insider*, June 17, 2013, https://www.businessinsider.com/chinas-excess-capacity-problem-2013-6.

51. Jacob Gunter et al., "Beyond Overcapacity: Chinese-Style Modernization and the Clash of Economic Models," Mercator Institute for China Studies, April 1, 2025, https://merics.org/en/report/beyond-overcapacity-chinese-style-modernization-and-clash-economic-models.

52. Shen, "Building a Digital Silk Road?"

53. Shen, "Building a Digital Silk Road?"

54. Axel Dreher et al., "Aid Effectiveness and Donor Motives," *World Development* 176 (2024): 106501, https://doi.org/10.1016/j.worlddev.2023.106501.

55. "Full Text: Proposal of the People's Republic of China on the Reform and Development of Global Governance," Ministry of Foreign Affairs of the People's Republic of China, trans. Xinhua News Agency, September 13, 2023, https://english.news.cn/20230913/edf2514b79a34bf6812a1c372dcdfc1b/c.html?mc_cid=8031f71d00&mc_eid=ccbfb1d564&utm_source=substack&utm_medium=email.

56. Phys.org, "Brazil Moves to Secure Telecom, Internet Systems After US Spying," August 14, 2013, https://phys.org/news/2013-08-brazil-telecom-internet-spying.html.

57. Chloe Yeung, "The Belt and Road Initiative 10 Years Later: China's Transition to 'Small and Beautiful,'" Asia Pacific Foundation of Canada, March 19, 2024, https://www.asiapacific.ca/publication/china-belt-and-road-initiative-10-years-later.

58. "Xi Urges Continuous Efforts to Promote High-Quality BRI Development."

59. Wang, "China Belt and Road Initiative (BRI) Investment Report 2025 H1."

60. Wang, "China Belt and Road Initiative (BRI) Investment Report 2025 H1."

61. "China to Advance Sci-Tech Innovation to Support High-Quality Belt and Road Cooperation," Xinhua News Agency, October 18, 2023, https://english.news.cn/20231018/c1fbd144716f4168947a28bcc623867e/c.html.

62. "First Belt and Road Conference on Science and Technology Exchange Opens in SW China's Chongqing," Xinhua News Agency, November 7, 2023, https://english.www.gov.cn/news/202311/07/content_WS65498b21c6d0868f4e8e1093.html.

63. Christoph Nedopil Wang, "China Belt and Road Initiative (BRI) Investment Report 2023," Green Finance & Development Center, February 5, 2024, https://greenfdc.org/china-belt-and-road-initiative-bri-investment-report-2023/.

64. "'Green,' 'Digital' Become Key Themes in New Phase of BRI Development," Xinhua News Agency, October 15, 2024, https://eng.yidaiyilu.gov.cn/p/03SL7S5V.html.

65. Christoph Nedopil Wang, "China Belt and Road Initiative (BRI) Investment Report 2025 H1," Green Finance & Development Center, July 17, 2025, https://greenfdc.org/china-belt-and-road-initiative-bri-investment-report-2025-h1/.

66. Christina Lu, "China's Belt and Road to Nowhere," *Foreign Policy*, February 13, 2023, https://foreignpolicy.com/2023/02/13/china-belt-and-road-initiative-infrastructure-development-geopolitics/.

67. "Xi Holds Talks with El Salvador President, Urging Solid Basis to Boost Cooperation," Ministry of Foreign Affairs of the People's Republic of China, November 1, 2018, https://www.fmprc.gov.cn/eng/xw/zyxw/202405/t20240530_11327394.html.

68. Yeung, "The Belt and Road Initiative 10 Years Later."

69. Yeung, "The Belt and Road Initiative 10 Years Later."

70. Wang, "China Belt and Road Initiative (BRI) Investment Report 2023."

71. Riley Duke, "Peak Repayment: China's Global Lending," Lowy Institute, May 2025, https://interactives.lowyinstitute.org/features/peak-repayment-china-global-lending/.

72. Bradley Parks et al., "Belt and Road Reboot: Beijing's Bid to De-risk Its Global Infrastructure Initiative," AidData, November 2023, https://docs.aiddata.org/reports/belt-and-road-reboot/Belt_and_Road_Reboot_Full_Report.pdf.

73. Parks et al., "Belt and Road Reboot."

74. Richard Heeks et al., "China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda," *The Information Society* 40, no. 2 (2024): 69–95, https://doi.org/10.1080/01972243.2024.2315875.

75. Yeung, "The Belt and Road Initiative 10 Years Later."

76. Christoph Nedopil Wang, "China Belt and Road Initiative (BRI) Investment Report 2024," Green Finance & Development Center, February 27, 2025, https://greenfdc.org/china-belt-and-road-initiative-bri-investment-report-2024/.

77. Andrea Benito, "How China Is Gaining Ground in the Middle East Cloud Computing Race," Rest of World, May 5, 2025, https://restofworld.org/2025/china-cloud-middle-east/; "South-east Asia Makes an AI Power Grab," *The Economist*, July 29, 2025, https://www.economist.com/asia/2025/07/29/south-east-asia-makes-an-ai-power-grab.

78. Eva Dou, *House of Huawei: The Secret History of China's Most Powerful Company* (New York: Portfolio, 2025); Jeff M. Smith, "China's Belt and Road Initiative: Strategic Implications and International Opposition," Heritage Foundation, *Backgrounder* No. 3331, August 9, 2018, https://www.heritage.org/sites/default/files/2018-08/BG3331_2.pdf.

79. Rush Doshi, "The United States, China, and the Contest for the Fourth Industrial Revolution," Brookings Institution, July 31, 2020, https://www.brookings.edu/articles/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution.

80. Data for 2015–2022 come from Elisa Oreglia and Weidi Zheng, "The Digital Silk Road between National Rhetoric and Provincial Ambitions," *The China Quarterly* 261 (March 2025): 183–195, https://doi.org/10.1017/S0305741024000936. The authors collected policy documents of the People's Republic of China central government by searching the databases of the State Council, the National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Commerce, Ministry of Foreign Affairs, and Ministry of Science and Technology using the terms 数字丝绸之路 (Digital Silk Road), 网上丝绸之路 (Cyber Silk Road), and 信息丝绸之路 (Information Silk Road) as keywords. This analysis was conducted for the years 2015–2022; this report's authors replicated the methodology for 2022–2025.

81. "Countries of the Belt and Road Initiative," Green Finance & Development Center, accessed September 12, 2025, https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri/; Oreglia and Zheng, "The Digital Silk Road between National Rhetoric and Provincial Ambitions."

82. Meia Nouwens, "China's Digital Silk Road: Integration into National IT Infrastructure and Wider Implications for Western Defence Industries," International Institute for Strategic Studies, February 2021, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/china-digital-silk-road---iiss-research-paper.pdf.

83. "China Looks Forward to Enhancing Tech, Innovation Cooperation with BRI Partner Countries," *Global Times*, October 30, 2023, https://www.globaltimes.cn/page/202310/1300855.shtml; "Key Takeaways from BRI White Paper," State Council of the People's Republic of China, October 11, 2023, https://english.www.gov.cn/news/202310/11/content_WS6526994fc6d0868f4e8e024a.html.

84. Meia Nouwens, "Identifying the Digital Silk Road," in Gordon and Nouwens, *The Digital Silk Road: China's Technological Rise and the Geopolitics of Cyberspace*, 53.

85. Nouwens, "Identifying the Digital Silk Road," 53.

86. Provinces are other key actors; however, recent studies have found that while provinces are perhaps the main actors that have taken up the *rhetoric* of the DSR, they have achieved "little success either internally or externally." See Oreglia and Zheng, "The Digital Silk Road between National Rhetoric and Provincial Ambitions."

87. Between 2023 and 2025, only the State Council, NDRC, and MOFA published any policy documents relating to the DSR.

88. Paul Triolo, "The Digital Silk Road and the Evolving Role of Chinese Technology Companes," in Gordon and Nouwens, *The Digital Silk Road, China's Technological Rise and the Geopolitics of Cyberspace*, 81.

89. Global Infrastructure Hub, "China—China Development Bank (CDB)," Guidance Note on National Infrastructure Banks & Similar Financing Facilities, Annex D, June 2019, https://cdn.gihub.org/umbraco/media/2617/china-case-study.pdf.

90. Anna Gelpern et al., "How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments," AidData,

2021, https://docs.aiddata.org/reports/how-china-lends.html.

91. "China's State Organizational Structure," Congressional-Executive Commission on China, accessed September 12, 2025, https://www.cecc.gov/chinas-state-organizational-structure; Anu Jose and Estella Qi, "China's EV Achievements Loom over the USA. Part 1: China 'Structure' and 'Trigger,'" Frost & Sullivan, July 31, 2024, https://www.frost.com/growth-opportunity-news/chinas-ev-achievements-loom-over-the-usa-part-1-china-structure-and-trigger/.

92. Jimmy Goodrich, "Reading the Tea Leaves on China's New Central Science and Technology Commission," University of California Institute on Global Conflict and Cooperation, September 25, 2024, https://ucigcc.org/blog/reading-the-tea-leaves-on-chinas-new-central-science-and-technology-commission/.

93. "Silk Road Fund Strengthens Connectivity," International Department, Central Committee of the Communist Party of China, October 2016, https://www.idcpc.org.cn/english2023/dzwk/qt/sss/202307/P020230717029989453934.pdf.

94. Melanie Hart and Jordan Link, "There Is a Solution to the Huawei Challenge," Center for American Progress, October 14, 2020, https://www.americanprogress.org/article/solution-huawei-challenge/.

95. "China Export and Credit Insurance Corporation (SINOSURE)," CC Solutions, updated August 3, 2025, http://cc-solutions.net/Handbook/Agency?Agency=111.

96. Daniel Runde, "The U.S. EXIM Bank in an Age of Great Power Competition," Center for Strategic and International Studies, June 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240618_Runde_EXIM_Competition.pdf.

97. Nouwens, "Identifying the Digital Silk Road.'

98. Laurie Chen and Yew Lun Tian, "China's Xi Warns against Decoupling, Lauds Belt and Road at Forum," Reuters, October 18, 2023, https://www.reuters.com/world/chinas-xi-lauds-belt-road-smaller-greener-summit-2023-10-18/.

99. Jacob J. Lew and Gary Roughead, "China's Belt and Road: Implications for the United States," Council on Foreign Relations, March 2021, https://www.cfr.org/task-force-report/chinas-belt-and-road-implications-for-the-united-states/findings.

100. "The Export-Import Bank of China (China Exim Bank)," Sovereign Wealth Fund Institute, accessed September 13, 2025, https://www.swfinstitute.org/profile/598cdaa50124e9fd2d05ac7c; "Rating Report China Export & Credit Insurance Corporation," Fitch Ratings, March 20, 2025, https://www.fitchratings.com/research/insurance/china-export-credit-insurance-corporation-20-03-2025; "The 5 Biggest Banks in China in 2025," Statrys, March 11, 2023, https://statrys.com/blog/biggest-banks-china; "Financial Statements," New Development Bank, 2023, https://www.ndb.int/annual-report/2023/pdf/NDB_Annual_Financial_Statements_2023.pdf; "China Export & Credit Insurance Corporation (SINOSURE) |Export Credit Agency (ECA) in China," Trade Finance Global, accessed September 13, 2025, https://www.tradefinanceglobal.com/export-finance/export-credit-agencies-eca/china-export-credit-insurance-corporation-china-eca/; "The Export-Import Bank of China," Industrial Park Platform, accessed September 13, 2025, https://ipp.unido.org/partner/export-import-bank-china; "The AIIB's 10 Biggest Beneficiaries," FDI Intelligence, accessed September 13, 2025, https://www.fdiintelligence.com/content/0e5c7a3f-3def-5188-ba0b-f61ae48ff621; Cao Desheng and Zhou Lanxu, "AIIB Hailed as Pioneer in International Financial Governance," China Daily, June 26, 2025, https://www.chinadailyasia.com/hk/article/614765; and "Silk Road Fund Strengthens Connectivity," New Stories on the Silk Road, October 2018, https://www.idcpc.org.cn/english2023/dzwk/qt/sss/202307/P020230717029989453934.pdf.

101. Oreglia and Zheng, "The Digital Silk Road between National Rhetoric and Provincial Ambitions."

102. Huawei, "Cinia Selects Huawei to Build Direct Digital Silk Road between Asia and Europe," press release, March 16, 2016, http://www.huawei.com/en/news/2016/3/build-direct-digital-silk-road.

103. Duke, "Peak Repayment: China's Global Lending."

104. Ryan McMorrow, "China Moves to Take 'Golden Shares' in Alibaba and Tencent Units," *Financial Times*, January 13, 2023, https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de.

105. CompaniesMarketCap, "Largest Chinese Companies by Market Capitalization," https://companiesmarketcap.com/china/largest-companies-in-china-by-market-cap/; HMNTech, "Company," https://www.hmntech.com/.

106. "2025 National Trade Estimate Report on Foreign Trade Barriers," United States Trade Representative, 2025, https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf.

107. Organisation for Economic Co-operation and Development (OECD), "Measuring Distortions in International Markets: Below-Market Finance," OECD Trade Policy Papers, no. 247, May 12, 2021, https://doi.org/10.1787/a1a5aa8a-en; OECD, "Government Support in Industrial Sectors: A Synthesis Report," OECD Trade Policy Papers, no. 270, April 7, 2023, https://www.oecd.org/en/publications/government-support-in-industrial-sectors_1d28d299-en.html.

108. Camille Boullenois et al., "Was Made in China 2025 Successful?" Rhodium Group, May 5, 2025, https://rhg.com/research/was-made-in-china-2025-successful/.

109. Boullenois et al., "Was Made in China 2025 Successful?"

110. Siddhant Nair, "Made in China 2025," Organization for Research on China and Asia, August 30, 2022, https://orcasia.org/made-in-china-2025.

111. Jonathan E. Hillman, "War and PEACE on China's Digital Silk Road," Center for Strategic and International Studies, May 16, 2019, https://www.csis.org/analysis/war-and-peace-chinas-digital-silk-road.

112. Anne Neuberger, "China Is Still Winning the Battle for 5G—and 6G: America Must Do More to Compete with Huawei," *Foreign Affairs,* May 1, 2025, https://www.foreignaffairs.com/united-states/china-still-winning-battle-5g-and-6g.

113. Neuberger, "China Is Still Winning the Battle for 5G—and 6G."

114. Hart and Link, "There Is a Solution to the Huawei Challenge."

115. Liza Lin et al., "The U.S. Wanted to Knock Down Huawei. It's Only Getting Stronger," *Wall Street Journal*, July 29, 2024, https://www.wsj.com/business/telecom/huawei-china-technology-us-sanctions-76462031.

116. Ian King and Debby Wu, "Huawei Building Secret Network for Chips, Trade Group Warns," Bloomberg, August 23, 2023, https://www.bloomberg.com/news/articles/2023-08-23/huawei-building-secret-chip-plants-in-china-to-bypass-us-sanctions-group-warns?embedded-checkout=true.

117. "Huawei Eyes Export of AI Chips to Middle East, Southeast Asia to Rival Nvidia," *South China Morning Post*, July 12, 2025, https://www.scmp.com/tech/big-tech/article/3317966/huawei-eyes-export-ai-chips-middle-east-southeast-asia-rival-nvidia.

118. Lin et al., "The U.S. Wanted to Knock Down Huawei"; "2024 Annual Report," Huawei, 2025, https://www.huawei.com/en/annual-report/2024. Government grant data were sourced directly from Huawei's publicly available annual reports and converted to U.S. dollars using the exchange rate of 1 RMB = 0.14 USD.

119. "Huawei Eyes Export of AI Chips to Middle East, Southeast Asia to Rival Nvidia."

120. Asia Society Policy Institute, "Key Takeaways from China's Two Sessions in 2025," March 11, 2025, https://asiasociety.org/policy-institute/key-takeaways-chinas-two-sessions-2025; Keyu Jin, *The New China Playbook: Beyond Socialism and Capitalism* (New York: Penguin Random House, 2023).

121. Liu Liehong, "Accelerate the Construction of a National Integrated Computing Network and Promote the Construction of a Chinese-Style Modern Digital Foundation," QSTHEORY.cn, June 2024, https://www.qstheory.cn/dukan/qs/2024-03/16/c_1130089697.htm.

122. "How ET City Brain Is Transforming the Way We Live—One City at a Time," Alibaba Cloud, June 11, 2018, https://www.alibabacloud.com/blog/how-et-city-brain-is-transforming-the-way-we-live-%E2%80%93-one-city-at-a-time_593745.

123. Barry Naughton, "Chinese Industrial Policy and the Digital Silk Road: The Case of Alibaba in Malaysia," *Asia Policy* 15, no. 1 (January 2020): 23–39, https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-1_2_digitalsilkroadrt_naughton_jan2020.pdf.

124. Runde, "The U.S. EXIM Bank in an Age of Great Power Competition."

125. Charles Wolf Jr., Xiao Wang, and Eric Warner, "China's Foreign Aid and Government-Sponsored Investment Activities," RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR118/RAND_RR118.pdf.

126. Wolf, Wang, and Warner, "China's Foreign Aid and Government-Sponsored Investment Activities."

127. Hart and Link, "There Is a Solution to the Huawei Challenge."

128. "CPPCC Daily: A Financial Pioneer Serving National Strategies," China Development Bank, March 6, 2013, http://web.archive.org/web/20220223175707/https://www.cdb.com.cn/xwzx/mtjj/201512/t20151224_1138.html.

129. "Loans for Strategic Emerging Industries," Export-Import Bank of China, accessed September 13, 2025, http://english.eximbank.gov.cn/Business/CreditB/SupportingCO/202110/t20211021_34885.html.

130. "The Belt and Road Initiative: A Key Pillar of the Global Community of Shared Future," *China Daily*, October 10, 2023, https://english.www.gov.cn/archive/whitepaper/202310/10/content_WS6524b55fc6d0868f4e8e014c.html.

131. Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal,* December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

132. Tony Roberts, "Safety and Regulating Risks: Who Is Safe in 'Safe Cities'?" Institute of Development Studies, October 30, 2023, https://www.ids.ac.uk/opinions/safety-and-regulating-risks-who-is-safe-in-safe-cities/.

133. "China Eximbank Provides RMB 1.225 Billion Government Concessional Loan for Konza Data Centre and Smart City Project," AidData, 2021, https://china.aiddata.org/projects/59366/.

134. Joey Roulette et al., "China Builds Space Alliances in

Africa as Trump Cuts Foreign Aid," Reuters, February 11, 2025, https://www.reuters.com/investigations/china-builds-space-alliances-africa-trump-cuts-foreign-aid-2025-02-11/.

135. Heeks et al., "China's Digital Expansion in the Global South."

136. Interview with F, September 9, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

137. Ryan McMorrow and Nian Liu, "China's 'AI-in-a-Box' Products Threaten Big Tech's Cloud Growth Strategies," *Financial Times*, May 19, 2024, https://www.ft.com/content/02537db9-8687-48eb-94c8-383f8332b5d6.

138. McMorrow and Liu, "China's 'AI-in-a-Box' Products."

139. McMorrow and Liu, "China's 'AI-in-a-Box' Products."

140. Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," *The New York Times*, April 24, 2019, https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

141. Charles Rollet, "Ecuador's All-Seeing Eye Is Made in China," *Foreign Policy*, August 11, 2025, https://foreignpolicy.com/2018/08/09/ecuadors-all-seeing-eye-is-made-in-china/.

142. Interviews with B, E, F, October 14–17, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

143. Interviews with B, E, F, October 14–17, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

144. David Sacks, "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do to Respond," Council on Foreign Relations, March 29, 2021, https://www.cfr.org/blog/china-huawei-5g.

145. Interviews with B, E, F, October 14-17, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

146. Alex Wooley, "AidData's New Dataset of 13,427 Chinese Development Projects Worth $843 Billion Reveals Major Increase in 'Hidden Debt' and Belt and Road Initiative Implementation Problems," *The First Tranche* (blog), September 29, 2021, https://www.aiddata.org/blog/aiddatas-new-dataset-of-13-427-chinese-development-projects-worth-843-billion-reveals-major-increase-in-hidden-debt-and-belt-and-road-initiative-implementation-problems.

147. "World Bank Listing of Ineligible Firms and Individuals," World Bank, accessed September 13, 2025, https://www.worldbank.org/en/projects-operations/procurement/debarred-firms.

148. Joshua Meservey, "Chinese Corruption in Africa Undermines Beijing's Rhetoric about Friendship with the Continent," Heritage Foundation, August 8, 2018, https://www.heritage.org/global-politics/report/chinese-corruption-africa-undermines-beijings-rhetoric-about-friendship-the.

149. Denis Mwangi, "China Accused of Bribing Government Officials for Tenders," Kenyans, September 13, 2018, https://www.kenyans.co.ke/news/33085-china-accused-bribing-government-officials-tenders.

150. "2024 National Trade Estimate Report on Foreign Trade Barriers," United States Trade Representative, March 1, 2024, https://ustr.gov/sites/default/files/2024%20NTE%20Report.pdf.

151. Interview with F, September 9, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

152. "Huawei Bribery Scandal: What We Know so Far," Politico, March 17, 2025, https://www.politico.eu/article/huawei-bribery-scandal-eu-chinese-tech-lobby-money-lobbying/.

153. "Pausing Foreign Corrupt Practices Act Enforcement to Further American Economic and National Security," The White House, February 11, 2025, https://www.whitehouse.gov/presidential-actions/2025/02/pausing-foreign-corrupt-practices-act-enforcement-to-further-american-economic-and-national-security/.

154. Dou, *House of Huawei*.

155. Bonnie Bley, "World Diplomacy Stocktake: A Shifting of the Ranks," Lowy Institute, November 27, 2019, https://www.lowyinstitute.org/the-interpreter/world-diplomacy-stocktake-shifting-ranks.

156. Nahal Toosi, "'Frustrated and Powerless': In Fight with China for Global Influence, Diplomacy Is America's Biggest Weakness," Politico, October 23, 2022, https://www.politico.com/news/2022/10/23/china-diplomacy-panama-00062828.

157. Interview with C, December 16, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

158. "Frequently Asked Questions about the Ministry of Foreign Affairs' 2023 Civil Service Recruitment," Ministry of Foreign Affairs of the People's Republic of China, October 24, 2022, https://www.mfa.gov.cn/wjb_673085/gbclc_603848/bkzn_660695/202210/t20221022_10790411.shtml.

159. "China Is Recruiting Embassy Staff with a Focus on Electric Vehicles, Source Says," *South China Morning Post*, December 17, 2024, https://www.scmp.com/news/

china/politics/article/3291139/china-recruiting-embassy-staff-focus-electric-vehicles-source-says; Ryan Fedasiuk et al., "China's Foreign Technology Wish List," Center for Security and Emerging Technology, May 2021, https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/.

160. Fedasiuk et al., "China's Foreign Technology Wish List."

161. "Home," China Science & Technology Exchange Center, accessed September 13, 2025, https://web.archive.org/web/20201113202532/http://www.cistc.gov.cn/Diplomacies_Service/.

162. "China, Saudi Arabia Cement Ties with Deals Including Huawei," Al Jazeera, December 8, 2022, https://www.aljazeera.com/news/2022/12/8/saudi-crown-prince-meets-chinas-xi-in-push-to-deepen-ties; Sherisse Pham, "China's Huawei Will Build Russia's 5G Network," CNN, June 6, 2019, https://www.cnn.com/2019/06/06/tech/huawei-china-russia-5g.

163. "China, Brazil Decide to Elevate Ties in Xi, Lula Meeting," State Council of the People's Republic of China, November 21, 2024, https://english.www.gov.cn/news/202411/21/content_WS673e5422c6d0868f4e8ed436.html.

164. Eduardo Baptista, "Chinese Rival to Starlink Strikes Deal to Enter Brazil," Reuters, November 20, 2024, https://www.reuters.com/technology/space/chinas-starlink-rival-agrees-deal-enter-brazilian-market-2024-11-20/.

165. David Carvalho, "Brazil Woos Chinese Starlink Rival Maker after Feuding with Musk," Bloomberg, November 8, 2024, www.bloomberg.com/news/articles/2024-11-08/brazil-woos-chinese-starlink-rival-maker-after-feuding-with-musk.

166. Abi Olvera and Dan Spokojny, "Diplomacy," 80,000 Hours, August 2024, https://80000hours.org/career-reviews/diplomacy/.

167. Hilary McGeachy, "US-China Technology Competition: Impacting a Rules-Based Order," United States Study Centre, May 2019, https://publicsectornetwork.com/wp-content/uploads/2020/01/US-China-technology-competition-impacting-a-rules-based-order.pdf.

168. "The Chinese Communist Party Central Committee and the State Council Publish the 'National Standardization Development Outline,'" Xinhua News Agency, trans. Center for Security and Emerging Technology, November 19, 2021, https://cset.georgetown.edu/publication/the-chinese-communist-party-central-committee-and-the-state-council-publish-the-national-standardization-development-outline/.

169. Enescan Lorci, "Shaping the Digital Order: China's Role in Technology Standards and the Implications for Taiwan," Global Taiwan Institute, February 5, 2025, https://globaltaiwan.org/2025/02/shaping-the-digital-order-chinas-role-in-technology-standards-and-the-implications-for-taiwan/.

170. Wei Yang and Yurong Zhang, "Standardization Catch-Up Strategy of Latecomer Enterprises: A Longitudinal Case of Huawei," *Humanities and Social Sciences Communications* 12 (2025): Article 150, https://doi.org/10.1057/s41599-025-04464-0.

171. Lorenzo Cassacia, "Is 3GPP Contribution Counting an Indicator of 5G Leadership?" Qualcomm, June 3, 2018, https://www.qualcomm.com/news/onq/2018/06/3gpp-contribution-counting-indicator-5g-leadership.

172. Alan Weissberger, "ABI Research: Major Contributors to 3GPP; How 3GPP Specs Become Standards," *IEEE ComSoc Technology Blog*, March 29, 2023, https://techblog.comsoc.org/2023/03/29/abi-research-major-contributors-to-3gpp-how-3gpp-specs-become-standards/; Lorenzo Cassacia, "Counting 3GPP Contributions—Even The 'Approved' Kind—Does Not Measure 5G Leadership and Value," Qualcomm, October 4, 2022, https://www.qualcomm.com/news/onq/2022/10/counting-3gpp-contributions---even-the--approved--kind---does-no.

173. "Seeds for the Future," Huawei, accessed September 13, 2025, https://www.huawei.com/en/seeds-for-the-future.

174. "MCIT, Huawei Host 5G Onboard Training Program under 'Thinktech' Initiative In Saudi Arabia," PR Network, August 27, 2019, https://pressreleasenetwork.com/site/2019/08/27/mcit-huawei-host-5g-onboard-training-program-under-thinktech-initiative-in-saudi-arabia/; "China Is Educating Engineers around the World," *The Economist*, October 19, 2023, https://www.economist.com/china/2023/10/19/china-is-educating-engineers-around-the-world.

175. "Alibaba Cloud Launches Generative AI Course to Upskill Global Digital Talent," Alibaba Cloud Community, May 16, 2024, https://www.alibabacloud.com/blog/alibaba-cloud-launches-generative-ai-course-to-upskill-global-digital-talent_601171.

176. "ICT Talent Cultivation for Kenya Digital Economy," Huawei Kenya and UNESCO, 2022, https://acts-net.org/wp-content/uploads/ICT-Talent-Cultivation-for-Kenya-Digital-Economy.pdf.

177. Interview with F, September 9, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

178. Chilukuri and Scanlon, "Countering the Digital Silk Road: Kenya."

179. "Why China Looks to Vocational Training to Build Bridges with the Global South," *South China Morning Post*, August 18, 2024, https://www.scmp.com/news/china/diplomacy/article/3274892/why-china-looking-vocational-training-build-bridges-global-south.

180. Shibani Mahtani and Joshua Irwandi, "Winning Friends by Training Workers Is China's New Gambit," *The Washington Post,* July 10, 2023, https://www.washingtonpost.com/world/interactive/2023/china-luban-workshops-global-influence/.

181. Mahtani and Irwandi, "Winning Friends by Training Workers Is China's New Gambit."

182. Christian Shephard, "How China Pulled Ahead to Be the World Leader in Electronic Vehicles," *The Washington Post,* March 3, 2025, https://www.washingtonpost.com/world/2025/03/03/china-electric-vehicles-jinhua-leapmotor/.

183. Will Kirkman et al., "Current- and Future-State Legacy Semiconductor Manufacturing Capacity," MITRE, May 24, 2024, https://www.mitre.org/news-insights/publication/current-and-future-state-legacy-semiconductor-manufacturing-capacity.

184. "Suppliers of Undersea Telecommunications Systems," Pioneer Consulting, March 2021, https://www.pioneerconsulting.com/wp-content/uploads/2021/03/Pioneer_Consulting_Suppliers_Report_Executive_Summary_Download.pdf.

185. "Suppliers of Undersea Telecommunications Systems."

186. Jayne Miller, "The Submarine Cable Boom as Told by a Decade of TeleGeography Maps," TeleGeography, May 8, 2025, https://blog.telegeography.com/submarine-cables-over-time-through-the-years. There were 299 active or planned subsea cables worldwide in 2015 and 650 in 2025. The difference is 351, representing a 117 percent increase.

187. Lane Burdette, "How Many Submarine Cables Are There, Anyway?" TeleGeography, February 27, 2025, https://blog.telegeography.com/how-many-submarine-cables-are-there-anyway. The equatorial circumference of the Earth is approximately 40,000 kilometers, and there are 1.5 million kilometers in total subsea cable infrastructure worldwide. Dividing the latter by the former equals 37.5.

188. "Submarine Cable Frequently Asked Questions," TeleGeography, accessed September 13, 2025, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

189. 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/.

190. Brock, "U.S. and China Wage War Beneath the Waves."

191. "HMN Technologies Co., Limited," HMNTech, https://www.hmntech.com/enCompany.jhtml; "Submarine Cable Frequently Asked Questions"; Jonathan Hillman, "China's Global Ambitions Retrace Britain's Imperial Past," *Financial Times*, May 16, 2019, https://www.ft.com/content/58c649f0-771c-11e9-be7d-6d846537acab. HMN Tech touts its deployment of over 108,000 kilometers of the estimated 1.5 million kilometers of submarine networks worldwide, or 7.2 percent.

192. Patrick Christian, "Chinese vs. U.S. Network Infrastructure in Asia, from Cloud to Cables," TeleGeography, October 17, 2024, https://blog.telegeography.com/chinese-vs-us-network-infrastructure-in-asia-from-cloud-to-cables.

193. Manish Singh, "Facebook, Telcos to Build Huge Subsea Cable for Africa and Middle East," TechCrunch, May 14, 2020, https://techcrunch.com/2020/05/14/2africa-africa-middle-east-facebook-subsea-cable/.

194. Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," Center for Strategic and International Studies, August 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

195. Alexander Wang and Wanyu Zhang, "China Slaps Export Restrictions on Two Critical Metals," Covington, July 6, 2023, https://www.globalpolicywatch.com/2023/07/china-slaps-export-restrictions-on-two-critical-metals/.

196. Iain Morris, "Huawei Defies US to Grow Market Share as RAN Decline Ends—Omdia," Light Reading, February 18, 2025, https://www.lightreading.com/5g/huawei-defies-us-to-grow-market-share-as-ran-decline-ends-omdia.

197. Ken Wieland, "Huawei, ZTE Cushioned by China," Light Reading, December 3, 2020, https://www.lightreading.com/5g/huawei-zte-cushioned-by-china.

198. Doug Brake, "A U.S. National Strategy for 5G and Future Wireless Innovation," Information Technology and Information Foundation, April 27, 2020, https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation/.

199. Morris, "Huawei Defies US to Grow Market Share as RAN Decline Ends—Omdia."

200. Cynthia Kroet, "Eleven EU Countries Took 5G Security Measures to Ban Huawei, ZTE," Euro News, December 8, 2024, https://www.euronews.com/next/2024/08/12/eleven-eu-countries-took-5g-security-measures-to-ban-huawei-zte.

201. Henrik Larsen, "Telecom Troubles: Adapting Networks to Defend Europe," Center for European Policy Analysis, June 20, 2023, https://cepa.org/article/telecom-troubles-adapting-networks-to-defend-europe/.

202. Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French Limits on Huawei 5G Equipment Amount to de Facto Ban by 2028," Reuters, July 22, 2020, https://www.reuters.com/article/technology/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R/.

203. Iain Morris, "Europe's Inaction on Huawei May Have Come at the Worst 5G Time," Light Reading, July 29, 2024, https://www.lightreading.com/5g/europe-s-inaction-on-huawei-may-have-come-at-the-worst-5g-time.

204. "Open Radio Access Network (Open RAN)," National Institute of Standards and Technology, accessed September 13, 2025, https://www.nist.gov/open-radio-access-network-open-ran.

205. "Open Radio Access Network (Open RAN)."

206. Tony Huang, "What's Getting in the Way of Open RAN?" January 2025, The Fast Mode, https://www.thefastmode.com/technology-solutions/39028-whats-getting-in-the-way-of-open-ran.

207. National Telecommunications and Information Administration, "Biden-Harris Administration Announces $450 Million Funding Opportunity to Promote Wireless Software Innovation," press release, December 17, 2024, https://www.ntia.gov/press-release/2024/biden-harris-administration-announces-450-million-funding-opportunity-promote-wireless-software.

208. "More than Half of the World's Population Now Covered by 5G," International Telecommunications Union, November 10, 2024, https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-mobile-network-coverage/.

209. "Worldwide Telecom Capex to Decline at a 2 Percent CAGR," Dell'Oro Group, April 10, 2025, https://www.delloro.com/news/worldwide-telecom-capex-to-decline-at-a-2-percent-cagr/.

210. "Overview of 6G (IMT-2030)," Digital Regulation Platform, April 28, 2025, https://digitalregulation.org/overview-of-6g-imt-2030.

211. Dan Jones, "America Has Already Lost the 6G Race," Fierce Network, April 9, 2025, https://www.fierce-network.com/wireless/op-ed-america-has-already-lost-6g-race.

212. Neuberger, "China Is Still Winning the Battle for 5G—and 6G."

213. "6G Technology," Anritsu America, accessed September 13, 2025, https://www.anritsu.com/en-us/test-measurement/solutions/6g-technology.

214. "6G," Qualcomm, accessed September 13, 2025,https://www.qualcomm.com/research/6g.

215. "The LEO Economy: Frequently Asked Questions," National Aeronautics and Space Administration, April 7, 2024, https://www.nasa.gov/humans-in-space/leo-economy-frequently-asked-questions/.

216. Olatunji Isreal and Ilesanmi Michael, "Low Earth Orbit (LEO) Satellites and Rural Internet Potential," ResearchGate, June 7, 2025, https://www.researchgate.net/publication/392660860_Low_Earth_Orbit_LEO_Satellites_and_Rural_Internet_Potential.

217. "Satellite Direct-to-Device Services," Digital Regulation Platform, April 28, 2025, https://digitalregulation.org/satellite-direct-to-device-services/.

218. "Starlink Direct to Cell," Starlink, accessed September 13, 2025, http://starlink.com/us/business/direct-to-cell.

219. Rajarshi Chatterjee, "Can LEO Satellites Transform How Global Supply Chains Work?" Stat Trade Times, October 6, 2024, https://www.stattimes.com/supply-chain/can-leo-satellites-transform-how-global-supply-chain-works-1353408.

220. Peter Garretson, "Thousand Sails: Why Low Earth Orbit Is the Next Frontier for Great Power Competition between the U.S. and China," American Foreign Policy Council, February 3, 2025, https://www.afpc.org/publications/policy-papers/thousand-sails-why-low-earth-orbit-is-the-next-frontier-for-great-power-competition-between-the-u.s-and-chinathum.

221. Howard Wang, Jackson Smith, and Cristina L. Garafola, "Chinese Military Views of Low Earth Orbit: Proliferation, Starlink, and Desired Countermeasures," RAND Corporation, March 24, 2025, https://www.rand.org/pubs/research_reports/RRA3139-1.html.

222. Eduardo Baptista and Greg Torode, "Insight: Studying Ukraine War, China's Military Minds Fret over US Missiles, Starlink," Reuters, March 8, 2023, https://www.reuters.com/world/studying-ukraine-war-chinas-military-minds-fret-over-us-missiles-starlink-2023-03-08/.

223. Stephen Chen, "China to Launch Nearly 13,000 Satellites to 'Suppress' Starlink: Researchers," *South China Morning Post*, February 24, 2023, https://www.scmp.com/news/china/article/3211438/china-aims-launch-nearly-13000-satellites-suppress-elon-musks-starlink-researchers-say.

224. Chen, "China to Launch Nearly 13,000 Satellites to 'Suppress' Starlink."

225. Kevin Pollpeter, "China's Role in Making Outer Space More Congested, Contested, and Competitive," China Aerospace Studies Institute, October 2021, https://www.cna.org/archive/CNA_Files/pdf/chinas-role-in-making-outer-space-more.pdf.

226. Garretson, "Thousand Sails."

227. "The Global Satellite Market Is Forecast to Become Seven Times Bigger," Goldman Sachs, March 5, 2025, https://www.goldmansachs.com/insights/articles/the-global-satellite-market-is-forecast-to-become-seven-times-bigger.

228. Hans Vestburg, "How Can We Bring 2.6 Billion People Online to Bridge the Digital Divide?" World Economic Forum, January 14, 2024, https://www.weforum.org/stories/2024/01/digital-divide-internet-access-online-fwa/.

229. "My Region Is at Capacity or Shows as 'Sold Out' on the Availability Map. What Does That Mean?" Starlink, accessed September 13, 2025, https://www.starlink.com/support/article/240ac933-68ce-00dd-d8ec-0d5bf5816f3d.

230. Tereza Pultarova Dobrijevic, "Starlink Satellites: Facts, Tracking and Impact on Astronomy," Space.com, April 14, 2022, https://www.space.com/spacex-starlink-satellites.html.

231. "Stories," Starlink, accessed September 13, 2025, https://www.starlink.com/stories.

232. Vaida Karaliunaite, "How Many Satellites Are in Space?" NanoAvionics, May 4, 2023, https://nanoavionics.com/blog/how-many-satellites-are-in-space/.

233. Zeyi Yang, "China's Effort to Build a Competitor to Starlink Is Off to a Bumpy Start," *Wired*, May 20, 2025, https://www.wired.com/story/china-starlink-competitor-satellites/.

234. "Satellite Map," SatelliteMap.Space, accessed September 13, 2025, https://satellitemap.space/.

235. "The Global Satellite Market Is Forecast to Become Seven Times Bigger."

236. Kevin Pollpeter, "China's Space Program: Making China Strong, Rich, and Respected," *Asia Policy* 15, no. 2 (April 2020): 12–18, https://www.jstor.org/stable/27023894.

237. Blaine Curcio, "A Rising China in the Global Satellite Market," Satellite Markets & Research, January 15, 2025, https://satellitemarkets.com/rising-china-global-satellite-market.

238. Andrew Jones, "Chinese Constellation Operator Spacesail Signs Agreement with Measat of Malaysia," SpaceNews, February 7, 2025, https://spacenews.com/chinese-constellation-operator-spacesail-signs-agreement-with-measat-of-malaysia/; "China's Satellite Internet Provider Spacesail Sets Up in Kazakhstan," bne IntelliNews, January 23, 2025, https://www.intellinews.com/china-s-satellite-internet-provider-spacesail-sets-up-in-kazakhstan-363065/; and Lam Le, "China's SpaceSail Is Expanding Where Elon Musk Is Stumbling," Rest of World, March 31, 2025, https://restofworld.org/2025/chinas-spacesail-is-expanding-where-elon-musk-is-stumbling/.

239. Andrea Shalal and Joey Roulette, "Exclusive: US Could Cut Ukraine's Access to Starlink Internet Services over Minerals, Say Sources," Reuters, February 22, 2025, https://www.reuters.com/business/us-could-cut-ukraines-access-starlink-internet-services-over-minerals-say-2025-02-22/.

240. Holly Otterbien et al., "Musk Grabs for the Third Rail," Politico, March 10, 2025, https://www.politico.com/newsletters/west-wing-playbook-remaking-government/2025/03/10/musk-grabs-for-the-third-rail-00222270.

241. Le, "China's SpaceSail Is Expanding Where Elon Musk Is Stumbling."

242. Nivedita Bhattacharjee et al., "Chinese Rivals to Musk's Starlink Accelerate Race to Dominate Satellite Internet," Reuters, February 24, 2025, https://www.reuters.com/technology/musks-starlink-races-with-chinese-rivals-dominate-satellite-internet-2025-02-24/.

243. Andrew Jones, "China Launches Fourth Batch of Thousand Sails Megaconstellation Satellites," SpaceNews, January 23, 2025, https://spacenews.com/china-launches-fourth-batch-of-thousand-sails-megaconstellation-satellites/.

244. "Hyperscale Data Centers Hit the Thousand Mark; Total Capacity Is Doubling Every Four Years," Synergy Research Group, April 17, 2024, https://www.srgresearch.com/articles/hyperscale-data-centers-hit-the-thousand-mark-total-capacity-is-doubling-every-four-years.

245. "The World's Total Data Center Capacity is Shifting Rapidly to Hyperscale Operators," Synergy Research Group, June 24, 2025, https://www.srgresearch.com/articles/the-worlds-total-data-center-capacity-is-shifting-rapidly-to-hyperscale-operators.

246. "Data Center Market Size, Share, & Trends Analysis Report By Component (Hardware, Software), by Type (On-Premise), by Server Rack Density, by Redundancy, by PUE, by Design, by Tier Level, by Enterprise Size, by End Use, by Region, and Segment Forecasts, 2025–2030," Grand View Research, 2024, https://www.grandviewresearch.com/industry-analysis/data-center-market-report.

247. Olivier Rival et al., "Accelerating Compute Needs Underpin Southeast Asia's Rapid Data Center Growth," Boston Consulting Group, October 15, 2024, https://www.bcg.com/publications/2024/southeast-asia-accelerating-compute-needs-underpin-southeast-asias-rapid-data-center-growth.

248. "Saudi Arabia Data Center Market Investment Analysis & Growth Opportunities 2025–2030: Saudi Arabia Emerges as a Digital Hub as Data Center Market Set to Hit $3.9 Billion by 2030," GlobeNewswire, March 12, 2025, https://www.globenewswire.com/news-release/2025/03/12/3041661/28124/en/Saudi-Arabia-Data-Center-Market-Investment-Analysis-Growth-Opportunities-2025-2030-Saudi-Arabia-Emerges-as-a-Digital-Hub-as-Data-Center-Market-Set-to-Hit-3-9-Billion-by-2030.html; "Africa Data Center Market—Industry Outlook & Forecast 2022–2027," Arizton, January 2022, https://www.arizton.com/market-reports/africa-data-center-market.

249. Max A. Cherney and Stephen Nellis, "US Tech Firms Nvidia, AMD Secure AI Deals as Trump Tours Gulf States," Reuters, May 14, 2025, https://www.reuters.com/

world/middle-east/saudi-arabia-partners-with-nvidia-spur-ai-goals-trump-visits-2025-05-13/.

250. Lennart Heim (@ohlennart), "To put the new 5GW AI campus in Abu Dhabi (UAE) into perspective. It would support up to 2.5 million NVIDIA B200s," X, May 15, 2025, https://x.com/ohlennart/status/1923091524688007474.

251. "Worldwide Market Share of Leading Cloud Instrastructure Service Providers," Statista, August 21, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

252. "Cloud Performance Benchmark 2019–2020 Edition," Cisco Thousand Eyes, accessed September 13, 2025, https://www.thousandeyes.com/resources/cloud-performance-benchmark-report-november-2019; "Gartner Magic Quadrant for Cloud Infrastructure and Platform Services," Gartner, September 2020, https://www.gartner.com/en/documents/3989743.

253. Christian, "Chinese vs. U.S. Network Infrastructure in Asia."

254. Kyle Wiggers, "Anthropic's CEO Says DeepSeek Shows US Export Rules Are Working," TechCrunch, January 29, 2025, https://techcrunch.com/2025/01/29/anthropics-ceo-says-deepseek-shows-that-u-s-export-rules-are-working-as-intended/; Meaghan Tobin, "The Coder 'Village' at the Heart of China's A.I. Frenzy," *The New York Times*, July 6, 2025, https://www.nytimes.com/2025/07/06/technology/china-artificial-intelligence-hangzhou.html.

255. Mackenzie Hawkins and Ram Anand, "Malaysia Downplays Huawei Deal as US Checks China's AI Reach," Bloomberg, May 20, 2025, https://www.bloomberg.com/news/articles/2025-05-20/malaysia-downplays-huawei-deal-as-us-aims-to-curb-china-ai-power?embedded-checkout=true.

256. Dan Swinhoe, "DataVolt Plans 1.5GW Data Center Campus in Neom's Oxagon," Data Centre Dynamics, February 11, 2025, https://www.datacenterdynamics.com/en/news/datavolt-plans-15gw-data-center-campus-in-neoms-oxagon/; Georgia Butler, "Ezditek Breaks Ground on 24MW Data Center in Riyadh, Saudi Arabia," Data Center Dynamics, November 21, 2024, https://www.datacenterdynamics.com/en/news/ezditek-breaks-ground-on-24mw-data-center-in-riyadh-saudi-arabia/; Humain, "HUMAIN and NVIDIA Announce Strategic Partnership to Build AI Factories of the Future in Saudi Arabia," press release, May 13, 2025, https://www.humain.ai/en/news/humain-and-nvidia-stategic-partnership/; NVIDIA, "Saudi Arabia and NVIDIA to Build AI Factories to Power Next Wave of Intelligence for the Age of Reasoning," press release, May 13, 2025, https://nvidianews.nvidia.com/news/saudi-arabia-and-nvidia-to-build-ai-factories-to-power-next-wave-of-intelligence-for-the-age-of-reasoning; AMD, "AMD and HUMAIN Form Strategic, $10B Collaboration to Advance Global AI," press release, May 13, 2025, https://ir.amd.com/news-events/press-releases/detail/1250/amd-and-humain-form-strategic-10b-collaboration-to-advance-global-ai; Humain, "Saudi Arabia's New AI Enterprise, HUMAIN, Joins Forces with AMD and Cisco to Launch Groundbreaking AI Infrastructure Collaboration," press release, May 13, 2025, https://www.humain.ai/en/news/humain-and-amd-and-cisco/; Amazon, "AWS and HUMAIN Announce a More than $5B Investment to Accelerate AI Adoption in Saudi Arabia and Globally," press release, May 13, 2025, https://www.aboutamazon.com/news/company-news/amazon-aws-humain-ai-investment-in-saudi-arabia; "Cloud Regions," TeleGeography, accessed September 13, 2025, https://www.cloudinfrastructuremap.com/#/?metros=jeddah-saudi-arabia%2Criyadh-saudi-arabia&buildings=22962%2C23713; Groq, "Aramco Digital and Groq Announce Progress in Building the World's Largest Inferencing Data Center in Saudi Arabia Following LEAP MOU Signing," press release, September 12, 2024, https://groq.com/news/aramco-digital-and-groq-announce-progress-in-building-the-worlds-largest-inferencing-data-center-in-saudi-arabia-following-leap-mou-signing; Groq, "Saudi Arabia Announces $1.5 Billion Expansion to Fuel AI-powered Economy with AI Tech Leader Groq," press release, February 10, 2025, https://groq.com/news/saudi-arabia-announces-1-5-billion-expansion-to-fuel-ai-powered-economy-with-ai-tech-leader-groq; Oliver Peckham, "HPE to Build 100+ Petaflops Shaheen III Supercomputer," HPC Wire, September 27, 2022, https://www.hpcwire.com/2022/09/27/hpe-to-build-100-petaflops-shaheen-iii-supercomputer/; "Dammam-7—Cray CS-Storm, Xeon Gold 6248 20C 2.5GHz, NVIDIA Tesla V100 SXM2, InfiniBand HDR 100," Top 500, accessed September 13, 2025, https://top500.org/system/179885/; "Tuwaiq-1—PowerEdge XE8640, Intel Xeon Platinum 8462Y+ 32C 2.8GHz, NVIDIA HGX H100, Infiniband HDR," Top 500, accessed September 13, 2025, https://top500.org/system/180260/; "Public Cloud Regions," Oracle Cloud Infrastructure, accessed September 13, 2025, https://www.oracle.com/sa/cloud/public-cloud-regions/; Georgia Butler, "Oracle Launches Second Saudi Arabian Public Cloud Region," Data Center Dynamics, August 6, 2024, https://www.datacenterdynamics.com/en/news/oracle-launches-second-saudi-arabian-public-cloud-region/; Dan Swinhoe, "Oracle Announces Plans for Third Saudi Arabia Cloud Region," Data Center Dynamics, February 6, 2023, https://www.datacenterdynamics.com/en/news/oracle-announces-plans-for-third-saudi-arabia-cloud-region/; Aramco, "Aramco to Bring Google Cloud Services to Saudi Arabia," press release, December 21, 2020, https://www.aramco.com/en/news-media/news/2020/aramco-to-bring-google-cloud-services-to-saudi-arabia; Dan Swinhoe, "Google to Launch Saudi Cloud Region This Week," Data Center Dynamics, November 13, 2023, https://www.datacenterdynamics.com/en/news/google-to-launch-saudi-cloud-region-this-week/; Georgia Butler, "Google Cloud to Develop AI Hub

in Saudi Arabia with PIF," Data Center Dynamics, October 31, 2024, https://www.datacenterdynamics.com/en/news/google-cloud-to-develop-ai-hub-in-saudi-arabia/; Georgia Butler, "Microsoft Completes Construction of Saudi Arabia Data Center Region," Data Center Dynamics, December 13, 2024, https://www.datacenterdynamics.com/en/news/microsoft-completes-construction-of-saudi-arabia-data-center-region/; Simon Dux, "Equinix Commits to $1bn Data Centre in Saudi Arabia," Mobile Europe, February 12, 2025, https://www.mobileeurope.co.uk/equinix-commits-to-1bn-data-centre-in-saudi-arabia/; Carrington Malin, "Saudi Arabia Launches World's Largest Sovereign AI Cloud," Middle East AI News, February 18, 2025, https://www.middleeastainews.com/p/saudi-arabia-launches-worlds-largest; Reina Takla and Nirmal Narayanan, "Tencent Cloud to Launch Saudi Operations in 2025 with $150m Investment, Says Official," *Arab News*, February 9, 2025, https://www.arabnews.com/node/2589572/business-economy; Dan Swinhoe, "Huawei Launches Saudi Cloud Region in Riyadh," Data Center Dynamics, September 4, 2023, https://www.datacenterdynamics.com/en/news/huawei-launches-saudi-cloud-region-in-riyadh/; "Saudi Cloud Computing Co. Launches Services as Riyadh Becomes Hub for Alibaba Cloud," *Arab News*, June 6, 2022, https://arab.news/6bfdm; "China Eximbank Provides RMB 1.225 Billion Government Concessional Loan for Konza Data Centre and Smart City Project," AidData, accessed September 13, 2025, https://china.aiddata.org/projects/59366; Sebastian Moss, "Huawei to Build Konza Data Center and Smart City in Kenya, with Chinese Concessional Loan," Data Center Dynamics, April 3, 2019, https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan; Microsoft, "Microsoft and G42 Announce $1 Billion Comprehensive Digital Ecosystem Initiative for Kenya," press release, May 22, 2024, https://news.microsoft.com/source/2024/05/22/microsoft-and-g42-announce-1-billion-comprehensive-digital-ecosystem-initiative-for-kenya/; Oracle, "Oracle Plans to Open a Public Cloud Region in Kenya," press release, January 31, 2024, https://www.oracle.com/news/announcement/oracle-plans-to-open-a-public-cloud-region-in-kenya-2024-01-31/; Dan Swinhoe, "AWS Launches New Indonesian Cloud Region in Jakarta," Data Center Dynamics, December 14, 2021, https://www.datacenterdynamics.com/en/news/aws-launches-new-indonesian-cloud-region-in-jakarta/; Davis Hart and Rick Harshman, "The New Google Cloud Region in Jakarta Is Now Open," Google Cloud Blog, June 24, 2020, https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-in-jakarta-now-open; "Google Cloud Expands AI-Ready Data Center Capacity in Jakarta," TechNode Global, May 14, 2025, https://technode.global/2025/05/14/google-cloud-expands-ai-ready-data-center-capacity-in-jakarta/; Microsoft, "Microsoft Opens Its First Cloud Region in Indonesia to Unlock the New AI Economy—Indonesia News Center," press release, May 27, 2025, https://news.microsoft.com/id-id/2025/05/27/microsoft-opens-indonesia-central/; "Available Regions and Zones," Alibaba Cloud, accessed September 13, 2025, https://www.alibabacloud.com/help/en/mongodb/user-guide/region-and-zone-restrictions; Dan Swinhoe, "Tencent Cloud Launches First Data Center in Jakarta, Indonesia," Data Center Dynamics, April 12, 2021, https://www.datacenterdynamics.com/en/news/tencent-cloud-launches-first-data-center-in-jakarta-indonesia/; Huawei Cloud, "Huawei Cloud Launches the Indonesia Region—Building the Cloud Foundation for a Digital Indonesia," press release, November 23, 2022, https://www.huaweicloud.com/intl/en-us/news/20221123190220884.html; Jason Ma, "Oracle Establishes Cloud Presence in Indonesia," Data Center Dynamics, July 11, 2025, https://www.datacenterdynamics.com/en/news/oracle-establishes-cloud-presence-in-indonesia/; Soma Velayutham, "Indonesia on Track to Achieve Sovereign AI Goals with NVIDIA, Cisco and IOH," Nvidia, July 10, 2025, https://blogs.nvidia.com/blog/indonesia-ai-center-of-excellence/; Niva Yadav, "Brazilian Local Government Passes Law to Support Scala's AI City Data Center Campus," Data Center Dynamics, December 20, 2024, https://www.datacenterdynamics.com/en/news/brazilian-local-government-passes-law-for-scalas-ai-city/; Mark Bowen, "Elea Announces Landmark Brazilian Data Center Project," Intelligent CIO, July 11, 2025, https://www.intelligentcio.com/latam/2025/07/11/elea-announces-landmark-brazilian-data-center-project/; Dan Swinhoe, "Tencent Cloud Launches First Data Center Region in Brazil," Data Center Dynamics, November 25, 2021, https://www.datacenterdynamics.com/en/news/tencent-cloud-launches-first-data-center-region-in-brazil/; Oracle, "Oracle Opens Second Brazilian Cloud Region in São Paulo," press release, May 12, 2021, https://www.oracle.com/news/announcement/oracle-opens-second-brazilian-cloud-region-2021-05-12/; Dan Swinhoe, "Microsoft to Invest $2.7bn in Cloud and AI Infrastructure in Brazil," Data Center Dynamics, September 27, 2024, https://www.datacenterdynamics.com/en/news/microsoft-to-invest-27bn-in-cloud-and-ai-infrastructure-in-brazil; Peter Judge and Tatiane Aquim, "IBM Opens Multizone Cloud Region in Brazil," Data Center Dynamics, March 18, 2021, https://www.datacenterdynamics.com/en/news/ibm-opens-multizone-cloud-region-brazil/; and Letici Fucuchima, Marcela Ayres, and Bernardo Caram, "Exclusive: TikTok Owner Weighs Data Center Project in Brazil, Sources Say," Reuters, April 25, 2025, https://www.reuters.com/sustainability/climate-energy/tiktok-owner-weighs-data-center-project-brazil-sources-say-2025-04-25/.

257. Mackenzie Hawkins and Yuan Gao, "Huawei Seeks AI Chip Clients in Middle East, Southeast Asia," Bloomberg, June 10, 2025, https://www.bloomberg.com/news/articles/2025-07-10/huawei-seeks-ai-chip-customers-in-middle-east-southeast-asia.

258. Georgia Butler, "Alibaba Cloud Launches Mexico Cloud Region," Data Center Dynamics, February 19, 2025, https://www.datacenterdynamics.com/en/news/alibaba-cloud-launches-mexico-cloud-region/; Huawei, "Huawei Launches Nigeria's First Hyperscale Local Cloud,"

press release, December 12, 2024, https://www.huaweicloud.com/intl/en-us/news/20241212084526769.html.

259. Kyle Chan and Ray Wang, "Leashing Chinese AI Needs Smart Chip Controls," RAND Corporation, August 7, 2025, https://www.rand.org/pubs/commentary/2025/08/leashing-chinese-ai-needs-smart-chip-controls.html.

260. "LLM Chatbot Arena Leaderboard," Hugging Face, accessed September 13, 2025, https://huggingface.co/spaces/lmarena-ai/chatbot-arena-leaderboard.

261. Bill Drexel and Ruby Scanlon, "Trump Must Rebalance America's AI Strategy," *Foreign Policy*, September 2, 2025, https://foreignpolicy.com/2024/12/04/trump-ai-strategy-biden-frontier-national-security/.

262. Sebastian Elbaum and Adam Segal, "What If China Wins the AI Race?" *Foreign Affairs*, June 13, 2025, https://www.foreignaffairs.com/united-states/what-if-china-wins-ai-race.

263. Chris Miller, "How US Export Controls Have (and Haven't) Curbed Chinese AI," AI Frontier, July 8, 2025, https://ai-frontiers.org/articles/us-chip-export-controls-china-ai.

264. Colin H. Kahl, "America Is Winning the Race for Global AI Primacy—for Now: To Stay Ahead of China, Trump Must Build on Biden's Work," *Foreign Affairs*, January 17, 2025, https://www.foreignaffairs.com/united-states/america-winning-race-global-ai-primacy-now.

265. "Browser Market Share Worldwide," StatCounter, accessed September 13, 2025, https://gs.statcounter.com/browser-market-share#monthly-200901-202506.

266. Donna Lu, "We Tried Out DeepSeek. It Worked Well, until We Asked It about Tiananmen Square and Taiwan," *The Guardian*, January 28, 2025, https://www.theguardian.com/technology/2025/jan/28/we-tried-out-deepseek-it-works-well-until-we-asked-it-about-tiananmen-square-and-taiwan.

267. Julian Barnes, "China Turns to A.I. in Information Warfare," *The New York Times,* August 6, 2025, https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html.

268. Michael C. Horowitz and Radha Iyengar Plumb, "What America Gets Wrong about the AI Race," *Foreign Affairs*, April 18, 2025, https://www.foreignaffairs.com/united-states/what-america-gets-wrong-about-ai-race.

269. Kahl, "America Is Winning the Race for Global AI Primacy."

270. Keegan McBride and Dean W. Ball, "The United States Must Win the Global Open Source AI Race," Just Security, November 7, 2024, https://www.justsecurity.org/104676/american-ai-leadership-requires-support-open-source/.

271. Kahl, "America Is Winning the Race for Global AI Primacy."

272. "LLM Chatbot Arena Leaderboard."

273. Liza Lin, Josh Chin, and Rafaelle Huang, "China Is Quickly Eroding America's Lead in the Global AI Race," *The Wall Street Journal,* July 1, 2025, https://www.wsj.com/tech/ai/artificial-intelligence-us-vs-china-03372176.

274. Foster Wong, "DeepSeek Limits Access to AI Model as Demand Strains Capacity," Bloomberg, February 6, 2025, https://www.bloomberg.com/news/articles/2025-02-06/deepseek-limits-access-to-ai-model-as-demand-strains-capacity.

275. Malcolm Moore, "Saudi Aramco Chief Says DeepSeek AI Makes 'Big Difference' to Operations," *Financial Times*, March 4, 2025, https://www.ft.com/content/0d24dcf4-b53b-48e5-b49c-99606958a96d.

276. "Alibaba Cloud Rolls out Expanded Suite of AI Models, Tools in Overseas Push," *South China Morning Post*, January 21, 2025, https://www.scmp.com/tech/big-tech/article/3295689/alibaba-cloud-rolls-out-expanded-suite-ai-models-development-tools-overseas-push; Huawei, "Huawei Cloud Goes Live in Egypt," press release, May 24, 2024, https://www.huawei.com/en/news/2024/5/huawei-cloud-goes-live-in-egypt; Huawei Cloud, "Embracing the AI Era: Huawei Cloud Thailand Launched New Cloud Service Series to Accelerate Enterprises' Shift to AI-Native," press release, March 17, 2025, https://www.huaweicloud.com/intl/en-us/news/20250320114008265.html; Scott Birch, "Huawei Cloud: Digital Transformation 'In Brazil, For Brazil,'" DataCentre Magazine, November 23, 2023, https://datacentremagazine.com/technology-and-ai/huawei-cloud-digital-transformation-in-brazil-for-brazil.

277. "Smart Cities Market Size, Share & Trends Analysis Report by Application (Smart Governance, Smart Building, Smart Healthcare), by Smart Governance, by Smart Utilities, by Smart Transportation, by Smart Healthcare, by Region, and Segment Forecasts, 2025–2030," Grand View Research, 2025, https://www.grandviewresearch.com/industry-analysis/smart-cities-market.

278. Hillman and McCalpin, "Watching Huawei's 'Safe Cities.'"

279. Jacqueline Hicks, "Export of Digital Surveillance Technologies from China to Developing Countries," Institute of Development Studies, August 2022, https://opendocs.ids.ac.uk/ndownloader/files/48183331.

280. Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports," Brookings Institution, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf.

281. "Global Surveillance Camera Market to 2027 with Chinese Companies Such as Hikvision and Dahua Dominating

the Market," Yahoo Finance, September 29, 2022, https://uk.finance.yahoo.com/news/global-surveillance-camera-market-2027-093800723.html.

282. Bryan Burgess et al., "Investing in Narratives: How Beijing Promotes Its Development Projects in the Philippines," AidData, September 2024, https://docs.aiddata.org/reports/investing-in-narratives/Investing_in_Narratives__How_Beijing_promotes_its_development_projects_in_the_Philippines.pdf.

283. Shan Zhiguang, "New Trends in the New Type of Smart City Development," June 17, 2018, http://www.besticity.com/viewpoint/219707.html.

284. "Cyberspace Administration of China: Sharing the Smart City as an Important Component of BRI," HC Security Network News, April 18, 2016, http://info.secu.hc360.com/2016/04/180933855855.shtml.

285. Hillman and McCalpin, "Watching Huawei's 'Safe Cities.'"

286. Erin Baggott Carter and Brett L. Carter, "Exporting the Tools of Dictatorship: The Politics of China's Technology Transfers," *Perspectives on Politics* 23, no. 3 (September 2025): 1089–1108, https://doi.org/10.1017/S1537592724002226.

287. Emmanuel Tupas, "DILG Scraps P20 Billion Safe Philippine Project," Philstar.Com, May 17, 2022, https://www.philstar.com/nation/2022/05/17/2181558/dilg-scraps-p20-billion-safe-philippine-project.

288. "Home," U.S.-ASEAN Smart Cities Partnership, https://www.usascp.org/.

289. Jeremy Goldberg, "AI in the City: Microsoft at Smart City Expo World Congress 2023," Microsoft, October 16, 2023, https://www.microsoft.com/en-us/industry/blog/government/2023/10/16/ai-in-the-city-microsoft-at-smart-city-expo-world-congress-2023/; "Cities and Communities," Cisco, accessed September 13, 2025, https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities.html#~capabilities.

290. U.S. Trade and Development Agency, "USTDA to Pilot Smart City Solutions for Nusantara," press release, September 16, 2024, https://www.ustda.gov/ustda-indonesia-to-pilot-smart-city-solutions-for-nusantara/.

291. U.S. Trade and Development Agency, "USTDA to Pilot Smart City Solutions for Nusantara."

292. Mark Bowen, "Huawei and SC2 Embark on Smart City Projects in KSA," Intelligent CIO, June 29, 2020, https://www.intelligentcio.com/me/2020/06/29/huawei-and-sc2-embark-on-smart-city-projects-in-ksa/; Neom, "NEOM Launches Infrastructure Work for the World's Leading Cognitive Cities in an Agreement with STC," press release, July 27, 2020, https://www.neom.com/en-us/newsroom/neom-cognitive-cities; "Huawei and SC2 Strike Agreement to Collaborate on Saudi Smart Cities," Smart Cities World, June 29, 2020, https://www.smartcitiesworld.net/mobility/huawei-and-sc2-strike-agreement-to-collaborate-on-saudi-smart-cities; "KSA's New Murabba Signs MoU with Tech Giant NAVER Cloud," Breaking Travel News, July 1, 2025, https://www.breakingtravelnews.com/news/article/ksas-new-murabba-signs-mou-with-tech-giant-naver-cloud/; King Abdullah Financial District, "Honeywell and King Abdullah Financial District to Collaborate on Advanced Sustainable City Development," press release, October 29, 2022, https://www.kafd.sa/en/media-centre/honeywell/; Cisco, "Cisco to Design Infrastructure Network for King Abdullah Economic City," press release, January 29, 2008, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2008/m02/cisco-to-design-infrastructure-network-for-king-abdullah-economic-city.html; David Shi, "Smart Cities at the Heart of a Digital Middle East," Huawei, September 2022, https://e.huawei.com/en/ict-insights/global/ict_insights/ict33-digital-city/cover-story/smart-cities-at-the-heart; "Smart Madinah Program," Madinah Region Development Authority, accessed September 13, 2025, https://smartmadinah.city/; Ayman Al Harbi, "Connectivity and Intelligence Help Industrial Cities Evolve," Huawei, accessed September 13, 2025, https://e.huawei.com/br/ict-insights/global/ict-new-horizons-podcasts/Keynotes/sc-barcelona-ayman-al-harbi; Diriyah Company, "Diriyah Company Appoints Giza Systems as the Delivery Partner for Ambitious Smart City Initiative," press release, February 12, 2025, https://www.diriyahcompany.sa/en/news/diriyah-giza-systems-partner; Deema Al-Khudair and Dana Alomar, "Saudi Heritage Site Diriyah Gate to Have Modern Smart City Infrastructure, Says CEO," Arab News, June 8, 2022, https://arab.news/2nhjg; Cisco, "Knowledge Economic City and Cisco Team Up to Develop World-Class Connected City," press release, January 20, 2008, https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2008/m01/knowledge-economic-city-and-cisco-team-up-to-develop-world-class-connected-city.html; "Smart City Strategy: Knowledge Economic City (Saudi Arabia)," Urban and Regional Innovation Research, February 23, 2015, https://urenio.org/2015/02/23/smart-city-strategy-knowledge-economic-city-saudi-arabia/; "Waad Al Shamaal City Development," Bechtel, accessed September 13, 2025, https://www.bechtel.com/projects/waad-al-shamaal-city-development/; Cisco, "Cisco Announces Multi-Million-Dollar Agreement with Saudi's TRSDC to Design Red Sea Project's Smart Destination," press release, March 9, 2020, https://news-blogs.cisco.com/emea/en-uae/2020/03/09/cisco-announces-multi-million-dollar-agreement-with-saudis-trsdc-to-design-red-sea-projects-smart-destination/; Alexandre Michael, "Meeting the Challenges—Creating a Smart Destination," Red Sea Global, February 18, 2021, https://www.redsea-global.com/en/w/media-center/meeting-the-challenges-creating-a-smart-destination/; "Cisco Plans Launch of Smart City Initiative in Saudi," Mechanical Electrical Plumbing, April 3, 2018, https://www.mepmiddleeast.com/projects/project-news/70703-cisco-plans-launch-of-smart-city-initiative-in-saudi; "Rio de Janeiro's Centre of Operations: COR," Centre for Public Impact, March

25, 2016, https://centreforpublicimpact.org/public-impact-fundamentals/rio-de-janeiros-centre-of-operations-cor/; Roberta Prescott, "Inside Brazil's First Smart City," RCR Wireless News, August 18, 2015, https://www.rcrwireless.com/20150818/featured/inside-the-brazils-first-smart-city-whats-there-and-whats-missing-tag5; Alisson Ficher, "China Has Offered R$9 TRILLION per Brazilian City to Transform It into a Futuristic Metropolis! This Amount Would Be Enough to Pay off ALL of Brazil's Current Debt," CPG Click Petroleo e Gas, November 29, 2024, https://en.clickpetroleoegas.com.br/China-offered-R%249-trillion-per-Brazilian-city-to-transform-it-into-a-futuristic-metropolis.-The-amount-would-be-enough-to-pay-off-all-of-Brazil%27s-current-debt./; Amy Sarkar, "NewsHuawei and TIM Brasil Signs MoU to Make First 5G City," HC Newsroom, March 5, 2022, https://www.huaweicentral.com/huawei-and-tim-brasil-signs-mou-to-make-first-5g-city/; Leo Schwartz, "Major Surveillance Firms Are 'Gifting' Tools to Find a Foothold in Latin America," Rest of World, August 12, 2021, https://restofworld.org/2021/surveillance-latin-america-access-now/; "Nusantara Capital Project Gains Momentum with Foreign Investment," ASEAN Business News, May 23, 2025, https://www.aseanbriefing.com/news/indonesias-new-capital-sees-us4b-in-investments/; Albert Nonto, "Huawei Ingenuity to Power 'Smart Cities," Jakarta Globe, May 17, 2015, https://jakartaglobe.id/context/huawei-ingenuity-power-smart-cities; Khamila Mulia, "Rama Raditya of Qlue on Building a Smart City: Startup Stories," KrASIA, June 10, 2019, https://kr-asia.com/rama-raditya-of-qlue-on-building-a-smart-city-startup-stories; "A Smart and Interactive Livable City Plan for the City of Makassar," ADB, April 13, 2022, https://www.adb.org/news/videos/smart-and-interactive-livable-city-plan-city-makassar; "KONZA Cloud: Kenya Embarks on a Cloud Journey to Shape a Digital Future," Huawei Cloud, accessed September 13, 2025, https://www.huaweicloud.com/intl/en-us/cases/konzacloud.html; Njeri Wangari, "In Africa's First 'Safe City,' Surveillance Reigns," Coda Story, November 8, 2023, https://www.codastory.com/authoritarian-tech/africa-surveillance-china-magnum/; Huawei, "Huawei Hosts Safe City Summit in Africa to Showcase Industry Best Practices," press release, October 17, 2016, https://www.huawei.com/en/news/2016/10/safe-city-summit-africa; "Kenya: $355 Million to Restore Nairobi River," Africa News Agency, March 13, 2025, https://africa-news-agency.com/kenya-355-million-to-restore-nairobi-river/; "Tatu Connect," Tatu City, December 23, 2019, https://www.tatucity.com/news/tatu-city-selects-landisgyr-and-honeywell-for-smart-utilities-infrastructure/; "Kisumu Sustainable Mobility Plan," Institute for Transportation and Development Policy, March 17, 2021, https://itdp.org/publication/kisumu-sustainable-mobility-plan/; and "MMTC Annual Healthwalk," Mwale Medical & Technology City, accessed September 13, 2025, https://mwalemedicalandtechnologycity.com/.

293. Interview with E, October 15, 2024. All interviews were conducted in confidentiality, and the names of interviewees have been withheld by mutual agreement.

294. Esther Majerowicz and Miguel Henriques de Carvalho, "China's Expansion into Brazilian Digital Surveillance Markets," Centre for Digital Development, 2023, https://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/dd_wp100.pdf.

295. Susan Phalen, "Chairman Rogers and Ranking Member Ruppersberger Warn American Companies Doing Business with Huawei and ZTE to 'Use Another Vendor,' U.S. House Select Committee on Intelligence, October 8, 2012, https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=326&.

296. Jill C. Gallagher, "U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests," Congressional Research Service, January 5, 2022, https://www.congress.gov/crs-product/R47012.

297. Gallagher, "U.S. Restrictions on Huawei Technologies."

298. Gallagher, "U.S. Restrictions on Huawei Technologies"; Secure and Trusted Communications Networks Act of 2019, Public Law 116-124, 134 Stat. 158, https://www.govinfo.gov/app/details/PLAW-116publ124.

299. David Ljunggren and Steve Scherer, "Canada to Ban Huawei/ZTE 5G Equipment, Joining Five Eyes Allies," Reuters, May 20, 2022, https://www.reuters.com/business/media-telecom/canada-announce-ban-use-huawei-zte-5g-equipment-source-2022-05-19/; Johan Ahlander and Supantha Mukherjee, "Swedish Court Upholds Ban on Huawei Selling 5G Network Gear," Reuters, June 22, 2021, https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/; "Japan Decides to Exclude Huawei, ZTE from Gov't Procurement," Japan Wire, December 10, 2018, https://english.kyodonews.net/articles/-/8779; Rosemain and Barzic, "Exclusive: French Limits on Huawei 5G Equipment Amount to de Facto Ban by 2028"; Gagandeep Kaur, "India Tightens Restrictions on Huawei, ZTE," Light Reading, July 12, 2022, https://www.lightreading.com/5g/india-tightens-restrictions-on-huawei-zte.

300. Sam Jones, "Germany Orders Ban on Chinese Companies from Its 5G Network," *Financial Times*, July 11, 2024, https://www.ft.com/content/aacd77a2-048a-489e-98f8-b9f436e448b6.

301. "Explore Key Takeaways from Prague Proposals," Prague Cyber Security Conference, December 2021, https://www.praguecybersecurityconference.com/prague-proposals/.

302. "The Clean Network."

303. "The Clean Network," U.S. Department of State, accessed September 13, 2025, https://2017-2021.state.gov/the-clean-network.

304. "What We Offer," U.S. International Development Finance Corporation, accessed September 13, 2025, https://www.dfc.gov/what-we-offer/our-products.

305. Phelim Kine, "What Has China House Done?" Politico, December 12, 2024, https://www.politico.eu/newsletter/china-watcher/what-has-china-house-done/.

306. "American Diplomacy and Global Leadership: Review of the FY24 State Department Budget Request," U.S. Senate Foreign Relations Committee, March 22, 2023, https://www.foreign.senate.gov/hearings/american-diplomacy-and-global-leadership-review-of-the-fy24-state-department-budget-request-03-22-2023.

307. "Solutions," Export-Import Bank of the United States, accessed September 13, 2025, https://www.exim.gov/solutions.

308. "Competitiveness Reports," Export-Import Bank of the United States, accessed September 13, 2025, https://www.exim.gov/news/reports/competitiveness-reports.

309. "Competitiveness Reports"; "7 Factors & Jobs Plan," Export-Import Bank of the United States, accessed September 13, 2025, https://www.exim.gov/about/special-initiatives/ctep/7-factors-jobs-plan.

310. "Digital Connectivity and Cybersecurity Partnership," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/.

311. "Digital Connectivity and Cybersecurity Partnership."

312. Digital Connectivity and Cybersecurity Partnership, 22 U.S.C. 10307 (2023), https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title22-section10307.

313. "The Department of State, Foreign Operations, and Related Programs: Fiscal Year 2020 Appropriations Bill," U.S. Senate Committee on Appropriations, December 16, 2019, https://www.appropriations.senate.gov/download/sfops-fy2020-press-summary-12-15.

314. "Consolidated Appropriations Act, 2023: Summary of Appropriations Provisions by Subcommittee," U.S. House Committee on Appropriations, 2023, https://democrats-appropriations.house.gov/sites/evo-subsites/democrats-appropriations.house.gov/files/FY23%20Summary%20of%20Appropriations%20Provisions.pdf; Further Consolidated Appropriations Act, Public Law 118-47, 138 Stat. 460 (2024), https://www.govinfo.gov/content/pkg/PLAW-118publ47/html/PLAW-118publ47.htm.

315. "Review of the Fiscal Year 2024 Unites States Agency for International Development Budget," U.S. Senate Committee on Foreign Relations, April 26, 2023, https://www.govinfo.gov/content/pkg/CHRG-118shrg53434/html/CHRG-118shrg53434.htm; "American Diplomacy and Global Leadership: Review of the FY24 State Department Budget Request."

316. U.S. Department of Justice, "Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States," press release, June 17, 2020, https://www.justice.gov/archives/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea.

317. Jonathan Barrett, "Exclusive: U.S. Warns Pacific Islands about Chinese Bid for Undersea Cable Project—Sources," Reuters, December 17, 2020, https://www.reuters.com/article/technology/exclusive-us-warns-pacific-islands-about-chinese-bid-for-undersea-cable-proje-idUSKBN28R0KW/.

318. "The United States Partners with Australia and Japan to Expand Reliable and Secure Digital Connectivity in Palau," U.S. Department of State, October 29, 2020, https://2017-2021.state.gov/the-united-states-partners-with-australia-and-japan-to-expand-reliable-and-secure-digital-connectivity-in-palau/?safe=1.

319. U.S. Department of the Interior, "Trump Administration Approves Use of $7 Million in Compact Funding to Support Palau Telecommunications Security and Resiliency," press release, July 31, 2020, https://www.doi.gov/oia/press/trump-administration-approves-use-7-million-compact-funding-support-palau.

320. Federal Communications Commission, "FCC Bans Authorizations for Devices That Pose National Security Threat," press release, November 25, 2022, https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat.

321. David Shepardson, "Biden Administration Finalizes US Crackdown on Chinese Vehicles," Reuters, January 14, 2025, https://www.reuters.com/business/autos-transportation/biden-administration-finalizes-us-crackdown-chinese-vehicles-2025-01-14/.

322. "The U.S. Department of State International Technology Security and Innovation Fund."

323. "Public Wireless Supply Chain Innovation Fund," National Telecommunications and Information Administration, accessed September 13, 2025, https://www.ntia.gov/funding-programs/public-wireless-supply-chain-innovation-fund.

324. "Bureau of Cyberspace and Digital Policy," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

325. "Office of the Special Envoy for Critical and Emerging Technology," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-special-envoy-for-critical-and-emerging-technology/.

326. "Cyberspace and Digital Policy Tradecraft," U.S. Department of State Student Information System, accessed September 13, 2025, https://sis.fsi.state.gov/MySISWeb/s/

course/a0J3d000000qVTgEAM/cyberspace-and-digital-policy-tradecraft.

327. Maggie Miller, "State Department Cyber, Tech Cuts Deeper than Previously Known," Politico, July 17, 2025, https://www.politico.com/news/2025/07/17/cyber-tech-state-ai-00460679.

328. U.S. Government Accountability Office, "Cyber Diplomacy: The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests," GAO-25-108445, April 29, 2025, https://www.gao.gov/products/gao-25-108445.

329. "Investment Strategy," Office of Strategic Capital, accessed September 13, 2025, https://www.cto.mil/osc/investment-strategy/.

330. "Investment Strategy."

331. "About the U.S. Department of State," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/about/; "Cyber Capacity Building," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/cyber-capacity-building/; "Infrastructure Transaction and Assistance Network," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/infrastructure-transaction-and-assistance-network-itan; "Infrastructure Transaction Advisory Services," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/development-finance/taf; U.S. House Committee on Appropriations, "Consolidated Appropriations Act, 2023: Summary of Appropriations Provisions by Subcommittee"; U.S. Congress, "Senate Congressional Record," *Congressional Record*, July 16, 2025, https://www.congress.gov/119/crec/2025/07/16/171/122/CREC-2025-07-16-pt1-PgS4429-4.pdf; "Functional Bureau Strategy: Bureau of Economic and Business Affairs," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/wp-content/uploads/2023/01/FBS_EB_29July2022_Public.pdf; Erin L. Murphy, "Protect, Promote, Secure: Maximizing the International Technology Security and Innovation Fund," Center for Strategic and International Studies, May 15, 2023, https://www.csis.org/analysis/protect-promote-secure-maximizing-international-technology-security-and-innovation-fund-0; Rishi Iyengar, "U.S. Adds India to Its Global Semiconductor Alliance," *Foreign Policy*, September 2, 2025, https://foreignpolicy.com/2024/09/08/us-itsi-semiconductor-chips-india-manufacturing-state-department/; "The U.S. Department of State International Technology Security and Innovation Fund"; "Office of the U.S. Special Coordinator for the Partnership for Global Infrastructure and Investment," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-u-s-special-coordinator-for-the-partnership-for-global-infrastructure-and-investment/; "Global Markets," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/global-markets; "Gold Key Service," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/gold-key-service; "International Company Profile," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/international-company-profile; "International Partner Search," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/international-partner-search; "Trade Show Representation," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/trade-show-representation; "Customized Market Research," International Trade Administration, accessed September 13, 2025, https://www.trade.gov/customized-market-research-0; "Digital Connectivity and Cybersecurity Partnership," U.S. Department of State, accessed September 13, 2025, https://www.state.gov/digital-connectivity-and-cybersecurity-partnership/; "(U) Inspection of the Bureau of East Asian and Pacific Affairs," Office of the Inspector General, U.S. Department of State, December 2021, https://www.stateoig.gov/report/isp-i-22-06; Consolidated Appropriations Act; "Foreign Commercial Service," American Foreign Service Association, accessed September 13, 2025, https://afsa.org/foreign-commercial-service; National Institute of Standards and Technology, "NIST Awards $15 Million to ASTM International to Establish Standardization Center of Excellence," press release, October 15, 2024, https://www.nist.gov/news-events/news/2024/10/nist-awards-15-million-astm-international-establish-standardization-center; U.S. Government Accountability Office, "National Institute of Standards and Technology: Improved Workforce Planning Needed to Address Recruitment and Retention Challenges," GAO-23-105521, February 28, 2023, https://www.gao.gov/products/gao-23-105521; Office of Strategic Capital, "Investment Strategy"; U.S. International Development Finance Corporation, "What We Offer"; "Investment Funds," U.S. International Development Finance Corporation, accessed September 13, 2025, https://www.dfc.gov/what-we-offer/our-products/investment-funds; "Technical Assistance and Feasibility Studies," U.S. International Development Finance Corporation, accessed September 13, 2025, https://www.dfc.gov/what-we-offer/our-products/technical-assistance-feasibility-studies; "Political Risk Insurance," U.S. International Development Finance Corporation, accessed September 13, 2025, https://www.dfc.gov/what-we-offer/our-products/political-risk-insurance; U.S. Trade and Development Agency, "About Us," accessed September 13, 2025, https://www.ustda.gov/about/; "Feasibility Studies and Technical Assistance," U.S. Trade and Development Agency, accessed September 13, 2025, https://www.ustda.gov/about-tools/feasibility-studies-and-technical-assistance/; "Pilot Projects," U.S. Trade and Development Agency, accessed September 13, 2025, https://www.ustda.gov/about-tools/pilot-projects/; "Training Grants," U.S. Trade and Development Agency, accessed September 13, 2025, https://www.ustda.gov/about-tools/training-grants/; "Reverse Trade Missions," U.S. Trade and Development Agency, accessed September 13, 2025, https://www.ustda.gov/about-tools/reverse-trade-missions/; "Global Procurement Initiative," U.S. Trade and Development Agency, accessed September 13, 2025, https://www.ustda.gov/ustda-special-initiative/global-procurement-initiative/; "About,"

Millenium Challenge Corporation, accessed September 13, 2025, https://www.mcc.gov/about/; "Compacts," Millenium Challenge Corporation, accessed September 13, 2025, https://www.mcc.gov/how-we-work/program/compact/; "Organization Chart," Millenium Challenge Corporation, accessed September 13, 2025, https://www.mcc.gov/about/org-chart/; "China and Transformational Exports Program," Export-Import Bank of the United States, accessed September 13, 2025, https://www.exim.gov/about/special-initiatives/ctep; "Tools and Products," Export-Import Bank of the United States, accessed September 13, 2025, https://www.exim.gov/leadership-governance/Congressional-Government-Stakeholders/exim-financing-tools-and-products; and "Introducing USAID Digital Policy: International Development Is Digital," ICTWorks, July 31, 2024, https://www.ictworks.org/usaid-digital-policy/; Adva Saldinger, "The Millennium Challenge Corporation will survive, but many programs might not," Devex, July 29, 2025, https://www.devex.com/news/millennium-challenge-corporation-will-survive-but-many-programs-might-not-110602.

332. U.S. Department of the Treasury, "Remarks by Deputy Secretary of the Treasury Wally Adeyemo at the 2024 Partnership for Global Infrastructure and Investment Investor Forum," press release, September 25, 2024, https://home.treasury.gov/news/press-releases/jy2610.

333. "Office of the Special Envoy for Critical and Emerging Technologies."

334. U.S. Trade and Development Agency, "USTDA, Indonesia Partner on Next Generation Network Deployment," press release, February 22, 2024, https://www.ustda.gov/ustda-indonesia-partner-on-next-generation-network-deployment/; U.S. Trade and Development Agency, "USTDA, Hexa Partner on Direct Submarine Cable Link Between Southeast Asia and United States," press release, November 15, 2023, https://www.ustda.gov/ustda-hexa-partner-on-direct-submarine-cable-link-between-southeast-asia-and-united-states/.

335. "Quad Joint Leaders' Statement," Prime Minister of Australia, May 24, 2022, https://www.pm.gov.au/media/quad-joint-leaders-statement; "Quad Leaders' Joint Statement," Prime Minister of Australia, May 20, 2023, https://www.pm.gov.au/media/quad-leaders-joint-statement; "Joint Statement From the Leaders of Australia, India, Japan, and the United States," Prime Minister of Australia, September 21, 2024, https://www.pm.gov.au/media/joint-statement-leaders-australia-india-japan-and-united-states.

336. "Quad Joint Leaders' Statement."

337. The White House, "Readout of the Quad Investors Network Event at the White House," press release, October 18, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/18/readout-of-the-quad-investors-network-event-at-the-white-house/.

338. Runde, Murphy, and Bryja, "Safeguarding Subsea Cables."

339. "Fact Sheet: Partnership for Global Infrastructure and Investment in the Lobito Trans-Africa Corridor," U.S. Embassy & Consulates in China, December 5, 2024, https://china.usembassy-china.org.cn/fact-sheet-partnership-for-global-infrastructure-and-investment-in-the-lobito-trans-africa-corridor/.

340. Brock, "U.S. and China Wage War Beneath the Waves."

341. Daniel Erikson, "China's Strategy toward Central America: The Costa Rican Nexus," Jamestown Foundation, May 27, 2009, https://jamestown.org/program/chinas-strategy-toward-central-america-the-costa-rican-nexus/.

342. Lily Hay Newman, "The US Is Sending Money to Countries Devastated by Cyberattacks," *Wired*, March 29, 2023, https://www.wired.com/story/white-house-costa-rica-albania-ransomware-aid/; Export-Import Bank of the United States, "EXIM Board of Directors Approves Preliminary Commitment to Support Development of 5G Network in Costa Rica," press release, June 9, 2023, https://www.exim.gov/news/exim-board-directors-approve-preliminary-commitment-support-development-5g-network-costa-rica.

343. Alvaro Murillo, "China Rejects Spying Concerns from Costa Rica Leader over 5G Network," Reuters, December 7, 2023, https://www.reuters.com/technology/cybersecurity/china-rejects-spying-concerns-costa-rica-leader-over-5g-network-2023-12-07/.

344. U.S. Department of State, "Joint Statement on Enhancing Digital Economy Cooperation Between the United States of America and the Republic of Costa Rica," press release, April 11, 2024, https://2021-2025.state.gov/joint-statement-on-enhancing-digital-economy-cooperation-between-the-united-states-of-america-and-the-republic-of-costa-rica/.

345. Alex Irwin-Hunt, "Costa Rican Trade Minister Warns against Huawei's 'Excessive Pressure,'" FDI Intelligence, April 17, 2025, https://www.fdiintelligence.com/content/96534606-f1a7-4904-9d96-90758cbf1086.

346. "Promoting the Export of The American AI Technology Stack," The White House, July 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/.

347. Kurt M. Campbell and Rush Doshi, "Underestimating China," *Foreign Affairs*, April 10, 2025, https://www.foreignaffairs.com/china/underestimating-china#selection-1657.31-1657.51.

348. "Facts and Figures on the European Union," European Union, accessed September 14, 2025, https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_en.

349. "New Africa-Europe Digital Economy Partnership,"

European Commission, March 8, 2021, https://international-partnerships.ec.europa.eu/document/download/bffc3bc7-b4a9-4b9a-ba5e-424873d822ab_en?file-name=new-africa-eu-digital-economy_en.pdf.

350. "Policy and Regulation Initiative for Digital Africa (PRIDA)," European Union, accessed September 14, 2025, https://international-partnerships.ec.europa.eu/policies/programming/programmes/policy-and-regulation-initiative-digital-africa-prida_en.

351. "About the D4D Hub," Global Gateway, accessed September 14, 2025, https://d4dhub.eu/who-we-are.

352. "2021 State of the Union Address by President von der Leyen," European Commission, September 14, 2021, https://ec.europa.eu/commission/presscorner/detail/en/speech_21_4701.

353. "EU-Africa: Global Gateway Investment Package," Global Gateway, accessed September 14, 2025, https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-sub-saharan-africa/eu-africa-global-gateway-investment-package_en.

354. "EU-Africa: Global Gateway Investment Package."

355. "Global Gateway," European Commission, accessed September 14, 2025, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en; Development Bank of Latin America and the Caribbean, "The EU Will Invest 45 Billion Euros in Latin America and the Caribbean," press release, July 17, 2023, https://www.caf.com/en/currently/news/the-eu-will-invest-45-000-million-euros-in-latin-america-and-the-caribbean/.

356. Gustavo Beliz, Angel Melguizo, and Victor Munez, "EU and Latin America's Great Digital Opportunity," Development Bank of Latin America and the Caribbean, October 5, 2023, https://www.caf.com/en/blog/eu-and-latin-americas-great-digital-opportunity/.

357. "Smart City & Parks," NTT, November 10, 2022, https://www.global.ntt/insights-hub/smart-city-parks/.

358. "Smart City & Parks."

359. Hiroaki Shiga, "The New Dynamics of Japan's Official Development Assistance in an Era of Great Power Competition," *Journal of Contemporary East Asia Studies* 12, no. 1 (2023): 249–263, https://doi.org/10.1080/24761028.2023.2292438.

360. "Towards Free and Open Indo-Pacific," Government of Japan, November 2019, https://www.mofa.go.jp/files/000407643.pdf.

361. David Brunnstrom et al., "Biden and Japan's Suga Project Unity against China's Assertiveness," Reuters, April 16, 2021, https://www.reuters.com/world/china/biden-welcome-japans-suga-first-guest-key-ally-china-strategy-2021-04-16/.

362. "Joint Statement on the Launch of the U.S.-Japan Global Digital Connectivity Partnership," U.S. Department of State, June 3, 2021, https://2021-2025.state.gov/joint-statement-on-the-launch-of-the-u-s-japan-global-digital-connectivity-partnership/?safe=1.

363. Shiga, "The New Dynamics of Japan's Official Development Assistance."

364. Kondoh Hisahiro, "Japan's Strategic Interests in the Global South: Indo-Pacific Strategy," Center for Strategic and International Studies, May 21, 2024, https://www.csis.org/analysis/japans-strategic-interests-global-south-indo-pacific-strategy.

365. Media Connect, "Japan's ODA Undergoes Historical Shift to a New Offer-Based Approach—The Shared Future of Asia and Japan," press release, December 16, 2024, https://mediaconnect.com/japans-oda-undergoes-historical-shift-to-a-new-offer-based-approach; Alex Willemyns, "Report: China Is Exporting Digital Control Methods," Radio Free Asia, April 17, 2024, https://www.rfa.org/english/news/china/internet-repression-exports-04172024133621.html.

366. "Stepping Up Our Engagement in the Pacific," Australian Government, 2017, https://www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/foreign-policy-white-paper/chapter-seven-shared-agenda-security-and-prosperity/stepping-our.html.

367. Colin Packham, "Ousting Huawei, Australia Finishes Laying Undersea Internet Cable for Pacific Allies," Reuters, August 28, 2019, https://www.reuters.com/article/technology/ousting-huawei-australia-finishes-laying-undersea-internet-cable-for-pacific-al-idUSKCN1VI08H/.

368. "About," Australian Infrastructure Financing Facility for the Pacific, accessed September 14, 2025, https://www.aiffp.gov.au/about.

369. "AIFFP Advances $2B Infrastructure Investment in the Pacific," Australia Pacific Islands Business Council, February 4, 2025, https://apibc.org.au/2025/aiffp-advances-2b-infrastructure-investment-in-the-pacific/.

370. Export Finance Australia, "Australia, US and Japan Announce Trilateral Partnership," press release, accessed September 14,2 025, https://www.exportfinance.gov.au/newsroom/australia-us-and-japan-announce-trilateral-partnership/.

371. Export Finance Australia, "Australia, US and Japan Announce Trilateral Partnership."

372. "The United States Partners with Australia and Japan to Expand Reliable and Secure Digital Connectivity in Palau"; Winston Qiu, "Japan, Australia, US to Fund East Micronesia Cable System (EMCS)," Submarine Cable

Networks, June 9, 2023, https://www.submarinenetworks.com/en/systems/trans-pacific/emcs/japan-australia-us-to-fund-east-micronesia-cable-system-emcs.

373. Simon Sharwood, "Pacific Telco Backed by Australia, Japan, US Bins Huawei," The Register, October 5, 2023, https://www.theregister.com/2023/10/05/digicel_pacific_nokia_replaces_huawei/; U.S. International Development Finance Corporation, "Joint Statement by Australia, Japan and the United States on Telecommunications Financing," press release, May 19, 2023, https://www.dfc.gov/media/press-releases/joint-statement-australia-japan-and-united-states-telecommunications-financing.

374. Richard Fontaine and Gibbs McKinley, "Global Swing States," Center for a New American Security, accessed September 14, 2025, https://www.cnas.org/research/global-swing-states.

375. "Promoting the Export of The American AI Technology Stack."

376. "Building Digital Solidarity: The United States International Cyberspace & Digital Policy Strategy," U.S. Department of State, May 6, 2024, https://www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/.

377. Kennedy, "Reauthorizing DFC in Lame Duck Period Avoids Disrupting an Important Foreign Policy Tool."

378. Enhancing American Competitiveness Act of 2023.

379. "The U.S. Department of State International Technology Security and Innovation Fund."

380. "The Department of State, Foreign Operations, and Related Programs: Fiscal Year 2020 Appropriations Bill."

381. "Review of the Fiscal Year 2024 Unites States Agency for International Development Budget"; "American Diplomacy and Global Leadership: Review of The FY24 State Department Budget Request."

382. Global Development Institute, "Digital Development Working Papers," accessed September 14, 2025, https://www.gdi.manchester.ac.uk/research/publications/di/.

383. International Trade Administration, "Who We Are."

384. American Foreign Service Association, "Foreign Commercial Service."

385. U.S. Government Accountability Office, "Economic and Commercial Diplomacy: State and Commerce Implement a Range of Activities, but State Should Enhance Its Training Efforts," GAO-22-104181, December 13, 2021, https://www.gao.gov/products/gao-22-104181.

386. Norges Bank Investment Management, "The Fund's Value."

387. "Promoting the Export of The American AI Technology Stack."

388. "Promoting the Export of The American AI Technology Stack."

389. "Global Gateway Projects," European Union, accessed September 14, 2025, https://international-partnerships.ec.europa.eu/policies/global-gateway/global-gateway-projects_en.

390. "EU-LAC Global Gateway Investment Agenda—Infographics," European Union, July 17, 2023, https://international-partnerships.ec.europa.eu/publications-library/eu-lac-global-gateway-investment-agenda-infographics_en.

391. Digital Development, "What Is a DECA?"

392. David Shepardson, "US Imposing New Export Controls on Biotech Equipment over China Concerns," Reuters, January 15, 2025, https://www.reuters.com/technology/us-imposing-new-export-controls-biotechnology-equipment-2025-01-15/; "Commerce Announces New Trade Controls Affecting Quantum Technologies and AI Developers," Morrison Foerster, September 12, 2024, https://www.mofo.com/resources/insights/240912-recent-ai-and-advanced-technologies-developments.

393. Bhattacharjee et al., "Chinese Rivals to Musk's Starlink Accelerate Race to Dominate Satellite Internet."

394. "Submarine Cable Frequently Asked Questions"; "Experience," HMNTech, accessed September 14, 2025, https://www.hmntech.com/enExperience.jhtml.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.

©2025 Center for a New American Security

All rights reserved.

CNAS Editorial

DIRECTOR OF STUDIES
Katherine L. Kuzminski

PUBLICATIONS & EDITORIAL DIRECTOR
Maura McCarthy

SENIOR EDITOR
Emma Swislow

ASSOCIATE EDITOR
Caroline Steel

CREATIVE DIRECTOR
Melody Cook

DESIGNER
Alina Spatz

Cover Art & Production Notes

COVER ILLUSTRATIONS FOR THE SERIES
Rin Rothback, Melody Cook, and Alina Spatz

PRINTER
CSI Printing & Graphics
Printed on an HP Indigo Digital Press

Center for a New American Security
1701 Pennsylvania Ave NW
Suite 700
Washington, DC 20006
CNAS.org
@CNASdc

CEO
Richard Fontaine

Executive Vice President & Director of Studies
Paul Scharre

Senior Vice President of Development
Anna Saito Carson

Contact Us
202.457.9400
info@cnas.org

Center for a
New American
Security