MICHAEL J. MAZARR, HABIBA AHMED, MARZIA GIAMBERTONI, SHEA HENDERSON,
ROBERT ULRICH NAGEL, CHRISTIAN TROTTI

The Emerging Digital Battleground

The Critical Factors That Produce Advantage in the U.S.-China Competition for Digital Networks, Annex

This research was independently initiated and made possible by RAND's own resources, including income from operations, unrestricted gifts from RAND supporters, and distributions from its long-term investment fund.

Annex

For more information on this publication, visit **www.rand.org/t/RRA4569-1**.

About RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our research integrity is grounded in RAND's core values of quality and objectivity. Rigorous quality assurance procedures, conflict of interest screening, and transparency in funding ensure that every study is objective and nonpartisan. Learn more at www.rand.org/integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.
© 2026 RAND Corporation
RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, visit www.rand.org/about/publishing/permissions.

RR-A4569-2

About This Annex

In this annex, we provide detailed analysis and case studies related to our report examining what determines success in the U.S.-China competition for influence over global digital networks. In the appendixes presented here, we define the competition for digital networks in 2026, discuss four primary components of such networks, and offer case studies of those components and of the competitions unfolding in three select countries and one technology area. The main report is available at www.rand.org/t/RRA4569-1.

China Research Center

RAND Global and Emerging Risks is a division of RAND that delivers rigorous and objective public policy research on the most consequential challenges to civilization and global security. This work was undertaken by the division's China Research Center, which seeks to improve U.S., ally, and partner policymaker and their publics' understanding of the People's Republic of China.

Funding

This research was independently initiated and conducted within the China Research Center using a gift from philanthropist Michael Tang, as well as gifts from other RAND supporters and income from operations. RAND donors and grantors have no influence over research findings or recommendations.

Acknowledgments

We acknowledge the generous support of the China Research Center, and its director Jude Blanchette and associate director Gerard DiPippo, in making this research possible, and we thank Jude for his helpful comments on an earlier draft. We are grateful to Jeffrey B. Wenger and Richard Williamson for their thoughtful peer reviews.

Contents

About This Annex iii
Figure and Tables v
Appendix A. A Snapshot of the Competition for Digital Networks in 2026 1
Telecommunications Networks 1
Cloud Computing and Data Centers 5
Space Systems 8
Undersea Cables 10
Summary: The Status of the Competition for Digital Networks 13
Appendix B. Evaluating the Priority Areas: Factors Influencing Success 14
Physical Connectivity and Infrastructure 14
Wireless and Internet of Things Networks and Infrastructure 22
AI Infrastructure and Data Ecosystems 29
Cooperative Space Programs 35
Appendix C. Country and Functional Issue Case Studies 43
Costa Rica 43
Nigeria 48
The Philippines 52
Serbia 58
Undersea Cables 62
Abbreviations 72
References 74

Figure and Tables

Figure

Figure A.1. Global Huawei Deployment Status, October 2025 3

Tables

Table A.1. 5G Patents 5
Table A.2. AI Compute Data Centers—Vendor Focus 6
Table A.3. Data Center Capacity, by Availability Zone 7
Table A.4. Undersea Cable Suppliers Global Market, December 2025 11
Table A.5. Undersea Cable Providers: Systems Planned for 2026 to 2029 12
Table C.1. Comparison of Key Metrics in Undersea Cable Supply and Installation Market 63
Table C.2. Comparison of Insights Across Case Studies 70

Appendix A. A Snapshot of the Competition for Digital Networks in 2026

This study is not primarily concerned with a net assessment of the competition for global digital network power. Our main purpose is to identify the factors leading to U.S., Chinese, or other national success in winning market share, profit, and other indicators of network influence. We did, however, survey the existing literature for information about trends in this contest. Understanding broadly where the competition stands can provide important insight into the potential importance of different factors. In this appendix, we survey some of the current evidence in four domains of digital competition: telecommunications networks, cloud computing and data centers, space systems, and subsea cables.

Telecommunications Networks

The story of telecommunications rivalries over the past several years is straightforward. It involves the rise of Huawei through a seemingly unmatched set of cost and quality advantages; major pushback against that Chinese firm by companies concerned about Chinese government access to data; a significant hit to Huawei's ascent; and then a steadying of its global position with the potential for making further progress.

By 2017, Huawei had attained a dominant position in domestic Chinese 5G markets and a growing position in global markets, in both developed and developing countries.[1] Citing concerns over espionage, intellectual property theft, and Huawei's alleged ties to the Chinese Communist Party, a growing number of countries began imposing restrictions on the company's involvement in 5G infrastructure development.[2] The United States has taken the most aggressive stance by adding Huawei to the Commerce Department's Entity List, prohibiting U.S. firms from doing business with the company without government approval, and extending these controls by restricting foreign semiconductor manufacturers that rely on U.S. equipment or software from supplying Huawei.[3]

In 2020, Washington further escalated its campaign by launching the Clean Network initiative, an effort to assemble a coalition of governments and telecommunications providers committed to "secure" digital infrastructure by excluding vendors deemed untrustworthy, such as

[1] Yap, "State Support Helped Fuel Huawei's Global Rise."

[2] Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"

[3] Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"

Huawei and ZTE.[4] The initiative sought not only to align governments but also to influence private-sector vendor relationships, encouraging major telecom operators (such as Jio in India and KT in South Korea) to avoid Chinese suppliers in next-generation network deployments.[5]

Restrictions on Huawei have been especially pronounced among members of the Five Eyes intelligence alliance—the United States, Australia, Canada, New Zealand, and the United Kingdom—all of which have banned Huawei equipment from their 5G networks.[6] Japan and Taiwan have adopted similar approaches, prohibiting Huawei from government contracts, with Taiwan actively removing existing Huawei equipment from public systems.[7] Across Europe, a growing number of countries, including Belgium, the Czech Republic, Estonia, France, Germany, Luxembourg, Poland, Portugal, Romania, and Sweden, have implemented varying degrees of restrictions under the framework of the European Union's (EU's) 5G Cybersecurity Toolbox, particularly targeting high-risk vendors in core network components.[8] In January 2026, the EU took a further step by releasing a draft proposal that would mandate the phaseout of equipment from high-risk suppliers.[9] This proposal would be mandatory, requiring mobile operators to remove key components from designated vendors within 36 months of the publication of an official high-risk supplier list.[10]

Despite these restrictions, Huawei continues to maintain a substantial global presence in 5G deployment. According to publicly available data on vendor selection and announced deployment plans, approximately 109 countries are using or are likely to use Huawei technologies in their 5G networks. By contrast, 27 countries appear unlikely to adopt Huawei equipment, while 17 countries have implemented partial restrictions or outright bans on the company's participation in their 5G ecosystems (see Figure A.1). As one recent study reported,

> As of September 2025, over 3.2 billion people outside China resided in countries that use 5G networks that rely on Huawei equipment, while another 370 million live in countries where Huawei is not banned but is absent from their 5G networks. Huawei remains embedded in the 5G networks of nine U.S. allies—Hungary, Iceland, Italy, South Korea, Spain, the Netherlands, the Philippines, Thailand, and Turkey—and is being phased out from six others: Belgium, France, Germany, Poland, Romania, and the United Kingdom. Among the rest,

[4] U.S. Department of State, "The Clean Network."

[5] U.S. Department of State, "The Clean Network."

[6] Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"

[7] Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"

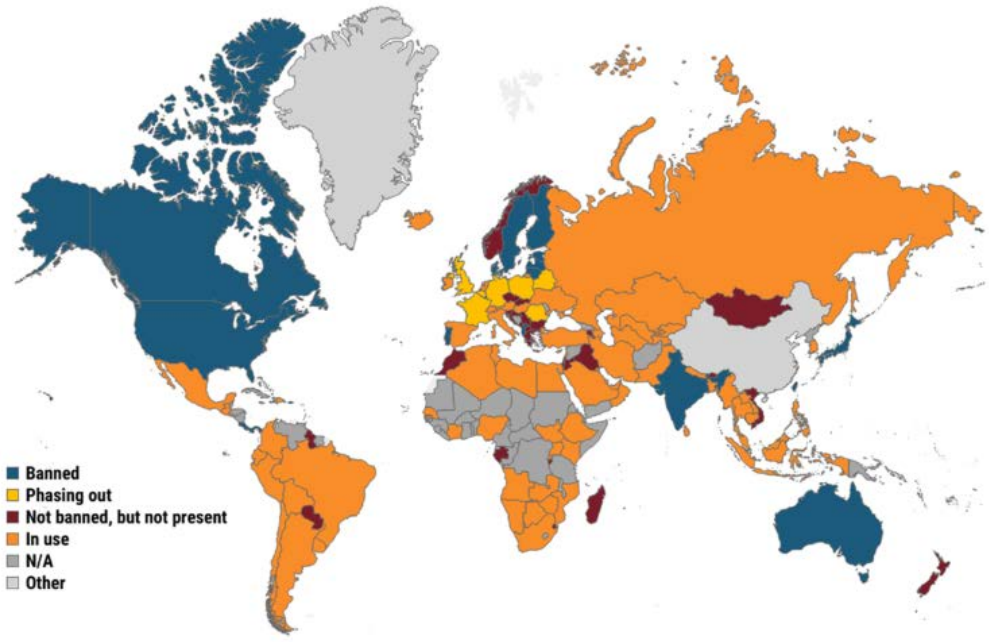
[8] Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"

[9] Chee, "EU Plan to Phase-Out High-Risk Tech Draws Fire from China's Huawei."

[10] Chee, "EU Plan to Phase-Out High-Risk Tech Draws Fire from China's Huawei"; "EU Moves to Force the Phase-Out of Chinese Suppliers from Key Infrastructure, FT Reports."

Huawei's 5G is banned in 12 countries, and 10 countries have excluded the company without the need for a ban.[11]

Figure A.1. Global Huawei Deployment Status, October 2025



SOURCE: Reproduced from Balbontin, "Backfire," Figure 1 (CC BY 4.0).

Most telecommunications products targeted at wireless networks fall into the category of radio access network (RAN) equipment, which includes the hardware and software used in macro and small cell base stations and represents the critical layer that connects wireless devices to operators' core networks. The global RAN equipment market is highly concentrated. In 2024, five vendors, Huawei, Ericsson, Nokia, ZTE, and Samsung, collectively accounted for 93.7 percent of global RAN revenue.[12]

As of mid- to late 2025, Huawei remained competitive in many global markets. According to data as of mid-2025, the firm was the leading RAN vendor in Asia and Oceania, the Middle East and Africa, and Latin America and the Caribbean. Even in Europe, major telecommunications providers in Spain and the EU, including Deutsche Telekom and Vodaphone, continue to employ Huawei systems.[13] Overall, 2025 saw mostly stable global market position for the European 5G

[11] Balbontin, "Backfire," p. 6.

[12] Balbontin, "Backfire."

[13] Morris, "Huawei Overtakes Nokia Outside China as Open RAN 'Stabilizes.'" An example of these tensions emerged recently with Huawei's role in the 2026 Mobile World Congress meeting held in Barcelona, where the firm's offerings were on prominent display, and some countries, notably Spain, openly admitted the difficulty of

providers and some growth for Huawei. Outside China, Ericsson remains the top RAN vendor, with Huawei second and Nokia third.[14] Huawei remained "the world's largest provider of 5G networks and a dominant player in telecom equipment" and had driven many U.S. firms—Motorola, Cisco, and Lucent—out of the industry altogether.[15] China is gaining momentum in other areas of telecommunications connectivity as well. As a 2026 Rhodium Group report concluded,

> The connectivity layer is highly contested, with the G7+ (Group of Seven Plus) and China each dominating within their increasingly protected home markets and competing for share in non-aligned third markets. However, the growth trajectory has favored China for the past two decades. Starting from zero in the 2000s, China now matches the G7+ in global RAN equipment sales and is highly competitive in other key network equipment categories spanning optical transport, routers, subsea and terrestrial cabling. China's emergence as a leading provider of full-stack communications networks benefitted from a decades-long industrial policy push to build up local champions within China's large, and increasingly protected, home market in the first instance before promoting their expansion abroad with generous export financing and coordinated diplomatic support.[16]

Ownership of 5G standard-essential patents (SEPs) enables firms to not only collect licensing royalties but also to shape the technical trajectory of the global wireless ecosystem as it evolves toward 5G-Advanced and ultimately 6G. Control over SEPs translates into agenda-setting power within standards bodies, influence over interoperability decisions, and long-term leverage over downstream markets.[17] As of 2025, just six countries (China, South Korea, the United States, Japan, Sweden, and Finland) collectively account for more than 90 percent of all declared 5G SEPs. China holds a commanding lead with approximately 40.8 percent of global SEPs, followed by South Korea at 18 percent and the United States at 15.1 percent. At the firm level, SEP ownership is also highly concentrated, with the top ten patent holders controlling roughly 75 percent of all 5G SEPs (see Table A.1). By contrast, U.S. leadership is more narrowly anchored in Qualcomm, the second largest holder of 5G SEPs with almost 10 percent.

---

weaning themselves of its technology despite a wider European effort to constrain its position in their networks. See Pollet, "China's Huawei Dominates Telco Jamboree Despite European Bans."

[14] Wooden, "Huawei Makes RAN Gains in Several Global Regions."

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

[16] Goujon et al., *Fighting Hubris in AI Strategy*, pp. 30–31.

[17] The figures in this paragraph are drawn from LexisNexis, "Who Is Leading the 5G Patent Race?"

Table A.1. 5G Patents

Owner	Headquarters	SEP Count	Percentage of Total
Huawei	Shenzhen, China	8,408	15.0
Qualcomm	California, United States	5,487	9.8
Samsung	Seoul, South Korea	4,770	8.5
LG	Seoul, South Korea	4,744	8.5
Ericsson	Stockholm, Sweden	4,160	7.4
ZTE	Shenzhen, China	3,564	6.4
Nokia	Espoo, Finland	3,004	5.4

SOURCE: Features information from Spaargaren, *The World's Leading 5G Patent Owners*.

These figures measure declared SEP ownership, which indicates the volume of patenting activity directed at 5G standardization but is an imperfect proxy for technological leadership or commercial influence. Declaration is a self-reported process, as firms notify standards bodies of patents they believe may be essential, and those declarations are not examined for essentiality at the time of filing. Because declared patents may not be in fact essential to the standard, and because over-declaration practices vary across firms and jurisdictions, raw counts may not be directly comparable across countries. Count alone also does not capture value because patents differ in scope and in the centrality of the technology they cover, so a smaller portfolio anchored in foundational technologies may generate more royalty revenue and more leverage in cross-licensing than a larger portfolio of narrower claims.

Western controls on Huawei have therefore succeeded in constraining its expansion in advanced economies but have fallen well short of undermining the company as a global competitor. By concentrating on its domestic market, advancing 6G innovation, and generating revenue in non-U.S.-aligned markets, Huawei and ZTE have preserved the technological leadership and production scale needed to compete internationally.[18] As much progress as Huawei has made, however, and as dominant as its position has become among developing countries, several major countries have barred it from significant components of their digital networks, and the competition for 6G networks could partially reset the global landscape—if the United States and others compete effectively in that space.

Cloud Computing and Data Centers

In the cloud computing and data center context, U.S. firms retain a far stronger position, a product of both technological quality and path dependence of reliance on U.S. providers. One

[18] Balbontin, "Backfire."

prominent though incomplete database has identified 11,631 publicly listed data centers globally.[19] Of these, more than 46 percent are in the United States, while approximately 4 percent are in China. The data also show a broad international distribution, with five other countries or regions hosting more publicly listed data centers than China, including the EU, which accounts for nearly 20 percent of the total. Of the top ten data center operators in each region, U.S. firms operate about 1,200 of the 1,800 total facilities. This concentration underscores the dominance of U.S. firms in the global data center market, particularly among large-scale operators, and highlights how global digital infrastructure remains heavily centered in a small number of advanced economies.

A census of nine leading public cloud providers—three U.S. (Amazon Web Services [AWS], Google Cloud, Microsoft Azure), three Chinese (Alibaba Cloud, Huawei Cloud, Tencent Cloud), and three European (Exoscale, Hetzner, OVHcloud)—mapped 225 cloud regions across 43 countries as of November 2024.[20] Of the 132 AI-enabled cloud regions identified globally, U.S. providers operate 87 (66 percent), including 24 domestic and 61 international, while Chinese providers operate 39 (30 percent), 20 domestic and 17 international (see Table A.2). This distribution highlights the U.S. lead in both total AI-capable regions and its greater global reach, with U.S. providers present in more than three times as many foreign regions as Chinese providers. Across the nine leading cloud providers, the United States clearly outpaces China in global AI data center infrastructure.

Table A.2. AI Compute Data Centers—Vendor Focus

Location	U.S. Providers	Chinese Providers
USA	24	2
China	2	20
International	61	17
Total	**87**	**39**

SOURCE: Features data from Cloudscene, “North America.”

[19] Cloudscene maintains a market-driven global database of data centers compiled from a combination of crowd-sourced submissions, operator-claimed listings, and publicly available information (including company disclosures and industry announcements). As a result, the dataset primarily captures commercially relevant facilities, notably colocation data centers and cloud provider–operated facilities that are publicly listed or market-facing. It does not systematically include private enterprise data centers, confidential hyperscale sites, or facilities that operators choose not to disclose, meaning that the database reflects the publicly visible commercial ecosystem rather than a comprehensive physical census of all data centers worldwide. See Cloudscene, “North America.”

[20] The dataset was constructed using publicly available information from cloud providers’ websites and customer interfaces. *Cloud regions*, defined as concentrated clusters of interconnected data centers, were assessed for AI accelerator capacity, categorized as training-relevant (capable of supporting frontier-scale AI models) or inference-relevant (primarily for serving trained models). The dataset represents approximately 70 percent of the global cloud market and 78 percent of infrastructure spending.

In an analysis of *availability zones*, the physically distinct data centers within each cloud region, a more granular view of AI infrastructure capacity can be seen. U.S. providers account for nearly 62 percent of all availability zones among the nine leading cloud providers, while Chinese providers operate roughly 36 percent (see Table A.3). This demonstrates that U.S. companies not only control more AI-enabled regions but also maintain greater density within each region, further amplifying their overall compute capacity.

Table A.3. Data Center Capacity, by Availability Zone

Companies	Availability Zones	Percentage of Total
Microsoft	93	23.72
AWS	84	21.43
Google	66	16.84
		61.99
Alibaba	61	15.56
Huawei	44	11.22
Tencent	38	9.69
		36.47
OVHcloud	5	1.27
Exoscale	1	0.26
Total	392	100.00

SOURCE: Features information from Satariano and Mozur, "The Global A.I. Divide."
NOTE: The blue shaded row identifies the United States' percentage of the total data center availability zones. The red shaded row identifies China's percentage of the total data center availability zones.

Although available information on relative AI infrastructure buildout is limited and counts of publicly listed data centers, cloud regions, and availability zones indicate infrastructure presence and geographic reach, it is important to note that these do not measure deployed compute capacity, utilization rates, or market share. Availability zones vary considerably in physical size, power draw, and compute density, so a zone operated by one provider is not equivalent to a zone operated by another. The convergence of these presence-based indicators strengthens the overall inference, but these indicators are not a direct measure of deployed compute.

Space Systems

The United States' Global Positioning System (GPS) constellation consists of 31 operational satellites in medium earth orbit (MEO) at an altitude of approximately 20,200 km.[21] These satellites are arranged within a 27-slot configuration, with four additional satellites available to ensure continuous service or replace decommissioned units.[22] GPS provides real-time positioning accuracy of about 4.9 m for smartphone users, and, in 2021, it served an estimated 4 billion users worldwide.[23] However, updated statistics are difficult to determine because most modern devices now support multiple global navigation satellite system (GNSS) constellations to achieve enhanced accuracy.

China's BeiDou (北斗) Navigation Satellite System achieved full global operational capability in 2020 with more than 40 satellites in a hybrid constellation, including 28 in MEO, seven in geostationary orbit (GEO), and ten in inclined geosynchronous orbit (IGSO) as of January 2026.[24] The People's Republic of China (PRC) presents BeiDou's independent innovation as its core competitive advantage, emphasizing that autonomy in research, design, construction, and operation has ensured that critical technologies remain domestically developed and controlled.[25] This commitment to self-reliance has enabled BeiDou to offer distinctive capabilities, such as Short Message Service (SMS), ground- and satellite-based augmentation, and international search and rescue services.[26] Although the BDS-3 constellation only became fully operational in 2020, BeiDou serves more than 2 billion users worldwide and has introduced functionalities that in some respects surpass those of GPS, and its satellites are observed more frequently than GPS satellites in 130 of 195 countries.[27] It has been noted that the BeiDou system and related technology service more than 140 countries and regions around the world.[28]

These numbers indicate the reach of GPS and BeiDou signals and the prevalence of systems-capable hardware, but they do not themselves establish reliance on Chinese space infrastructure for positioning. Contemporary GNSS receivers are typically multi-constellation, tracking GPS, Galileo (EU), GLONASS (Russia), and BeiDou simultaneously and computing a blended position solution. Similarly, the frequency with which satellites are observed reflects

---

[21] Pollpeter, "To Be More Precise."

[22] GPS, "Space Segment."

[23] Pollpeter, "To Be More Precise."

[24] The total operational number is always changing with new launches and decommissions. See Space-Track.org, "Query Builder."

[25] State Council Information Office of the People's Republic of China, "China's BeiDou Navigation Satellite System in the New Era."

[26] State Council Information Office of the People's Republic of China, "China's BeiDou Navigation Satellite System in the New Era."

[27] Pollpeter, "To Be More Precise."

[28] "The Output Value of Our Country's Satellite Navigation Industry Reached 575.8 Billion Yuan."

constellation size and orbital geometry rather than the extent to which receivers depend on those signals. A constellation's claim to serve a given number of countries likewise often denotes signal availability or cooperation agreements rather than operational dependence.

In broadband communications and space-terrestrial integration, the United States currently leads in scale, maturity, and global reach, while satellite navigation is more closely contested given BeiDou's global reach. China is also actively pursuing a vertically integrated, state-directed model that seeks to reduce foreign dependence and embed Chinese satellite systems into national and partner-country digital ecosystems.

Navigation: GPS remains the world's dominant GNSS, acting as the default system for all countries and serving an estimated 4 billion users globally. Yet its constellation design and functionality are becoming outdated, operating as a one-way system, reliant on extensive ground infrastructure, and lacking messaging capabilities, intersatellite links, or integrated search-and-rescue functions. China's BeiDou system offers a more multifunctional alternative: a hybrid constellation with built-in SMS, intersatellite links, and search-and-rescue capability. These features give BeiDou competitive advantages in underserved and infrastructure-poor regions.

Broadband: The United States holds a decisive lead in low earth orbit (LEO) broadband. SpaceX's Starlink has achieved unmatched scale, deployment tempo, and operational maturity with thousands of satellites in orbit, millions of users, and an expansive global gateway network. Amazon's Leo and Eutelsat's OneWeb further reinforce U.S. and allied dominance while adding competitive diversity. Chinese LEO constellations, including Guowang and Qianfan, remain in early deployment and lag significantly in both scale and adoption. While China has announced ambitious targets, often matching or exceeding Western plans on paper, actual deployment has been severely constrained.

Space-terrestrial integration: The United States pioneered data relay systems through the National Aeronautics and Space Administration's (NASA's) Tracking and Data Relay Satellite System (TDRSS), but the constellation is aging and technologically constrained. The United States has taken measures to introduce commercial actors and outsource modernization to private firms, yet the U.S. system still lags China's. China's Tianlian system, though smaller, is newer and increasingly capable. It provides Beijing with greater autonomy over satellite data flows and tighter integration with its growing LEO constellations. It can thus support a broader strategy of creating an ecosystem of space capabilities: satellite manufacturing, launch, ground stations, remote sensing, BeiDou, lunar communications, LEO broadband, cloud and data services, and eventually space-based data relay. Tianlian plays a critical role by offering an advanced relay system and reducing dependence on ground stations.

The United States is advancing direct-to-device satellite connectivity through commercial partnerships, enabling incremental extensions of terrestrial networks without restructuring existing telecom systems. China, by contrast, is embedding satellite communications into national industrial policy. China's Ministry of Industry and Information Technology has explicitly directed integration with 5G, future 6G architectures, and artificial intelligence (AI).

China's licensing of state-owned telecom operators to provide satellite mobile services, combined with operational GEO systems, suggests a coordinated effort to build a sovereign communications stack spanning space and ground.

The United States continues to dominate the operational space-based digital network ecosystem, but China is taking decisive action to close the gap. Beijing is not merely developing functionally competitive systems; it is building a unified, interoperable architecture designed for international deployment. China will continue advancing its technological edge through sustained research and development (R&D) while signaling global ambition, as evidenced by its filing with the International Telecommunication Union for more than 180,000 satellite slots.[29] Yet despite these announcements, actual satellite deployment remains constrained, reflecting a persistent gap between declared intentions and operational reality.

Undersea Cables

A fourth component of the digital network competition is undersea cables. As of December 2025, there are approximately 570 installed and active undersea cable systems worldwide, with an additional 81 systems planned.[30] Many of the installed systems are small, localized networks for which limited public information is available. But we were able to identify almost 400 total active systems to specific suppliers. These traced systems account for roughly 1,465,842 km of submarine cable out of a total global installed length of approximately 1,559,073 km.[31] In other words, systems with identifiable suppliers represent more than 94 percent of the total installed cable length.

The undersea cable supply and installation market is highly concentrated and, as noted in Table A.4, dominated by three firms. France's Alcatel Submarine Networks (ASN) is the market leader, having installed more than one-third of global undersea cable infrastructure, measured both by number of systems (37.53 percent) and total cable length (39.42 percent). The United States' SubCom is the second-largest supplier, accounting for 18.36 percent of systems but a substantially larger 33.90 percent of total cable length, reflecting its specialization in fewer, longer-distance routes compared with ASN. Japan's Nippon Electric Company (NEC) ranks third, installing 13.23 percent of systems and 16.21 percent of total cable length. Collectively, these three suppliers have installed nearly 70 percent of all submarine cable systems and more than 85 percent of total deployed cable length. China's most prominent supplier, HMN Tech, remains a developing firm in the undersea cable market. To date, it has installed 10.09 percent of global systems but only 4.72 percent of total deployed cable length, indicating a focus on shorter regional routes relative to the leading suppliers. There exist cable systems that were installed by

[29] Jones, "China Files ITU Paperwork for Megaconstellations Totaling Nearly 200,000 Satellites."

[30] TeleGeography, "Submarine Cable Frequently Asked Questions."

[31] TeleGeography, "Submarine Cable Frequently Asked Questions."

more than one supplier. Where public information permitted, we apportioned between suppliers according to the share of the route's geographic distance each contributed; where it did not, we divided both the system and its length equally among the participating firms.

Table A.4. Undersea Cable Suppliers Global Market, December 2025

Undersea Cable Supplier	Headquarters	Number of Systems	Percentage of Total Systems	Total Distance of Cables (km)	Percentage of Total Distance
ASN	Paris, France	145.04	37.53	577,878	39.42
SubCom	Eatontown, New Jersey, United States	70.96	18.36	496,900	33.90
NEC	Tokyo, Japan	51.11	13.23	223,018	15.21
HMN Tech	Tianjin, China	39	10.09	69,172	4.72
Prysmian	Milan, Italy	35	9.06	37,444	2.55
Ericsson	Stockholm, Sweden	11	2.85	2,514	0.17
Nexans	Paris, France	12	3.11	6,372	0.43
Fujitsu	Kawasaki, Japan	5.33	1.38	35,634	2.43
Hexatronic	Gothenburg, Sweden	7	1.81	1,068	0.07
ZTT	Nantong, China	3	0.78	2,191	0.15
Hellenic	Athens, Greece	2	0.52	274	0.02
CCSI	Beijing, China	2	0.52	150	0.01
JSC Optic	Saransk, Russia	1	0.26	12,650	0.86
Padtec	São Paulo, Brazil	1	0.26	390	0.03
AT&T SSI	Dallas, Texas, United States	1	0.26	187	0.01
Total		386.44		1,465,842	

SOURCE: Features data from TeleGeography, "Submarine Cable Map."
NOTE: The blue shaded rows identify U.S. companies; red shaded rows identify Chinese companies.

As noted in Table A.5, according to information on planned installations as of December 2025, this balance of influence is set to remain roughly consistent over the next three years. The quality and reliability advantages of U.S., European, and Japanese firms, in the context of broader geopolitical issues with Chinese oversight of data transmission, are so far preventing more-dramatic Chinese gains in the sector. China has a major initiative underway to build ties

with Global South countries in undersea cable projects and related areas,[32] but it remains unclear how much headway it can gain given long-term commitments in place. However, if China applies powerful industrial policy levers to this and related areas, it could potentially gain ground on Western suppliers by offering cheaper options tied into compelling ecosystems of advantage.

Table A.5. Undersea Cable Providers: Systems Planned for 2026 to 2029

Undersea Cable Supplier	Headquarters	Number of Systems	Percentage of Total Systems	Total Distance of Cables (km)	Percentage of Total Distance
ASN	Paris, France	17	34.00	84,220	27.94
SubCom	Eatontown, New Jersey, United States	16	32.00	145,903	48.41
NEC	Tokyo, Japan	6	12.00	47,382	15.72
HMN Tech	Tianjin, China	4	8.00	17,338	5.75
Prysmian	Milan, Italy	6	12.00	6,424	2.13
Hexatronic	Stockholm, Sweden	1	2.00	130	0.04
Total		50		301,397	

SOURCE: Features data from TeleGeography, "Submarine Cable Map."
NOTE: The blue shaded row indicates a U.S. company; the red shaded row identifies a Chinese company.

China's position in this market remains structurally constrained in important ways. HMN Tech has increased its activity in recent years and now accounts for roughly 10 percent of systems, yet its share of deployed cable length remains below 5 percent, indicating a focus on shorter, regional routes. Political pressure, export controls, and security concerns among Western governments have further restricted HMN's ability to compete for high-value global projects. Planned systems through 2029 suggest that HMN Tech will continue to maintain approximately 10 percent of systems and 5 percent of cable length. Meanwhile, Western governments have moved to secure greater control over the market. France's government effectively nationalized ASN in 2024, U.S. national security–focused private equity firm Cerberus acquired SubCom in 2018, and Japan's government has substantially increased subsidies to NEC. These developments signal a growing consensus that subsea connectivity constitutes a critical national security interest requiring direct government support.

These supplier and pipeline metrics capture distinct aspects of participation in the subsea markets—manufacturing and installation capability—but they do not themselves indicate ownership, operational control, traffic routing, or data access. Manufacturing covers the production of the cable equipment and is where supplier share is measured. Installation is often performed by the same firm but relies on a separate asset base of specialized cable-laying

[32] Goujon et al., *Fighting Hubris in AI Strategy*, p. 35.

vessels, whose availability is itself a constraint on who can execute large projects. Ownership rests with the consortium of carriers and content providers that finances the system and contracts with the supplier, so the choice of supplier does not determine which countries' operators hold equity stakes. Operation encompasses the landing stations, the terrestrial network connecting them, and the network operation centers that manage capacity and routing.

Summary: The Status of the Competition for Digital Networks

China has made tremendous progress in the competition for key elements of global digital networks, especially in 5G telecommunications. The United States and its allies retain a sizable lead in many of those elements, as well as inherent technological advantages in such areas as space and cables. China is investing heavily in those technologies, however, and using subsidized and integrated package offers—as it has done in 5G—to make its offerings more appealing.

The contest, in short, is live, and its outcome is far from settled. China is pouring tens of billions into securing dominance over these networks, and the 5G experience makes clear that beating it back will demand a coordinated U.S. response across every instrument of statecraft. To build that strategy, U.S. public- and private-sector leaders need to understand what drives success in these competitions.

The United States and its allies are not going to eliminate China's influence across the components of global digital networks. In some cases, such as 5G, they are not likely to gain a majority share of third-country networks. In all the areas assessed here, from 5G to space systems to cable systems, the future will reflect a complex balance of positions and influence rather than a binary victory or loss for either side.

Appendix B. Evaluating the Priority Areas: Factors Influencing Success

As noted in Chapter 2, we applied several criteria of importance to identify four domains of the digital network competition for closer analysis: physical connectivity and infrastructure, wireless and Internet of Things (IoT) connectivity and standards, AI infrastructure and data systems, and space systems. This appendix provides those more detailed assessments. Because the elements of the domains are distinct, each of the sections below approaches its subject with a distinct analytical framework. But each concludes with a section on the factors that govern success in its domain and a short summary of the major lessons of that domain analysis. Those specific findings were incorporated into Chapter 3.

Physical Connectivity and Infrastructure

Any robust analysis of the competition to shape *digital* networks must begin by addressing traditional *physical* infrastructure. Indeed, the planning and facilitation of physical infrastructure projects as tools of statecraft—from the United States' Marshall Plan to China's Belt and Road Initiative (BRI)—both precede and set the strategic context for today's competition in digital infrastructure. And most importantly, physical infrastructure is itself a critical component of digital networks, embodying the hardware that both enables software innovations and transmits data and energy in the digital age.[33] In this appendix, we assess the key factors shaping the U.S.-China rivalry in physical connectivity and infrastructure across three facets.

First, undersea and terrestrial *fiber-optic cables*, also known as "optical core infrastructure,"[34] play a central role in global communications. These cables are composed of thin glass fibers that transmit and amplify light from laser-based modems. With each fiber capable of carrying tens of terabits of data per second, the cables can ferry vast amounts of information at incredible speeds and very low latency. Undersea cables represent the primary connective tissue of this infrastructure, connecting continents via landing points that link to "terrestrial backhaul networks."[35] Because of their cost effectiveness relative to wireless and satellite communications,[36] undersea cables are responsible for transmitting 95 percent to 99 percent of

[33] For more on the relationship between software and hardware, see Brackup, Harting, and Gonzales, *Digital Infrastructure and Digital Presence*.
[34] Botting and Jordan-Zoob, "Optical Core Infrastructure."
[35] Botting and Jordan-Zoob, "Optical Core Infrastructure."
[36] Burningham, "Why Microsoft and Facebook Are Building a Superfast Trans-Atlantic Cable."

intercontinental data,[37] valued at trillions of dollars per day. However, given the relatively small number of undersea cables,[38] the narrow market of cable manufacturing and repair firms,[39] and the vulnerability of these cables to accidental and intentional disruptions, there are grave concerns about the resilience of these communications chokepoints.

If data represent one of the major commodities of the digital age, then energy is another. *Energy infrastructure* supports many cutting-edge technologies, including by powering the following: the management of mobile data traffic for wireless 5G networks;[40] the computational might necessary to train and apply AI models;[41] and the launch, propulsion, and energy storage and transmission requirements of sophisticated space missions and satellite architectures.[42] Thus, domestic and global energy infrastructure serves as a physical enabler of digital connectivity.[43] This infrastructure includes plants and facilities to extract natural resources (e.g., oil rigs, critical minerals mines), refine or transform those resources into energy (e.g., oil refineries, nuclear reactors, solar panels, wind turbines), and store and transmit energy within and across countries (e.g., electricity grids, power plants, gas pipelines, liquid natural gas terminals). Moreover, this infrastructure is not only an enabler of digital innovation but also a beneficiary, as IoT sensors, AI-enabled data analytics, and decentralized digital monitoring and energy management systems can vastly improve the efficiency of energy plants.[44]

Finally, unlike optical and energy infrastructure, *transportation infrastructure* does not produce the inputs that directly enable today's leading digital technologies. However, ports, airports, bridges, roads, and railroads—as well as the logistical systems and international regimes that underpin them—continue to play a critical role in global trade and can therefore (more indirectly) supply the financial, physical, and human capital necessary for growth in emerging technology markets. But perhaps most interestingly, like its energy counterpart, transportation infrastructure is a major beneficiary of the digital revolution, as such systems as traffic control and supply management can enjoy greater productivity through digital augmentation.[45]

This section does not cover the bespoke physical infrastructure that underpins emerging technology stacks, such as 5G and 6G base stations and AI data centers. Whereas these latter infrastructure components bear the dedicated purpose of advancing their respective digital

---

[37] *Wall Street Journal*, "The Trillion-Dollar Battle for Fiber-Optic Supremacy"; Federal Communications Commission, "FCC Acts to Accelerate Submarine Cable Buildout & Security."

[38] Botting and Jordan-Zoob, "Optical Core Infrastructure"; TeleGeography, "Submarine Cable Frequently Asked Questions"; SubOptic, "How Many Submarine Cables Are There, Anyway?"

[39] For example, 98 percent of undersea cables are manufactured and installed by four firms. See Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 2.

[40] Williams, Sovacool, and Foxon, "The Energy Use Implications of 5G."

[41] De Vries, "The Growing Energy Footprint of Artificial Intelligence."

[42] U.S. Department of Energy, *Energy for Space*.

[43] Allan, *Regaining Geopolitical Advantage*.

[44] Gargeyas, "Digital and Energy Infrastructure Are Fueling Important Progress."

[45] Yeoh and Chen, "China-US Competition."

technologies,[46] the more traditional physical infrastructure examined here has general-purpose applications beyond the digital world. Accordingly, because of the more direct links between the hardware and software elements of digital technology stacks, these stacks are governed by slightly different theories of success and are therefore covered separately.

The U.S.-China Competition in Physical Connectivity

The United States' interest in global physical infrastructure long precedes its competition with China. After World War II, U.S. policymakers pioneered a variety of investment and financing mechanisms to develop infrastructure projects in Europe and around the world to undermine the appeal of communism, build economic corridors within and across the Western bloc, and promote a rules-based international order for the flow of goods and ideas.[47] While the United States was never the "only game in town,"[48] its early action at the outset of the Cold War and its central role in both global institutions and physical infrastructure projects have provided a first-mover advantage for competing with the Soviet Union and now the PRC.

Today, this advantage is multifaceted and includes a sophisticated statecraft toolset for supporting global infrastructure projects, which has expanded in the 21st century to include the U.S. International Development Finance Corporation (DFC) and the Export-Import Bank of the United States (EXIM);[49] a variety of global institutions and mechanisms for coordinating with allies and partners;[50] and commercial leadership in key components of the telecommunications and energy sectors.[51] These first-mover advantages allow the U.S. public and private sectors to iterate on new innovations, expand on existing partnerships with developed and developing countries, and scale up a variety of projects across the telecommunications, energy, and transportation sectors.

However, these advantages are now complicated by a variety of challenges. First, stringent U.S. financial regulations—including rules designed to prevent corruption and promote civil liberties—often create high barriers to entry for countries in the developing world while slowing

---

[46] Schindler et al., "The Second Cold War," p. 1099.

[47] Schindler et al., "The Second Cold War."

[48] For example, the Soviet Union sought to compete by supporting such infrastructure projects as the Aswan Dam.

[49] Allan, *Regaining Geopolitical Advantage*, p. 4.

[50] Examples include the Minerals Security Partnership, the Indo-Pacific Economic Framework, the U.S.-EU Trade and Technology Council, and the Americas Partnership for Economic Prosperity. See Allan, *Regaining Geopolitical Advantage*, p. 4.

[51] In the telecommunications sector, for example, U.S. (SubCom), European (ASN), and Japanese (Nippon Electric Company) companies have installed more than 85 percent of undersea fiber-optic cables and command 87 percent of market share. See Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 2. In the energy sector, for example, the United States' resurgence as a net energy exporter since 2019 has positioned it as a crucial supplier of LNG, prompting interest from the Trump administration in developing other countries' energy infrastructure to "pave the way for increased U.S. energy exports" as a means of energy dominance. See "US Looks to Invest in Foreign Energy Projects to Promote Exports, USTDA Says."

the pace of new infrastructure projects.[52] Second, the U.S. public and private sectors often maintain unnecessary silos between digital and physical infrastructure, thereby prioritizing long-term innovation for "dedicated digital infrastructure" rather than the potential near-term gains that would be wrought by integrating and diffusing digital technologies across more traditional physical infrastructure.[53] Third, U.S. interest in global infrastructure has waned since the Cold War, thereby signaling inconsistent commitment to prospective partners.

Finally, U.S. leadership is challenged by China's rise as "the world's largest investor in other countries."[54] This is the culmination of a long-term effort to boost the competitiveness of its state-owned enterprises—one that began with information technology theft and government subsidies,[55] before shifting to exports and the development of global physical infrastructure. Through the BRI, China invested $679 billion in infrastructure projects across almost 150 countries between 2013 and 2022—including energy ($241 billion); transportation ($202 billion); industry, mining, and construction ($202 billion); communications ($26 billion); and water supply and sanitation ($9 billion)—compared with only $76 billion by the United States in the same period.[56]

These Chinese projects feature a greater appreciation for the interdependencies between digital and physical connectivity in the information age. Indeed, China adheres more closely to a "hybrid digital infrastructure" model, which "emphasizes the implementation of digital services on traditional infrastructure."[57] This approach spans across telecommunications, energy, and transportation projects, including accelerated efforts to install undersea cables and capture 60 percent of the fiber-optic cable market through a focus on developing countries;[58] the development of renewable energy to power digital innovation in emerging economies;[59] and the installation of intelligent container terminals and other digital augmentations to improve the efficiency of port infrastructure.[60]

---

[52] U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States."

[53] Yeoh and Chen, "China-US Competition."

[54] U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States."

[55] For example, Chinese banks lent Huawei more than $14 billion between 1997 and 2019 to develop new products. See Botting and Jordan-Zoob, "Competing Visions for the Future of the Internet."

[56] U.S. Government Accountability Office, *International Infrastructure Projects*, p. 12; U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States."

[57] Yeoh and Chen, "China-US Competition."

[58] In 2022, China finished installing its "Peace Cable," a 15,500-mile-long cable that cost $425 million. It links nearly a dozen countries in Asia, Africa, and Europe. For more details, see *Wall Street Journal*, "The Trillion-Dollar Battle for Fiber-Optic Supremacy."

HMN Tech (formerly Huawei Marine Networks) now holds an 11-percent share of the undersea cable market. Undersea and terrestrial fiber-optic cable competition is part of China's 2015 Digital Silk Road (DSR) strategy. See Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 2.

[59] Allan, *Regaining Geopolitical Advantage*, p. 6.

[60] Yeoh and Chen, "China-US Competition."

Thus, China enjoys a second-mover advantage in physical connectivity: By riding the wave of technological diffusion, it prioritizes rapid deployment and application of digital technologies in its infrastructure projects, thereby enabling efficiency gains rather than deep integration and long-term innovation. This is attractive to developing countries, even if it builds dependencies.

However, China faces challenges related to trust,[61] both in the "connectivity and technology performing as advertised" and "in the political and legal systems that inform and govern their operations."[62] First, while the quality of Chinese products is improving, it lags behind comparable U.S. products in such sectors as undersea cables.[63] Second, China's projects often fail to add new and enduring value to developing economies. For example, "Chinese investments often correspond to the last stage of assembly," only capitalizing on efficiency gains at the end of a product's supply chain,[64] and many of these projects import Chinese labor rather than employing and training local workers. Third, the PRC has developed a reputation for predatory lending and ownership practices, including debt-trap diplomacy that increases dependencies through high interest rates and opaque commitments,[65] as well as ownership of and influence over physical infrastructure, such as ports and undersea cables,[66] which could create vectors for geopolitical advantage during crises and conflicts.

Factors Governing Success in Physical Connectivity

Given the general-purpose utility of traditional physical infrastructure, it can serve various roles in the digital world. We identify two distinct theories of success for conceptualizing the ways in which traditional physical infrastructure contributes to geopolitical competition over digital networks. The primary difference between these theories is the function of the infrastructure—i.e., whether the infrastructure serves as an enabler of digital innovation or as a transmitter of strategic commodities. While these two functions are not mutually exclusive, and some infrastructure can serve both functions simultaneously, we posit that each function (as conceived by U.S. and Chinese leadership) drives its own theory of success and thereby emphasizes different factors that uniquely contribute to those theories.

The first theory focuses on physical infrastructure as an *enabler* of digital technology. Indeed, one function of this infrastructure is to supply the key resources powering the information age. Energy is an illustrative example. Given that the training and inference phases

---

[61] Kumar, "China's Digital Expansionism in Africa and the US Counter-Strategies."

[62] Arha, *Trusted Connectivity*, p. 3.

[63] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 6.

[64] Allan, *Regaining Geopolitical Advantage*, p. 6.

[65] U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States."

[66] Liu, "Tracking China's Control of Overseas Ports"; Runde, Hardman, and Bonin, *Responding to China's Growing Influence in Ports of the Global South*; Brooke-Holland, "Seabed Warfare: Protecting the UK's Undersea Infrastructure."

of AI development are very energy-hungry[67]—and that the computational power necessary to develop Machine Learning models has doubled every five to six months since 2010[68]—critical energy infrastructure, such as electricity grids, will be essential for the future of AI. Another enabler of digital innovation is undersea and terrestrial fiber-optic cables, which "provide the high-bandwidth connections necessary to support the rise of cloud computing and integrated 5G networks" while supplying sufficient data to train and refine new AI models.[69] Just as these physical enablers represent the commanding heights that fuel U.S. and Chinese technological innovation, they can also support digital networks in middle powers and developing countries.

Accordingly, these enablers play a critical role in the U.S.-China competition to shape digital networks and accrue geopolitical influence.[70] Drawing on the criteria listed in Chapter 1, physical infrastructure enablers can allow a developing country to improve its *pace of innovation*, thereby facilitating virtuous cycles of technological development and diffusion, as energy and data inputs power new digital advancements in AI, 5G and 6G, IoT, and space technologies, while digitalization enables more-efficient energy and data use in turn.[71] Consequently, the country that can most reliably provide these enablers will be better positioned to secure relational success with its partner nations, including by building capacity and fostering greater trust and legitimacy among local populations. Accordingly, it emphasizes the factors discussed in the next sections.

Cost and Economic Feasibility

Infrastructure is expensive, and national leadership is often swayed by the cost of the offers it receives. Given that the PRC continues to heavily subsidize Chinese state-owned enterprises and private-sector firms, these firms can undercut the price of their competitors and offer unique packages.[72] However, the United States can improve the cost competitiveness of U.S.-owned companies through subsidies, development finance institutions, multilateral development banks, export credit agencies, and public-private partnerships,[73] while levying sanctions and tariffs to undermine the cost competitiveness of Chinese firms.[74]

---

[67] De Vries, "The Growing Energy Footprint of Artificial Intelligence."
[68] *Financial Times*, "AI Power Demand Could Stifle Industry's Growth."
[69] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 1.
[70] Patterson et al., *Winning Without Fighting*; Trotti, "A New Playbook for Irregular Warfare."
[71] Gargeyas, "Digital and Energy Infrastructure Are Fueling Important Progress"; Mahmood et al., "Impacts of Digitalization on Smart Grids, Renewable Energy, and Demand Response."
[72] For example, Chinese telecommunications vendors can provide discounts of more than 30 percent. Hart and Link, *There Is a Solution to the Huawei Challenge*.
[73] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 6.
[74] Bazmi, "China Hits U.S. Optical Fiber Suppliers with Rate Hikes in Trade Tension Escalation."

Ecosystem Advantages

Financial and physical capital represent a major currency for infrastructure projects, but energy and data are also key inputs into digital innovation. Although U.S. companies are often not as cost competitive as their Chinese counterparts, the United States can rely on its more traditional, qualitative advantages in energy exports and fiber-optic cables to prepare more competitive and enticing bids for developing countries.

On-the-Ground Presence

Beijing is often better at demonstrating consistent presence through both public- and private-sector engagement. However, beyond the quantity of engagements, nations often seek genuine partnerships that allow them to develop technical skill sets and improve industrial capability and capacity over time. Despite its narrative emphasis on empowering the Global South, Beijing has only sought to render developing countries dependent on China instead of the West. By contrast, U.S.- and Western-led infrastructure projects are often better at genuinely building capacity and cultivating local skill sets, especially through the promise of technical assistance.

Political, Strategic, and Business Culture Alignment

Both the United States and the PRC have appealed to broader strategic interests and cultural values, beyond the immediate infrastructure deal in question, to accrue influence with existing and prospective partners. While the PRC claims to offer an alternative model of development from that of the West, the United States emphasizes democratic ties, commitments to civil rights, and security concerns about Chinese espionage.

The second theory of success conceptualizes physical infrastructure as critical *transmitters* of strategic commodities. The functional emphasis here is not on the enablement of digital innovation but rather on the broader physical connectivity that underpins the global economy. Examples of transmitters include transportation infrastructure, such as ports, airports, and terminals, which can be augmented by digital technologies, and undersea and terrestrial fiber-optic cables, which ensure the transnational exchange of data and communications.

This second theory of success posits that physical infrastructure transmitters represent key *chokepoints* in the world economy. Unlike digital technologies, physical infrastructure is tangible and can thus be disrupted, blocked, or destroyed. Given the dependence of cutting-edge software on reliable hardware, vulnerabilities in physical connectivity can undermine digital connectivity.

Therefore, any material influence over these physical infrastructure transmitters represents a chokepoint, which a state can wield to pursue strategic success. For example, the West's dominance of undersea cables permits the secure exchange of data, but Chinese efforts to spy on, disrupt, or even destroy these cables could compromise that information and cause higher

latencies (or even internet blackouts[75]) in targeted regions around the world, thereby generating asymmetric advantage. As a second example, China's ownership of and influence over BRI-funded port infrastructure can create opportunities to spy on (e.g., through digital backdoors in augmented infrastructure) or otherwise exclude (e.g., through ownership and military presence) Western vessels while ensuring the PRC's own resilience against U.S.-led containment in the case of a blockade or embargo. This theory emphasizes the following factors, which are markedly different from the factors for enablers.

Regulatory, Legal, and Policy Environments

Laws, agreements, and other institutions and regimes can serve as effective tools in either undermining or bolstering chokepoint control. Local jurisdictional law governs the exchange of strategic commodities in each location and can be used to enforce certain requirements or even exclude certain vendors. For example, strict Chinese localization requirements grant the PRC access to data passing through telecommunications infrastructure on or near its territory.[76] However, the United States uses its own licensing regimes to exclude Chinese firms from undersea cables and related projects that connect to the United States.[77] However, local legal regimes are not only tools to be wielded by the great powers but also obstacles to overcome because many third-party countries have overly burdensome permitting processes, which delay the development of physical infrastructure.[78] Separately, on a far grander scale, international agreements and multilateral initiatives also play a major role in deciding the fate of physical connectivity.[79]

Technology Capabilities and Quality

The ability to plan and execute physical infrastructure projects depends on a robust suite of technology, manufacturing, and repair capabilities. Control over supply chains is an important element. While the West maintains an advantage in designing and laying undersea cables, China's world-leading shipbuilding capacity will allow it to produce a large fleet for the

---

[75] For example, in September 2025, undersea cable cuts in the Red Sea (potentially by the Houthis) disrupted internet access in Asia and the Middle East. For more, see Gambrell, "Undersea Cables Cut in the Red Sea, Disrupting Internet Access in Asia and the Mideast."

[76] Botting and Jordan-Zoob, "Competing Visions for the Future of the Internet."

[77] Federal Communications Commission, "FCC Acts to Accelerate Submarine Cable Buildout & Security"; *Wall Street Journal*, "The Trillion-Dollar Battle for Fiber-Optic Supremacy."

[78] Botting and Jordan-Zoob, "How the US and Its Partners Can Ensure the Worlds' Data Super-Highways Remain Reliable, Secure, Open & Free"; Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 8.

[79] Liu, "Tracking China's Control of Overseas Ports"; Botting and Jordan-Zoob, "Competing Visions for the Future of the Internet"; Botting and Jordan-Zoob, "How the US and Its Partners Can Ensure the Worlds' Data Super-Highways Remain Reliable, Secure, Open & Free"; Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, pp. 8–9.

dedicated purpose of installing and repairing those cables, which generates new opportunities for chokepoint control.[80]

The capability to exploit and/or defend against potential attack vectors is also important. Given its tangibility, physical infrastructure is uniquely susceptible to various forms of disruption. For undersea cables in particular, these vulnerabilities present a new domain of competition: seabed warfare.[81] While ownership and management of undersea cables facilitate chokepoint control, three primary threats can contest this control: (1) *espionage* via optical and quantum techniques, (2) *disruption* to manipulate and corrupt signals, and (3) *sabotage*, which can vastly degrade or even entirely eliminate telecommunications and internet connectivity for weeks until the damage is repaired. Because of the difficulty of both locating undersea cables (to exploit attack vectors) and repairing damage (to defend against them), seabed warfare requires sophisticated military and civilian capabilities on both sides of the offense-defense balance.[82]

Finally, the ability to control any particular chokepoint demands resilience. For undersea cables, this may entail a repair capability to quickly identify and fix any damage; alternative access points and transmitters to reroute internet traffic until the physical damage is repaired; and, for crisis or conflict contingencies in the future, the ability to install additional cables during an emergency.[83] Greater resilience allows a state to withstand an adversary's influence (whether through cable ownership or disruption) over key undersea cables.

Taken together, these two theories highlight several crosscutting themes in digital network competition. They include

- financial issues and the use of investment and concessionary projects to increase the attractiveness of offerings
- the role of integrated programs that offer multiple components of an infrastructure or technology stack in coordinated efforts
- the importance of credibility and a reputation for trustworthiness in executing projects
- achieving chokepoint control of key resources or data in ways that convey leverage.

Wireless and Internet of Things Networks and Infrastructure

Wireless networks and IoT form the digital backbone of modern economic productivity and national security.[84] These interconnected systems—cellular infrastructure and satellite arrays

---

[80] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 3.

[81] Brooke-Holland, "Seabed Warfare."

[82] Aitken, "Undersea Cables Are Vulnerable to Sabotage—but This Takes Skill and Specialist Equipment."

[83] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, pp. 7–8; Gambrell, "Undersea Cables Cut in the Red Sea, Disrupting Internet Access in Asia and the Mideast."

[84] Martin, *Analyzing the Economic Impact of Each Additional 100MhZ of Mid-Band Spectrum for Mobile*; Edquist, Goodridge, and Haskel, "The Internet of Things and Economic Growth in a Panel of Countries"; U.S. Department of Homeland Security, "Securing the Internet of Things."

linked to sensor-embedded devices—increasingly determine global competitiveness. The combined market, now exceeding $1 trillion, reflects the domain's expanding reach across virtually every economic sector.[85] Control over global wireless and IoT ecosystems has therefore become a central axis of U.S.-China competition, in which dominance translates directly into influence.[86] In this section, we define the technologies, map the competitive dynamics, and evaluate the factors that determine success in the domain.

Wireless networks comprise base stations (radio towers that transmit and receive signals from mobile devices), core network servers (centralized systems that manage traffic routing and spectrum allocation), and backhaul connections (high-capacity links that tie base stations to broader telecommunications infrastructure).[87] Operating as software-defined, cloud-based platforms, they support billions of devices and run the central functions of the digital economy.[88] Mobile 5G subscriptions are projected to approach 5.6 billion by 2029, while 6G, targeting deployment in the 2030s, promises capabilities far beyond those of 5G.[89]

Of the ecosystems these networks carry, IoT ranks among the most strategically consequential. It bridges the physical and digital worlds through three functions: sensors detect changes, such as temperature or motion; actuators trigger physical responses; and networks relay data to cloud-based computing systems.[90] Applications range from remote surgery to autonomous vehicle coordination, with IoT increasingly powering predictive analytics, automated optimization, and operational intelligence across critical infrastructure sectors,[91] capabilities that AI and edge computing amplify by delivering low-latency insights.[92] Command of device manufacturing, connectivity standards, and data processing has thus become a defining arena of technological competition.[93]

---

[85] Statista, "Network Infrastructure"; Statista, "Internet of Things—Worldwide."

[86] Thussu, "China's Deepening Digital Presence in the Global South."

[87] Brackup et al., *Alternative Futures for Digital Infrastructure*.

[88] Shubhangi, "Software Defined Wireless Network"; Kai Loung et al., "Key Technologies and Future Trends of 5G Wireless Network Applications"; Zhang et al., "A Pilot Study on the Clinical Feasibility of 5G Remote Robot-Assisted Gastrectomy"; Zeng et al., "Joint Communication and Control for Wireless Autonomous Vehicular Platoon Systems"; Samuthira Pandi et al., "Revolutionizing Connectivity."

[89] Ericsson, "5G Explained"; De Luca, *The Path to 6G*.

[90] McKinsey & Company, "What Is the Internet of Things (IoT)?"

[91] Varol, *Enhancing and Adapting Security Risk Assessment Strategies on Critical Infrastructure Utilizing IoT Devices Using NIST Cybersecurity Framework 2.0*.

[92] Ficili et al., "From Sensors to Data Intelligence."

[93] Bradley et al., *The Next Big Arenas of Competition*.

The U.S.-China Competition in Wireless and Internet of Things Networks and Infrastructure

Unlike discrete product rivalries, wireless networks and IoT systems generate cascading dependencies across economic and security ecosystems.[94] Their dual-use nature amplifies the stakes: 5G networks that enable supply chain management also support military communications, and sensors that capture industrial data can also yield intelligence on infrastructure vulnerabilities, although what a supplier can actually observe depends on where telemetry is stored, whether traffic is encrypted end to end, and whether the vendor operates the network or merely equips it.[95] Governance adds another layer to this competition. Wireless networks are largely centralized through the 3rd Generation Partnership Project (3GPP), in which Chinese firms have aggressively penetrated the standard-setting process even as U.S. companies still chair a plurality of committees.[96] IoT oversight, by contrast, is fragmented across international, regional, and national bodies with overlapping jurisdictions, diffusing authority.[97]

Beyond the security risks of China's sway in the 3GPP, procurement itself creates dependencies that allow Washington and Beijing to exert influence over partner nations. Those dependencies run through several pathways. Countries that select Chinese equipment grow reliant on Huawei or ZTE for upgrades and maintenance, a commercial dependency that our cases document directly and one that ordinarily carries privileged administrative access to core network elements. That access is the best-attested technical route by which a supplier could reach signaling or subscriber data. The second route is legal. Chinese firms operate under published domestic obligations to assist state intelligence work.

A third, deliberately implanted backdoor is the route most often invoked in public debate and the least substantiated in the open record, and we treat it as an allegation rather than a finding.[98] U.S. alternatives create parallel dependencies on semiconductors and cloud platforms, which, as Chapter 3 notes, a growing number of governments now weigh in similar terms. Such choices lock nations into ecosystems, determining which devices connect, where sensitive data are processed, and which standards govern future deployments. To shape these decisions, Washington and Beijing pursue vastly different strategies.

---

[94] Yadav, Li, and Mortier, *IOT Network Behaviours and Dependencies*; Xing, "Cascading Failures in Internet of Things."

[95] U.S. Department of Defense, *Department of Defense 5G Strategy Implementation Plan*.

[96] Shao, "ITU and 3GPP"; Bruer and Brake, *Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy*; Lorci, *Shaping the Digital Order*.

[97] President's National Security Telecommunications Advisory Committee, *Internet of Things (IoT) Advisory Board (IoTAB) Report*.

[98] Cyber and Infrastructure Security Agency, *Overview of Risks Introduced by 5G Adoption in the United States*; Berman, Maizland, and Chatzky, "Is China's Huawei a Threat to U.S. National Security?"; Luong, *Forging the 5G Future*.

China's influence derives from a coordinated state-financial architecture that deploys banks as instruments of market capture. The China Development Bank and the Export-Import Bank of China extend concessional loans covering 85 percent of project costs at low rates with 15- to 20-year maturities, while domestic champions, such as Huawei, collect billions in tax relief and land discounts.[99] Beijing also reserves spectrum bands for Chinese carriers to conduct advanced testing, letting vendors refine products before international rivals enter the market.[100] The payoff is enormous scale; China's nearly 4 million 5G base stations generate unparalleled production volumes that drive down unit costs, reinforced by end-to-end vertical integration in which Huawei and ZTE design chips, antennas, cloud infrastructure, and IoT devices in-house.[101] Total cost of ownership is lower than that of Western alternatives, and domestic markets serve as both testing grounds and revenue bases, subsidizing international expansion.[102]

Chinese firms bundle products to gain leverage in partnerships. The DSR packages data centers, smart city platforms, and 5G infrastructure into turnkey deals spanning financing, deployment, cloud services, and human capital development across partner nations.[103] Beijing further operates Huawei ICT Academies that train 300,000 tech students annually across 110 countries.[104] Dependencies then accrue through several channels: Local manufacturing joint ventures deliver productivity gains but require Chinese components; vendor-managed services entrench operational reliance; and early adoption of Chinese standards, such as Narrowband-IoT (NB-IoT), locks partners into Beijing's compatibility sphere.[105]

Washington, citing surveillance concerns, has abandoned its laissez-faire stance in favor of initiatives that promote digital trust standards, interoperability, and 6G leadership. The Clean Network initiative exemplifies this pivot, uniting more than 60 countries, 200 telecommunications operators, and major technology firms around transparency and privacy in 5G platforms. Complementary efforts target dependency itself; the Open RAN Policy Coalition promotes interoperable solutions that reduce single-supplier reliance—an ongoing U.S. challenge—while the Next G Alliance drives North American 6G leadership.[106] Corporate

---

[99] Massa, *Export Finance Activities by the Chinese Government*; Yap, "State Support Helped Fuel Huawei's Global Rise."

[100] Johnson, "Next Steps to Close the Gap with China on Licensed Spectrum for Commercial 5G."

[101] "China Home to 3.92 Million 5G Base Stations"; Boullenois, Black, and Rosen, *Was Made in China 2025 Successful?*

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

[103] Council on Foreign Relations, "Assessing China's Digital Silk Road Initiative."

[104] Ting-Fang and Li, "Huawei Says It Is Training 300,000 Tech Students a Year amid U.S. Clampdown."

[105] Jiang et al., "International Joint Ventures and Internal Technology Transfer vs. External Technology Spillovers"; Johnson, "Smart Device Empire."

[106] Open RAN Policy Coalition, "Open RAN Policy Coalition Launches to Advance Open and Interoperable Solutions to Expand the Global Advanced Wireless Supply Chain"; President's National Security

investment reinforces these efforts. Qualcomm, for instance, holds a solid share of 5G patents while positioning itself as the primary 6G standard-setter.[107] The approach has paid partial dividends; Huawei's international 5G contracts have declined, although its market share remains intact.[108]

Washington has deployed other mechanisms to counter China's global infrastructure expansion. DFC works to block Chinese control over third countries' telecommunications, as demonstrated by its credit guarantee backing Telstra's acquisition of Digicel Pacific over a Chinese provider.[109] Supply chain–specific efforts further target Chinese capabilities: The United States' Chip 4 alliance with Japan, South Korea, and Taiwan monopolizes high-end semiconductor design and production, isolating China from chip technologies underpinning 6G systems.[110] The Partnership for Global Infrastructure and Investment, in turn, coordinates the Group of Seven's (G7's) responses to Beijing's BRI.[111] Despite financing meant to reduce reliance on Huawei, the United States remains reactive, mobilizing only after China's positions have entrenched.

Factors Governing Success in Wireless and Internet of Things Networks and Infrastructure

Assessing outcomes requires shifting the focus from how great powers compete to how recipient countries choose which technologies to adopt. Washington and Beijing frame this domain around technological leadership and spheres of influence, but developing nations prioritize immediate connectivity.[112] That disconnect may partly explain Chinese penetration despite sustained Western security warnings; governments choosing between costlier, often-delayed Western infrastructure and affordable, rapidly deployable Chinese alternatives select the latter when fiscal limits and popular demands press. Yet adoption transcends cost-benefit calculation. Sustainable advantage requires crafting compelling narratives of technological sovereignty, security guarantees, and economic partnership while still answering the resource constraints that ultimately govern adoption patterns.

Three interconnected factors structure this evaluation, functioning as sequential considerations that the United States can, to some extent, mold. They operate interdependently,

---

Telecommunications Advisory Committee, *Internet of Things (IoT) Advisory Board (IoTAB) Report*; Next G Alliance, "National 6G Roadmap."

[107] Casaccia, "Why Qualcomm Is the True Leader in 5G—a Story of Foundational Inventions"; Intel, "Intel, Biden-Harris Administration Finalize $7.86 Billion Funding Award Under US CHIPS Act."

[108] Lee-Makiyama and Baker, *How Huawei Weathered the Storm*.

[109] U.S. International Development Finance Corporation, "Supporting Resilient Telecommunications Infrastructure in the South Pacific."

[110] Jung, "The 'Chip 4 Alliance' and Taiwan-South Korea Relations."

[111] Arha, "The G7's $600 Billion Response to China's Belt and Road Initiative Is Here."

[112] Scanlon and Drexel, *Countering the Digital Silk Road*.

not hierarchically: Economic constraints may eliminate options regardless of political appeal, yet strong political relationships can justify premium costs, and compelling narratives can reshape how economic trade-offs are politically justified. Recipient countries weigh all three against their domestic circumstances and strategic environments.

Cost and Economic Feasibility

Fiscal viability is the first hurdle. Most developing countries face budgetary limits that render political preferences secondary to financing. Unlike adoption in developed nations, which can absorb premium costs for longer-term gain, adoption in countries with a low per-capita gross domestic product (GDP) often turns on financing terms. Chinese concessional loans often leave Chinese solutions as the only viable option, regardless of recipients' preferences. When Ethiopia—a nonaligned nation—initially selected Chinese vendors for its national 5G rollout, alternative financing would have raised costs by at least 30 percent and delayed deployment by years.[113] The United States can ease these constraints through multilateral financing, as in the 2022 East Micronesia Cable project, in which Australia, Japan, and the United States jointly committed more than $90 million to Pacific Island telecommunications.[114] Western alternatives become economically viable for such recipients only when allied nations pool resources to match Chinese concessional terms.

Political, Strategic, and Business Culture Alignment

Bilateral alignment can override economic calculation when relationship dynamics, security concerns, or domestic legitimacy outweigh fiscal constraints. In countries with higher per-capita GDP, choices demonstrate that political preferences can trump cost efficiency—for example, Japan chose mostly domestic and Western vendors for 5G despite higher costs, its Open RAN alignment taking precedence over economic optimization.[115] Political tensions can likewise render even the most attractive financial package unviable, turning procurement into a proxy statement of foreign policy, as in India's systematic exclusion of Chinese vendors following border conflicts.[116] Those exclusions enable higher-cost Western providers to capture market share, as illustrated by the United States and Finland collaborating to finance a major Nokia 5G deployment.[117] Where cost sets the baseline, political-strategic compatibility determines which viable options a country actually pursues, rewarding superior relationship management.[118]

---

[113] Endeshaw, "Ethiopia's State Telecom Launches 5G Services in Capital"; Luong, *Forging the 5G Future*; Yigzaw, "Ethiopia's Diplomatic Horizon."

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

[115] Fujitsu and Rakuten Mobile, "Rakuten Mobile Partners with Fujitsu to Accelerate 5G Network Expansion"; Thompson, "Japan's 5G Ambitions with the Quad."

[116] Chaudhary et al., "China's Huawei, ZTE Face India 5G Network Exclusion."

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

[118] McWaters, "5G and the Politics of Change."

Narrative resonance is also important for securing alignment. Persuasive framing recasts wireless-IoT procurement decisions as expressions of national identity, allowing countries to justify choices that might otherwise appear economically or strategically suboptimal. China's narrative resonates powerfully with developing countries, framing its solutions as pathways to rapid modernization and emphasizing shared development experiences and noninterference.[119] The United States, by contrast, invokes sovereignty and "democratic technology," casting upfront cost premiums as safeguards against future dependencies and surveillance risks.[120]

Such framing succeeds when it aligns with recipient countries' core legitimacy concerns. Many African leaders embrace the Chinese "partnership of equals" messaging and reject the United States' "capacity-building" language, which implies hierarchy rather than engagement between sovereign equals. [121] Increasingly, wireless-IoT competition unfolds in the realm of meaning-making, in which success depends on enabling recipient leaders to frame their choices as expressions of national values.

The Level of Digital Governance and Institutions

A country's ability to implement and maintain complex technology systems determines whether it locks into multigenerational vendor relationships or retains the flexibility to choose different providers. Effective deployment requires coordinated institutions, regulatory frameworks, and technical expertise.[122] Nigeria's Chinese smart city infrastructure, for instance, has suffered persistent operational disruptions—unreliable power, weak safety protocols, and scarce local expertise—requiring constant Chinese support.[123] Such shortcomings feed into future decisions. Successful implementations, by contrast, generate positive references that bolster vendor credibility and market access. Visible failures serve as cautionary signals for other countries' vendor selection, even when skepticism alone may not prompt strategic pivots for the affected country, given already-established dependencies.

The 5G to 6G transition is Washington's opportunity to reverse Chinese dominance in global wireless infrastructure, but only if U.S. strategy abandons both its reactive posture and the assumption that technological superiority automatically generates market adoption. Success requires preemptive coordination among development finance institutions, the private sector, and alliance structures to deliver integrated, interoperable packages combining competitive financing, strategic partnerships, sovereignty narratives, and implementation guarantees during this transition window. The stakes extend beyond market share to AI deployment and data access

---

[119] Frimpong, *China's Modernization*.

[120] White House, "Fact Sheet."

[121] Negussie, "The Discourse on Sino-African Relations."

[122] Lewis, *How 5G Will Shape Innovation and Security*.

[123] Bradsher and Nossiter, "In Nigeria, Chinese Investment Comes with a Downside"; Hungerland and Chan, "Assessing China's Digital Silk Road."

across the Global South, where 6G networks will be foundational infrastructure for billions of users. Whether the United States can leverage its technological advantages to gain access to ecosystems hinges on accepting that recipient countries evaluate procurement choices in terms of practical development imperatives rather than the logic of great-power competition.

Overall, the domain of wireless and IoT networks highlights the importance of the following themes:

- the ability to offer integrated, bundled turnkey solutions
- cost and economic feasibility
- governance structures and standards that shape the ecosystem for wireless adoption
- lock-in factors, including dependence on providers for updates and capacity-building and the limited infrastructure capacity of third countries, which restricts their ability to exit a technology ecosystem once committed
- trust factors, including data and information security
- political-strategic alignment between third countries and providers
- speed of deployment to meet developing countries' urgent connectivity needs
- narrative resonance that aligns with third countries' preferences.

AI Infrastructure and Data Ecosystems

AI is a critical component of the U.S.-China competition over digital networks, given the military, economic, diplomatic, and geopolitical advantages it provides. AI encompasses a broad range of technologies from narrow, task-specific algorithms to advanced systems capable of learning, reasoning, and simulating human cognition. These capabilities rely on a layered architecture known as the *AI stack*, across which China and the United States are competing at every level. This stack includes everything from the extraction of natural resources to the foundational hardware (such semiconductors, accelerators, and chip manufacturing), machine learning models and algorithms, data ecosystems, and the physical infrastructure (data centers, fiber-optic cables, and energy systems) that sustain large-scale AI operations.[124]

The global AI industry could contribute up to $15.7 trillion to global GDP by 2030, driven by productivity gains and consumer demand. [125] The United States and China dominate this AI ecosystem, but they do so in structurally different ways. Leveraging its lead in advanced compute, chips, and model development, the United States promotes frontier innovation and private-sector leadership, promising powerful, high-quality AI systems in return. China, by contrast, links AI to a broader state-driven digital industrial policy, embedding AI within such initiatives as the DSR and offering technologies as part of a full-stack, exportable digital

[124] Nucci, "AI Infrastructure Explained"; Colback, "Why It Is Vital That You Understand the Infrastructure Behind AI."

[125] Statista, "Artificial Intelligence—Worldwide."

ecosystem to its customers, all of which present an increasingly credible challenge that influences third-country adoption decisions.

In this section, we examine how the United States and China are competing in AI as a critical layer of digital network competition. Crucially, success in this space will not depend on the quality of technologies alone. Instead, it will depend on a broader set of factors, including infrastructure readiness, deployment strategies, cost and financing mechanisms, regulatory alignment, and the ability to offer sustained support and capacity-building to third countries.

The U.S.-China Competition in AI Infrastructure and Data Ecosystems

The United States retains a structural lead in AI, with advantages in frontier innovation, R&D, talent networks, and compute capacity for training and deploying advanced models. China, by contrast, leverages its strengths in large-scale energy production, manufacturing capacity, and an increasingly consolidated domestic talent base to accelerate AI expansion and deployment. As of 2025, the United States holds roughly 75 percent of global graphics processing unit (GPU) capacity and leads in foundation model development and performance,[126] and it accounts for nearly 75 percent of all large language models (LLMs).[127] This dominance in innovative and compute capacity help underwrite U.S. leadership across digital ecosystems, from cloud services to defense applications.

China, however, is working to close this gap. China has declared its goal of achieving global AI leadership by 2030, aiming for it to become a $100 billion industry and create an additional $1 trillion of value in other industries, and it is mobilizing its industrial and state capacity toward that end.[128] China has invested nearly $200 billion in its domestic semiconductor industry and is optimizing models for domestically produced hardware.[129] China's release of an open-source LLM, DeepSeek-R1, in January 2025 demonstrated how Chinese firms are seeking to close the gap with the United States through efficiency, scale, and open-source adaption despite continued U.S. export controls on advanced chips. DeepSeek has continued this trajectory with the April 2026 release of V4, which features major upgrades in reasoning and agentic capabilities; and, like its predecessors, V4 is open source, reflecting a deliberate strategy to compete with U.S. firms by scaling adoption. While the United States leads in quantity of models, benchmark analyses show that Chinese models are approaching or matching U.S. models in performance metrics.[130] China is also making striking gains in AI talent: By 2022, Chinese researchers

---

[126] Pilz et al., "Trends in AI Supercomputers."

[127] Council of the European Union, "ChatGPT in the Public Sector—Overhyped or Overlooked?"

[128] State Council of the People's Republic of China, *New Generation Artificial Intelligence Plan*.

[129] International Institute for Strategic Studies, "DeepSeek's Release of an Open-Weight Frontier AI Model."

[130] Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2025*.

comprised 47 percent of the world's top AI scholars,[131] and 40 percent of the most-cited AI papers in 2021 included Chinese authors, often through international collaboration.[132]

Technological superiority and first-mover advantage in AI model development will not, on their own, secure sustained U.S. leadership in the competition with China. The United States has relied heavily on export controls to restrict China's access to advanced AI chips, a strategy that has been effective in sharply constraining China's access to frontier GPUs and slowing model development. Recent reporting shows that China has begun rationing the Semiconductor Manufacturing International Corporation's chip output to prioritize Huawei; leading labs, such as DeepSeek, have delayed model releases for lack of hardware; and companies are resorting to workarounds, such as smuggling small batches of Nvidia chips, routing workloads through overseas clouds, or bundling thousands of lower-performance domestic chips into power-hungry training clusters.[133]

These responses show both the pressure created by U.S. controls and the adaptability of China's AI ecosystem. Despite the constraints, China's chip production capacity is projected to grow by roughly 40 percent over the next five years, and new models optimized for domestic hardware (e.g., DeepSeek-R1) demonstrate that China is actively adapting rather than stalling. At the same time, its data center footprint is expanding rapidly: The number of operational and announced facilities more than doubled between 2023 and 2024.[134]

Looking ahead, global data center electricity consumption is projected to reach 20 percent of total demand by 2035.[135] This emerging energy bottleneck could become an asymmetrical weakness for the United States, where grid capacity remains fragile. In contrast, China continues to add generational capacity, particularly through renewables and hydropower.

China's AI Plus plan illustrates how Beijing is positioning AI as a core industrial and economic driver. Released in 2024, the plan aims to integrate AI across 90 percent of China's economy by 2030, backed by subsidies, procurement mandates, and large-scale infrastructure investments.[136] This hyperfocus on domestic adoption and sectoral integration across manufacturing, logistics, public services, and robotics boosts China's productivity and innovation capacity and further generates the scale, cost efficiencies, and applied expertise that strengthen its overall competitive position.

---

[131] Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2025*, Chapter 2; MacroPolo, "The Global AI Talent Tracker."

[132] Feldgoise et al., "Studying Tech Competition Through Research Output."

[133] Wei, Ramkumar, and Whelan, "America's Chip Restrictions Are Biting in China."

[134] Strider and Special Competitive Studies Project, *China's AI Infrastructure Surge*.

[135] International Energy Agency, "AI Is Set to Drive Surging Electricity Demand from Data Centres While Offering the Potential to Transform How the Energy Sector Works."

[136] State Council of the People's Republic of China, "China Issues Guideline to Accelerate 'AI Plus' Integration Across Key Sectors."

If these trends—expanding chip production, rapid scaling of AI-ready infrastructure, and diffusion of Chinese AI systems abroad—persist, Chinese firms could soon export cost-competitive chips, cloud infrastructure, and AI platforms across emerging markets, particularly to the Global South. Huawei and other firms are already scaling production of their Ascend AI chips, with plans to double output in 2026 and expand exports to markets in the Middle East, alongside new AI systems positioned to compete with Nvidia-class offerings abroad.[137] For U.S. firms, this trend presents a long-term structural risk: potentially shrinking overseas market share, reduced R&D revenue, and slower innovation cycles. Over time, these pressures could erode the economies of scale that underpin U.S. leadership in frontier model development and global standards setting.

Ultimately, the AI competition will not be decided solely by who develops the most advanced models but by whose systems become embedded in global digital infrastructure—and whose governance frameworks, standards, and platforms shape the next generation of digital networks.

Factors Governing Success in AI Infrastructure and Data Ecosystems

China and the United States differ fundamentally in the systems, relationships, and strategies through which their AI technologies diffuse into foreign digital ecosystems. While both countries benefit from advances in AI, sustained U.S. leadership depends on translating its technological edge into durable economic, military, and geopolitical influence. Success in this competition is therefore shaped not only by superior models or compute power but also by deployment systems, financing mechanisms, capacity-building models, and narratives that determine how AI is embedded across global networks. According to the findings from our expert interviews, the following factors govern these outcomes.

Ecosystem Advantages

A central enabler of China's instrumental success is its ability to deliver vertically integrated, turnkey AI packages that bundle software, cloud compute, and data services. These systems are often financed through Chinese development banks or embedded within broader DSR initiatives. For many low-income or lower-capacity countries with limited internet access or physical infrastructure, such bundled offerings represent attractive pathways to rapid digitization.

Recent partnerships illustrate this trend. For instance, in early 2025, Cambodia and China signed multiple agreements covering AI infrastructure, workforce training, cloud services, and plans for a Cambodia LLM, potentially deepening the embedding of China's digital ecosystem within Cambodia's economy.[138] In Southeast Asia, there is a growing market for building LLMs tailored to local dialects and cultures. Ongoing efforts by Vietnam, Singapore, Indonesia, and

[137] Wei, Ramkumar, and Whelan, "America's Chip Restrictions Are Biting in China."

[138] Sokhean, "Cambodia, China Ink MoUs to Boost Innovation, AI, and Energy Cooperation."

India aim to do exactly that. Chinese AI firms are leading in this category, not only by providing the open-source foundations and knowledge but also by collaborating directly with Southeast Asian firms to build culturally tailored LLMs.

Other cooperation agreements in Hungary and Brazil and across Central Asia on AI build on long-standing Huawei and ZTE telecommunications networks, creating layered dependencies that could also extend into cloud and AI applications. This embeddedness across telecommunications infrastructure, cloud platforms, data centers, and increasingly AI systems greatly raise switching costs. Even when governments are concerned about data autonomy, surveillance, and other security risks emanating from Chinese partnerships or investments, governments face the prohibitive expenses of overhauling entire digital stacks. Expert interviews indicate that, in many emerging markets, the question has shifted from whether to adopt Chinese systems to whether it is still possible to replace them entirely, which would create powerful structural lock-in effects that could shape long-term alignment.

Cost and Economic Feasibility

Economic feasibility is another decisive adoption factor for instrumental success. China's state-supported financing architecture allows it to offer AI infrastructure at subsidized rates, backed by development loans and credit lines. For many governments, these are the only accessible sources of digital infrastructure funding. This model effectively lowers entry costs and increases dependency because repayment terms, maintenance contracts, and technical upgrades often tie countries to Chinese suppliers for years. By contrast, U.S. mechanisms, such as DFC, remain limited in scale or constrained by statutory mandates. Periodic lapses in authorization and risk-averse lending practices reinforce perceptions of inconsistency. Without competitive financing, U.S. systems, even when technically superior, can appear financially out of reach.

Lock-In Effects

Technical compatibility is another factor for instrumental success. China designs its AI models to run efficiently on domestically produced chip architectures. This tight coupling allows smoother deployment on Chinese-built infrastructure, especially in environments affected by U.S. export controls. U.S. models, in contrast, typically require access to high-end GPUs or proprietary platforms that are difficult for many developing countries to procure or maintain. Both approaches generate long-term dependencies, but partner decisions increasingly turn to which provider offers predictable service delivery and life-cycle support at a competitive cost.

On-the-Ground Presence

Relational success is also important. Countries increasingly want partners who will build digital ecosystems with them, not simply export technologies to them. The character of the partnership—co-development, local integration, and skills transfer—now rivals cost and performance as determinants of adoption. China is attempting to position itself as both a supplier

and partner in AI, embedding capacity-building into its digital diplomacy. China's 2025 *Global AI Governance Action Plan* emphasizes infrastructure investments and collaborative partnerships that build partner capacity and provide technical training.[139] In contrast, the United States' "Winning the AI Race" strategy supports innovation, deregulation, and export controls but largely frames partners as adopters of the U.S.-led stack, not as partners or co-developers.[140]

This perception is reinforced by a comparatively smaller and less continuous U.S. diplomatic and technical presence on the ground, whereas China maintains more than 50 science and technology attachés embedded at Chinese embassies globally, providing technical and research professional and workforce support.[141] The absence of a comparable corps of technical diplomats, combined with frequent policy shifts and lapses in financing tools, equally undermines perceptions of reliability.

Beyond the factors above that contribute directly to instrumental and relational success, the ability to secure strategic success often requires a more multifaceted approach. In many markets, "good enough" AI—systems that meet partner needs at a lower cost and at scale—can secure influence, expand market share, and create durable lock-in effects. Ultimately, strategic success will hinge on which country can convert domestic AI capability into sustained international influence by embedding its technologies, governance frameworks, and standards into the digital infrastructure of key regions.

Third-country digital decisions are rarely driven by ideology or a desire to access the most cutting-edge U.S. capabilities. Most states prioritize cost, optionality, and strategic flexibility. This often results in hedging behavior: Governments adopt Chinese AI tools for affordability and deployment speed while still seeking U.S. partnerships for defense, innovation, or high-end applications.

The United States sometimes struggles in these environments, not for technical reasons but because of a zero-risk posture that demands divestment from Chinese technology without offering viable alternatives or incentives. This approach can be self-defeating in markets in which speed, financing, and pragmatic risk tolerance drive decisionmaking.

Strategic success does not require the United States to displace China in every market. It depends on securing influence in sectors and geographies in which military, diplomatic, or economic stakes are highest. Chinese AI in low-stakes applications may be acceptable; what matters is preventing Chinese systems from gaining privileged access to sensitive data or becoming embedded infrastructures of pivotal states.

In sum, the domain of AI infrastructure and data systems points to several themes that are important to determine success in digital network competitions:

---

[139] "Reading Between the Lines of the Dueling US and Chinese AI Action Plans."

[140] White House, "White House Unveils America's AI Action Plan."

[141] Fedasiuk, Weinstein, and Puglisi, *China's Foreign Technology Wish List.*

- cost and economic feasibility issues
- the ability to offer vertically integrated turnkey packages of capabilities
- regulatory and technical alignment of the third country's digital networks with the providing state's AI and data center offerings
- the ability to offer sustained support, capacity-building, and workforce development, including through on-the-ground presence during and after deployment
- technology leadership implemented in ways that attract third party engagement.

Cooperative Space Programs

Outer space is no longer the preserve of a few powers. Low- and middle-income nations now treat space capabilities as crucial to development and governance. They depend on earth observation and remote sensing to manage agriculture, urban development, climate impacts, disaster response, environmental monitoring, and resource mapping; on satellite communications to extend broadband and digital inclusion to remote areas; and on positioning, navigation, and timing (PNT) systems, such as the U.S. GPS or China's BeiDou, which underpin digital networks, logistics, transportation, and smart city infrastructure used for public services, economic development, and security. Falling launch costs have opened the sector to more actors, but cooperative space programs remain essential for many countries to access these capabilities affordably.

Such programs pool resources, expertise, technology, and facilities toward common goals in exploration, research, or development, from shared costs and infrastructure to coordinated research, data exchange, and joint missions. By distributing costs and risks, partners can attempt more-ambitious projects, combining strengths for greater scientific, economic, and diplomatic returns than unilateral efforts could yield.

Equatorial launch sites, common across Africa, Latin America, and Asia, are especially suited to multilateral efforts. Earth's rotation near the equator gives rockets a velocity boost, which saves fuel, increases payloads, eases trajectories into geostationary orbits, and extends satellite lifespans. Accordingly, both China and the United States pursue cooperative programs with equatorial states, such as Brazil, Djibouti, Ecuador, Indonesia, and Kenya.

The U.S.-China Competition in Cooperative Space Programs

China's space program is a source of national pride, backed by high-level political support and funding and aimed at matching the United States across military, diplomatic, commercial, and economic dimensions.[142] Beijing pursues space cooperation bilaterally and multilaterally through the BRI and its components—the DSR and the BRI's Space Information Corridor—as well as the Asia-Pacific Space Cooperation Organization, the expanding BRICS bloc, and the International Lunar Research Station (ILRS).

[142] Bowe, *China's Pursuit of Space Power Status and Implications for the United States*.

U.S. private and government actors operate across many countries, but space cooperation is not a policy priority.[143] Lacking a whole-of-government approach, Washington's effort amounts to a set of agency projects that neither reliably advance partners' capabilities nor draw on existing partnerships, networks, and foreign-aid mechanisms.[144] China, by contrast, presents space cooperation as one incentive among many, alongside investment, infrastructure, educational exchanges, and security sector assistance, to bind governments closer to Beijing.[145]

Washington therefore struggles to compete with the BRI and the Space Information Corridor. Officials warn of security risks from Chinese technology but have not backed those warnings with adequate funding or alternatives,[146] and, despite such initiatives as the G7's Partnership for Global Investment and Infrastructure, the United States lacks the institutional mechanisms, funding, long-term vision, and state support to mount a credible counter.[147] Recipient countries, meanwhile, often discount long-term risks for immediate gains of lower costs, capacity-building, and technology transfer.[148]

Most third-party countries share neither power's interest in deep space exploration, lunar energy production, or space militarization; they want earth observation, satellite communication, PNT services, and space science.[149] They tend to view cooperation as both a means of advancing national space development and an end in strengthening strategic alliances, alongside the same costs, capacity,[150] and technology transfer gains.[151] Balancing long-term interests against short-term electoral incentives and policy constraints,[152] governments typically adopt a mixed or nonaligned posture, cooperating with both powers.[153] This favors China: A sufficient presence across layers secures its access to data and, with it, its intelligence-collection capacity.

---

[143] Klinger and Oniosun, *China's Space Collaboration with Africa*.

[144] Croshier, *Opportunities for US-Africa Space Cooperation and Development*.

[145] Klinger and Oniosun, *China's Space Collaboration with Africa*.

[146] Warner and Ajibade, "China's Smart Cities in Africa"; Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[147] Thussu, "China's Deepening Digital Presence in the Global South"; Carrai, "Is America Losing the Global South?"

[148] Edl, "Developing Space Programs and Cooperation in Latin America."

[149] Croshier, *Opportunities for US-Africa Space Cooperation and Development*.

[150] Beszeditz, *Chinese Space Cooperation in Latin America*.

[151] Klinger and Oniosun, *China's Space Collaboration with Africa*.

[152] Edl, "Developing Space Programs and Cooperation in Latin America."

[153] López, "Orbital Dynamics."

Factors Governing Success in Cooperative Space Programs

Ecosystem Advantages

China capitalizes on partners' ambitions to shift from resource-based to knowledge-based economies as a means of pursuing instrumental success. Governments see cooperation as a way to grow GDP; apply space data to agriculture, mapping, and climate science; connect rural communities; and centralize state activity across sectors[154]—socio-economic priorities that make Chinese funding more attractive than U.S. alternatives and an advantage that Beijing exploits to create dependencies.

Beijing's centralized approach bundles space cooperation infrastructure investments with large-scale technology deployment, particularly in information and telecommunications.[155] Under the DSR and the Space Information Corridor, it offers turnkey packages—feasibility studies, construction, labor, and management—financed through low-interest, state-backed loans that can run 30 to 40 percent below Western alternatives.[156] For recipients, affordable access through such networks as the China-Brazil Earth Resources Satellite (CBERS) program stretches limited budgets while meeting environmental monitoring goals.[157]

The Space Information Corridor aims to link Eurasia and Africa into a global digital ecosystem, joining communication and PNT satellites with ground stations, undersea cables, 5G networks, and data centers. To deepen that integration, Beijing promotes its BeiDou navigation system among BRI participants for civilian and military use, the intended "digital glue" of broader cooperation and a rival meant to surpass GPS in global PNT.[158] By 2019, BeiDou had more active satellites than GPS, ending the latter's monopoly.[159]

LEO internet is reshaping global connectivity by delivering service efficiently to remote areas. SpaceX's Starlink leads, its edge being vertical integration from satellite design and manufacturing through launch, operation, and service.[160] Yet some countries distrust that dominance;[161] SpaceX chief executive officer Elon Musk's decision to cut service in parts of

---

[154] Croshier, *Opportunities for US-Africa Space Cooperation and Development*.

[155] Scanlon and Drexel, *Countering the Digital Silk Road*.

[156] Warner and Ajibade, "China's Smart Cities in Africa."

[157] Chambers, *China's Space Program*.

[158] Nadarajah, "China."

[159] Thussu, "China's Deepening Digital Presence in the Global South."

[160] Giannopapa, Staveris-Poykalas, and Metallinos, "Space as Enabler for Sustainable Digital Transformation."

[161] Scanlon and Drexel, *Countering the Digital Silk Road*.

Ukraine during a counteroffensive against Russia underscored the risk of dependence,[162] and such states as Brazil have welcomed Starlink's competitor, the Chinese Qianfan network.[163]

Beijing also exploits others' underinvestment in space startups.[164] A 2020 U.S.-China Economic and Security Review Commission report found that large PRC state-owned enterprises absorb foreign know-how through mergers, acquisitions, and cooperation agreements,[165] then channel it home to boost domestic R&D. Sometimes the technology is secondary; experts note a pattern of PRC companies investing abroad chiefly to capture such assets as frequency allocations, leaving the acquired company underdeveloped.[166] Acquisition is not the only vector; even institutions that never collaborate with Beijing face state-sponsored espionage and cyberattacks aimed at stealing sensitive aerospace intellectual property.[167]

Two decades of launch services have, in turn, won China agreements that place PRC entities in roles across every phase of joint programs, disproportionately to Beijing's benefit.[168] Such contracts grant remote access to overseas ground stations, strengthening telemetry, tracking, and command (TT&C) capabilities and access to surveillance data from satellites and telescopes.[169]

Political, Strategic, and Business Culture Alignment

China's rapid progress and deepening global South partnerships challenge U.S. dominance while building greater relational success. Its posture is pragmatic, offering attractive terms while avoiding confrontation with Washington, and, through the Asia-Pacific Space Cooperation Organization and BRICS, it promotes cooperative satellite constellations, data-sharing, and the digital services underpinning partners' internet and data ecosystems.[170]

In October 2020, the United States and seven partners signed the Artemis Accords—13 provisions framing international collaboration on human exploration of celestial bodies.[171] By July 2025, Senegal had become the 56th signatory,[172] and, as an ILRS member too, exemplifies

---

[162] Roulette, Bryan-Low, and Balmforth, "Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia."

[163] Scanlon and Drexel, *Countering the Digital Silk Road*.

[164] Jagtiani, *Risky Configuration*.

[165] Stokes et al., *China's Space and Counterspace Capabilities and Activities*.

[166] Jagtiani, *Risky Configuration*.

[167] Weinbaum et al., *Challenges When Collaborating with China on Space Research and Technology*, p. 1.

[168] Stokes et al., *China's Space and Counterspace Capabilities and Activities*.

[169] Cadell and Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon."

[170] Ben-Itzhak, "Network Analysis of International Cooperation in Space 1958–2023."

[171] U.S. Department of State, "Artemis Accords."

[172] U.S. Embassy in Senegal, "Senegal Joins the Artemis Accords."

the pragmatism of cooperating with both powers.[173] The number and geographic spread of signatories attest to NASA's enduring appeal and continued U.S. leadership in the domain.

Decades of leadership bolster that position, with partnerships, service provision, and data-sharing feeding the United States' reputation and soft power.[174] NASA holds more than 640 active international agreements, yielding terabytes of shared earth observation data and training scientists worldwide.[175] Other public goods follow, including free weather and climate data, free GPS PNT data underpinning global banking and mapping, space situational awareness via U.S. Space Command's Space-Track.org, and satellite-tracked maritime data.[176] China's global image, meanwhile, has declined over the past two decades, despite foreign direct investment improving views in recipient states,[177] with the percentage of Latin American respondents in the AmericasBarometer survey rating China untrustworthy rising from 42 percent in 2012 to 62 percent in 2023.[178]

However, China has earned goodwill through international collaboration. In 2016, it signed a memorandum of understanding with the United Nations Office for Outer Space Affairs, opening the Tiangong Space Station to all member states,[179] and has since invited Gulf Cooperation Council states to join Tiangong missions.[180] By 2023, the China National Space Administration had signed more than 170 agreements with more than 50 countries and organizations,[181] including 23 bilateral partnerships in Africa, among them with traditional U.S. allies, such as Egypt.[182] A further example is China's 2021 BRICS space infrastructure agreement, a constellation of earth observation satellites tracking climate change, environmental degradation, and major disasters; members selected Brazil's satellite control center as a global data receiving station,[183] granting China access to Western Hemisphere capabilities.

China's most notable effort is the ILRS, with 13 countries signed on so far (as of this writing in mid-2026), intended to bolster Beijing's standing through multilateral soft power and leadership in developing space law.[184] Beijing frames it against Artemis, casting the U.S.

---

[173] Ben-Itzhak, "Network Analysis of International Cooperation in Space 1958–2023."

[174] Croshier, *Opportunities for US-Africa Space Cooperation and Development*.

[175] NASA, "Global Reach—NASA International Cooperation."

[176] Croshier, *Opportunities for US-Africa Space Cooperation and Development*.

[177] Xie and Jin, "Global Attitudes Toward China."

[178] LAPOP Lab, "AmericasBarometer Data Playground."

[179] Nadarajah, "China."

[180] Nadarajah, "China."

[181] Nadin and Kiryakova, *China's Growing Space and Communications Presence in Africa*.

[182] Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[183] Beszeditz, *Chinese Space Cooperation in Latin America*.

[184] Wu, "The International Lunar Research Station."

program as economically driven and its own as scientific and multilateral.[185] Yet Chinese scholars concede limited tangible results, citing Beijing's thin experience and weak capacity to lead multilateral efforts.[186] The BRI and BRICS frameworks offer venues for negotiation but lack the institutional arrangements to reconcile divergent interests and turn political will into coordinated action.[187]

On-the-Ground Presence

Capacity-building is an important contributor to relational success. Beijing casts its joint ventures as South-South, win-win cooperation, with technical exchange as that ideal in action.[188] Frustration with absent U.S. support has opened the door: "The U.S. had decades to help Africa to develop their space programs, but they never did,"[189] as has been the case with courting states already at odds with Washington, such as Bolivia.[190]

Not all these collaborations are new. China and Brazil launched the CBERS program in 1988 and have since jointly built and launched six satellites,[191] and engagement with Africa has grown alongside it. Egypt's first satellite plant became operational in 2023, with Egyptian engineers training at Chinese space and military sites,[192] while Bolivia sent 64 scientists to Beihang University before they joined Chinese-built ground stations at home.[193] Yet such efforts breed dependency: Equipment is often Chinese-made, Chinese personnel stay embedded in the facilities they build,[194] and partners' economic struggles have stalled domestic industry.[195]

Regulatory, Legal, and Policy Environment

Existing treaties leave many policy gaps, inviting new rule-making.[196] In this aspect, the United States' more comprehensive domestic framework lets it shape international space law, while China, despite developing its own legal regimes, still lags. First-mover advantages give the United States clear leads in launch facilities, launch vehicles, and crewed missions, although China's faster growth in payload weight is narrowing all three gaps.

---

[185] Wu, "The International Lunar Research Station."

[186] Wu, "The International Lunar Research Station."

[187] Wu, "The International Lunar Research Station."

[188] Klinger, "A Brief History of Outer Space Cooperation Between Latin America and China."

[189] Quoted in Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[190] Cadell and Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon."

[191] Ellis, "China-Latin America Space Cooperation."

[192] Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[193] Cadell and Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon."

[194] Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[195] Cadell and Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon."

[196] Li, "Comparing the Power Resources Critical to International Rulemaking in Outer Space."

Level of Digital Governance and Institutions

China has demonstrated a willingness to exploit weaker partner nation security safeguards and institutions to pursue strategic success. For example, ground stations—central to TT&C, the tracking of and communication with satellites—carry dual-use potential for espionage or counter-space operations. As the United States retreats from developing countries, its stations still outnumber China's overseas facilities.[197] Beijing's long-term, commodity-backed loans and debt-for-access deals have also raised concerns that its stations double as global intelligence outposts.[198] These partnerships tend to yield asymmetric outcomes, leaving foreign partners to shoulder significant risk while ceding control over data and infrastructure to Chinese military and industrial goals.[199]

Argentina's Neuquén space station, a Chinese-built military control station leased for 50 years, is the most notorious case. In 2019, U.S. Southern Command's Admiral Craig Faller warned that the space station might breach Argentina's civilian-only terms and could monitor and target U.S. and allied assets.[200] The following year, the SSC (formerly the Swedish Space Corporation), which leases facilities to Western partners, declined to renew Chinese contracts at sites in Argentina, Australia, and Chile, citing alleged terms violations and possible military intelligence-gathering.[201] Because China's military-civil fusion strategy can divert civilian technology into defense programs, prospective partners must conduct rigorous due diligence and implement robust security safeguards.[202]

Such reach is also defensive. With export controls constraining its space sector,[203] Beijing treats broad technology-sharing, and the ILRS itself, as the means to overcome those limits and to end what it calls the "US-led unipolar space order."[204]

This final domain highlights several themes that govern success in the digital network competition:

- regulatory and standards alignment with the recipient country
- offering integrated, turnkey deals
- some level of trust around information security
- alignment to the needs and goals of the recipient country, including multilateral approaches that increase credibility and legitimacy

---

[197] Cadell and Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon."

[198] Londoño, "From a Space Station in Argentina, China Expands Its Reach in Latin America"; Roulette et al., "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid."

[199] Weinbaum et al., *Challenges When Collaborating with China on Space Research and Technology*, p. 1.

[200] Faller, "Posture Statement of Admiral Craig S. Faller, Commander United States Southern Command."

[201] Funaiole et al., "Eyes on the Skies."

[202] Funaiole et al., "Eyes on the Skies."

[203] Wu, "The International Lunar Research Station."

[204] Wu, "The International Lunar Research Station," p. 6.

- lock-in factors around dependency on technology networks
- the ability and willingness to undertake capacity-building efforts.

Appendix C. Country and Functional Issue Case Studies

This appendix presents four country case studies that examine how the U.S.-China digital competition unfolds in specific national contexts. Costa Rica, Nigeria, the Philippines, and Serbia—selected to capture variation in geography, economic development, existing infrastructure, and geopolitical orientation—provide insight into the mechanisms, incentives, and constraints shaping competitive outcomes beyond regional trends. The analysis informed the study's broader assessment of conditions under which the United States can effectively compete for digital infrastructure partnerships. We also conducted a narrow issue-area case study on subsea cables, which appears at the end of the appendix.

In our research, we were excited and grateful to benefit from several detailed and thoughtful case studies completed in a parallel project from the Center for a New American Security, "Countering the Digital Silk Road."[205] That project, whose cases are cited throughout Chapter 4, examined the digital network competition in four countries: Brazil, Indonesia, Kenya, and Saudi Arabia. The project's findings offered critical input to our work. We chose cases partly designed to complement the countries it had already covered.

Costa Rica

Lead finding: Costa Rica demonstrates that combining rapid crisis response, long-term financing, and architecture-based standards can produce durable Western alignment even where Chinese vendors had secured early footholds. The 2022 ransomware attacks created political momentum for diversification, but it was sustained U.S. financing and a shift to Open RAN mandates—rather than politically contentious vendor bans—that translated that momentum into lasting infrastructure outcomes. The shift from country-based exclusions to architectural requirements suggests that technical standards offer small democracies a more sustainable mechanism for managing security risks while avoiding the diplomatic costs of outright vendor bans.

Costa Rica exemplifies how small democracies navigate the U.S.-China digital infrastructure competition, illustrating a notable U.S. success in a country once deemed "a beachhead for Beijing in Central and Latin America."[206] Though home to only 5 million people, the nation leads the region in broadband penetration and, in 2023, became the first Central American

[205] Chilukuri and Scanlon, *Countering the Digital Silk Road*.

[206] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 56.

country to adopt a National Artificial Intelligence Strategy.[207] In a show of Western alignment, Costa Rica even issued a decree barring non-signatories to the Budapest Convention on Cybercrime from participating in 5G networks, a decree that was widely interpreted as targeting Huawei.[208]

This pro-Western positioning, however, coexists with pragmatic hedging that undercuts the perception of decisive alignment. While collaborating with European firms, including Ericsson, on 5G systems, the government continues to allow Chinese vendors in older network generations and included Huawei among bidders for the state-owned Instituto Costarricense de Electricidad's (ICE's) 2025 5G tender after courts suspended the 2023 decree.[209] ICE's tender, however, now mandates an Open RAN architecture, ensuring interoperability across vendors and reducing single-vendor dependence. The shift from country-based exclusions to architecture mandates suggests that technical standards offer small democracies a more sustainable mechanism for managing security risks without the diplomatic costs of outright vendor bans.

The same pragmatic logic pervades Costa Rica's broader digital governance initiatives, which prioritize access, interoperability, and resilience over decisive geopolitical alignment. The Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) targets the digital divide while the complementary Digital Transformation Strategy modernizes public services and data governance through cross-agency interoperability and open data frameworks.[210] Formulated in response to the 2022 devastating ransomware attacks on government systems, the National Cybersecurity Strategy (2023 to 2027) prioritizes risk management, protection of critical infrastructure, and human rights safeguards.[211] Together, these frameworks position Costa Rica to engage multiple external partners without ceding decisive influence to any single actor.

Competing Engagement Strategies

Costa Rica's external partners primarily include Chinese and Western actors—U.S. and European government agencies and firms alike.

---

[207] Álvarez, "Costa Rica Will Be the First Country in Central America to Have an Artificial Intelligence Strategy."

[208] The decree was later suspended due an appeal by Huawei. See Freedom House, "Costa Rica."

[209] Ericsson, "Liberty and Ericsson Switch on First 5G Standalone Network for Mobile Services in Costa Rica and Central America"; Tele Info Today, "Costa Rica Advances 5G Deployment with Tender Evaluation."

[210] Costa Rica Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, *Plan Nacional de Desarrollo de las Telecomunicaciones 2022–2027*; GIP Digital Watch, "Costa Rica's Digital Transformation Strategy (2023–2027)."

[211] NATO Cooperative Cyber Defence Centre of Excellence, "Costa Rica Ransomware Attack (2022)"; Costa Rica Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, *Plan Nacional de Desarrollo de las Telecomunicaciones 2022–2027*.

China

China was the first to secure a 3G contract with ICE in 2009, submitting a bid that was both cheaper and more comprehensive than those of Western competitors.[212] That contract cemented Huawei as a primary supplier of early wireless technologies, whose consumer devices subsequently permeated Costa Rica's digital ecosystem. ICE now uses Huawei routers; private operators Telecable and Claro rely on Huawei modems; Huawei, Xiaomi, and Honor dominate the smartphone market; and municipalities have installed Chinese surveillance systems.[213]

Beijing has complemented Huawei's work with high-profile donations, security-sector assistance, infrastructure loans, and bond purchases. Contributions include a $100 million national stadium, hundreds of police vehicles, Huawei surveillance cameras, two small aircraft, and the purchase of $300 million in Costa Rican government bonds.[214] Notably, when Huawei breached contract terms in 2011 to 2014, Beijing turned potential reputational damage into deeper engagement by offering equipment donations in lieu of financial penalties, yielding an $8.3 million fixed internet expansion project that required ICE to contribute only $1.6 million.[215]

Corruption and implementation issues, however, have undermined this whole-of-government approach. The construction firm building the national stadium, Anhui Foreign Economic Construction Group, attempted to use duty-free imported equipment for other projects, and a proposed Soresco petroleum refinery project collapsed in 2016 because of noncompliance with Costa Rican standards.[216] These compliance failures undermined China's ambitions to be perceived as a reliable development partner and opened the door to alternative Western partnership models.

United States and Europe

Washington's engagement strategy combines large-scale public and private financing with formal capacity-building. Costa Rica's adherence to the U.S.-led Budapest Convention on Cybercrime laid the foundation for digital financing, and the United States has explicitly warned Costa Rica against including Chinese suppliers in its 5G networks, driving the security narrative that led to the 2023 decree.[217] In June 2023, EXIM issued a preliminary $300 million commitment to finance ICE's 5G network procurement.[218] Once the 2023 decree passes review, it will ensure that U.S. financing cannot be used to purchase Chinese equipment.

---

[212] BNamericas, "Costa Rica Investigates Alleged Irregularities in Huawei Contract."

[213] Ellis, "China's Successes and Struggles in Costa Rica."

[214] Ellis, "China's Successes and Struggles in Costa Rica."

[215] BNamericas, "Costa Rica Investigates Alleged Irregularities in Huawei Contract."

[216] Ellis, "China's Successes and Struggles in Costa Rica."

[217] Ammachchi, "Washington's Warning to Costa Rica."

[218] EXIM, "EXIM Board of Directors Approves Preliminary Commitment to Support Development of 5G Network in Costa Rica."

These efforts to align Costa Rica with Western technology standards have borne fruit. A 2024 U.S.–Costa Rica joint statement reiterated Costa Rica's commitment to exploring Open RAN–based approaches, advancing R&D with the United States, and collaborating on cybersecurity, AI, and cloud infrastructure.[219] One example is the SERVIR Central America hub in Costa Rica, which focuses on earth observation.[220] Projects are often bundled, with funding accompanied by training, logistics support, and strategic advisors.[221] U.S. firms have also taken root in Costa Rica's infrastructure. The Trans Americas Fiber System (TAM-1) submarine cable uses AT&T as its anchor tenant and the engineering firm Xtera as the turnkey supplier.[222] On land, the Inter-American Development Bank's private-sector entity, IDB Invest, arranged a $450 million sustainability-linked bond "to increase digital access and broadband quality."[223]

European initiatives have also flourished. The EU-Hispasat Project CONDOSAT under the Global Gateway program will build a shared satellite to provide high-speed broadband and data sovereignty for Costa Rica.[224] Similarly, the EU-funded 5G Connectivity in Costa Rica project established a 5G test bed in 2025, enabling small businesses to experiment with IoT, augmented reality, and industrial automation.[225] These initiatives complement commercial 5G deployments by Nokia and Ericsson and European-supported skills training.[226] Whether these Western gains reflect the intrinsic competitiveness of U.S. and European offerings or result primarily from Chinese compliance failures and the catalytic shock of the 2022 ransomware attacks remains ambiguous.

Success Assessment

Instrumental Success

Dependency on U.S.-aligned systems has deepened since Costa Rica anchored its 5G and cybersecurity architecture in Western suppliers. The $300 million EXIM credit line and U.S. firms as anchor tenants for such infrastructure as TAM-1 lock key assets into U.S. and Western ecosystems, raising switching costs for alternative suppliers. China's earlier success in supplying Costa Rica's 3G network has not translated into dominance in 5G, as exemplified by the 2023

---

[219] Office of the Spokesperson, "Joint Statement on Enhancing Digital Economy Cooperation Between the United States of America and the Republic of Costa Rica."

[220] Ridgeway, "NASA, USAID Launch SERVIR Central American Hub."

[221] U.S. Southern Command, "Partnership with Costa Rica to Establish Cyber Security."

[222] Submarine Cable Networks, "TAM-1."

[223] IDB Invest, "IDB Invest, Liberty Costa Rica Launch Digital Infrastructure Sustainability-Linked Bond."

[224] European Commission, "Costa Rica."

[225] TicosLand, "Costa Rica Launches Pioneering 5G Testbed."

[226] Nokia, "Nokia and RACSA Deploy First 5G Network in Costa Rica"; Ericsson, "Liberty and Ericsson Switch on First 5G Standalone Network for Mobile Services in Costa Rica and Central America"; Joint SDG Fund, "Transforming Territories in Costa Rica with Digital Innovation and Women's Leadership."

decree. Chinese technology remains embedded in routers, modems, and smartphones, but these are consumer devices rather than core network elements. Costa Rica's adoption of 3GPP-compliant 5G, Open RAN architectures, and GPS-aligned systems aligns with Western standards; there is no equivalent uptake of Chinese alternatives, aside from multi-constellation tracking.[227]

Relational Success

In the wake of debilitating ransomware attacks, U.S. aid was likely viewed as reliable and timely. U.S. officials worked closely with Costa Rica's Ministry of Public Security, providing advisers, training, and monetary support.[228] The April 2024 joint statement between the two nations reiterates their shared values and the U.S. position as Costa Rica's largest trading partner.[229] China's relational strategy relies on gifts and soft power (e.g., the national stadium), but poor execution left Costa Rican officials disappointed.

Strategic Success

The United States and its allies now hold greater advantages in Costa Rica, although the security gain is narrower and more specific than a general reduction in exposure. Excluding Chinese vendors from core networks closes the pathway that matters most—the privileged administrative access that a core network supplier holds over signaling and subscriber traffic—but it does not remove Chinese technology from the ecosystem, and what remains carries risk of a different character. The Huawei routers and modems in service at ICE, Telecable, and Claro sit at the network edge, where a supplier's reach is bounded by what transits an individual device. The Hikvision systems installed by municipalities are the most consequential remainder because video surveillance platforms typically retain vendor-managed update and support channels and hold footage of direct intelligence value. We are not aware of any publicly documented instance of exploitation in either case. On the U.S. side, involvement in TAM-1 and the SERVIR hub confers potential intelligence and situational awareness benefits, an inference we draw from the architecture of those systems, not from any public account of how their data are used.

Looking Forward

While these Western partnerships establish interconnected physical, wireless, and orbital infrastructure favoring secure, open standards, several inflection points will determine whether Costa Rica's Western alignment proves durable. ICE's 5G network procurement, with bids from

---

[227] CSA Group, "Costa Rica (SUTEL)—National Frequency Allocation Plan Update"; European Space Agency, "New ESOC GNSS Station in Costa Rica."

[228] U.S. Southern Command, "Partnership with Costa Rica to Establish Cyber Security"; Greig, "US Commits $25 Million to Costa Rica for Conti Ransomware Recovery."

[229] Office of the Spokesperson, "Joint Statement on Enhancing Digital Economy Cooperation Between the United States of America and the Republic of Costa Rica."

Ericsson, Samsung, Nokia, and a Huawei-led consortia under evaluation, could be decided in 2026. A court challenge temporarily suspending the 2023 decree leaves uncertain whether the final award will maintain Chinese vendor exclusion.[230]

Concurrent policy developments, including pending legislation to align data protection regimes with the EU's General Data Protection Regulation (GDPR) and the February 2026 appointment of an international chief technical adviser for the CONECTA digital transformation project, signal potential shifts in governance frameworks.[231] Longer-term planning commitments, including a 2024 semiconductor roadmap emphasizing nearshoring with the United States, suggest institutional momentum toward Western technology systems, although political transitions could alter these trajectories.[232]

For the United States and its allies, the Costa Rican case demonstrates that combining rapid crisis response, long-term financing, and support for strategy development yields greater legitimacy than simply warning against rivals. For Costa Rica, it highlights that vendor diversification and institutional transparency are effective tools for resisting coercive dependence. Where Chinese equipment remains, the exclusion of untrusted vendors from core networks still limits potential security risks. Replicating the U.S. approach in countries in which Chinese vendors are entrenched but institutions value the rule of law will be critical as the world moves toward 6G, AI-enabled networks, and space-based connectivity.

Nigeria

Lead finding: Nigeria illustrates the consequences of U.S. strategic abdication. China's persistent on-the-ground presence and cost competitiveness, combined with the departure of major U.S. tech firms from the market, have produced Chinese dominance across digital infrastructure layers, leaving only venture capital–scale U.S. engagement where infrastructure-scale investment is required.

While Nigeria has historically featured a primarily agricultural and export-dependent economy,[233] recent investments in both the hardware and software of Nigerian digital infrastructure have resulted in an explosion of its digital economy. Indeed, "Nigeria's data-centre market, which is the foundation of cloud services, telecoms, and digital platforms, is projected to grow from $278 million in 2024 to $671 million by 2030, according to industry data."[234] While

[230] TicosLand, "ICE Advances Landmark 5G Tender as Bidding Closes."

[231] Nemko Digital, "AI Regulation in Costa Rica."

[232] Costa Rica Ministry of Foreign Trade, *Roadmap for Strengthening the Semiconductor Ecosystem in Costa Rica*, p. 48.

[233] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 7.

[234] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

Nigerian companies continue to use a variety of U.S. software applications and data, especially for financial technology (fintech), they have been increasingly dependent on Chinese investments in physical and digital infrastructure—that is, the undersea and terrestrial fiber-optic cables, digitally enhanced transportation networks, and satellite systems that embody "the digital pipes that carry the data."[235] This is largely a result of China's engagement strategy, which merits closer analysis.

Competing Engagement Strategies

China

We assess that a core element of Chinese strategy in Nigeria—perhaps even its theory of success—is on-the-ground presence across both its private and public sectors. This is particularly evident through the grand scale of its investments. Indeed, by 2018 Chinese companies had invested more than $16 billion in Nigerian telecommunications.[236] The Chinese government agency Sinosure insured $427 billion in Chinese exports and overseas construction projects in 2013 alone, whereas EXIM issued only $5 billion of credit in 2014 and 2015.[237] But beyond these impressive and persistent investments, Beijing has also focused on building personal connections. By embedding commercial representatives within official state visits, China has fostered a united public-private front, thereby establishing the connections necessary to scale up digital infrastructure projects.[238]

Overall, China's approach to Nigeria can be understood within the context of its broader DSR strategy—by which it seeks to generate greater demand for Chinese telecommunications products abroad, create a more permissive environment via standards setting and other initiatives, and ultimately build closer relationships with countries that the United States and the broader West have potentially neglected. Nigeria is an especially important market because of its young population, which provides an ideal testing ground for China's new digital products.[239] By accelerating Nigeria's pace of innovation and enabling its transition to a modern economy, China can build greater economic partnerships while generating strategic leverage through increasing dependencies.

United States and Allies

By contrast, the United States lacks a coherent strategy vis-à-vis Nigeria, and, in the absence of clear direction from the U.S. government, the U.S. private sector adheres to free market

---

[235] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

[236] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

[237] Bradsher and Nossiter, "In Nigeria, Chinese Investment Comes with a Downside."

[238] Hungerland and Chan, "Assessing China's Digital Silk Road," pp. 7–8.

[239] Hungerland and Chan, "Assessing China's Digital Silk Road," pp. 4–8.

principles. Market trends reveal that many U.S. and Western companies are not sufficiently enticed by the Nigerian economy because of a variety of factors, including the fact that it is not a major market for premium products; fears of political instability and violence, such as those related to the Boko Haram insurgency; and Nigeria's history of nationalizing foreign industries, which "have prompted Western companies to demand very fat profits before putting money into the country—returns on the order of 25 to 40 percent a year. Their Chinese counterparts have been willing to accept 10 percent or less."[240] More recent issues, including the depreciation of the Nigerian currency and higher energy costs,[241] have caused U.S. tech titans, such as Meta, Microsoft, and IBM, to reduce their presence in 2024 and 2025.[242]

Only the smaller and more nimble U.S. commercial actors have found a sustained business case for working in Nigeria. Indeed, "[a]ccording to U.S. Consulate data, U.S. venture capital provides over 60 percent of total startup funding in Nigeria, and roughly 80 percent of Nigerian tech startups are legally incorporated in the United States. American accelerators such as Y Combinator and Techstars continue to nurture Nigerian founders, while U.S.-backed fintechs like Flutterwave and Paystack (now owned by Stripe) dominate payments innovation."[243] This support for Nigerian startups is important for empowering Nigeria's innovation ecosystem, but it does not represent the scale necessary to generate closer economic and strategic ties.

Success Assessment

Instrumental Success

Except for startups, Chinese companies are deeply embedded into Nigerian telecommunications and cloud service networks. For example, as of 2021, Huawei alone had invested $76 million within Nigeria to build smart cities, e-government applications, a rural digital connectivity network (RuralStar), cloud service centers, and a submarine cable connecting the Nigerian mainland to offshore oil platforms.[244] Chinese companies are also making inroads into the fintech, smartphone, and AI sectors, which have traditionally been dominated by U.S. firms, including through Opay, a mobile payment service valued at more than $1 billion; Opera, a browser company; Transsion Holdings, which has captured 60 percent of Nigeria's smartphone market; and the CloudMatrix 384 AI supernode platform.[245] By controlling both the hardware and increasingly the software underpinning Nigeria's emerging digital economy, China is

[240] Bradsher and Nossiter, "In Nigeria, Chinese Investment Comes with a Downside."

[241] Ijaseun, "Why More Multinational Firms May Exit Nigeria—Report."

[242] Jaiyeola, "American Company, IBM, Exits Nigeria in Latest Tech Exodus."

[243] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

[244] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 8.

[245] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

generating lock-in effects that almost guarantee additional opportunities for investment and collaboration in the future.[246]

Relational Success

There is certainly Nigerian demand for U.S. tech products, but China has facilitated greater relational success by offering better deals. Chinese products, such as Huawei's Ascend 910C GPU, are significantly cheaper than U.S. equivalents while providing sufficient quality for most applications.[247] Chinese companies also bundle digital and physical infrastructure projects—including in railways, port systems, and smart cities—which can meet several Nigerian sources of demand simultaneously.

Additionally, Chinese companies are producing stronger relationships through greater capacity-building, such as training centers and competitions at Nigerian universities to cultivate skill sets in information and communications technologies. While Nigerian markets are still dependent on Chinese products and labor, these training centers serve to improve the image of Chinese companies. This may reflect lessons learned from prior Chinese experiences in Sri Lanka and Vietnam, where increasing dependencies and reliance on Chinese labor produced tensions with local citizens.[248]

However, Beijing still faces challenges for relational success. In the mid-2010s, the Nigerian government conducted anticorruption investigations into Chinese construction contracts. Thus, while corruption sometimes helps Chinese companies enter certain markets and outcompete their U.S. counterparts, it can also generate backlash.[249] Additionally, quality and safety concerns—including operational disruptions, inconsistent power grids, and insufficient safety protocols—may haunt Chinese companies, as local frustrations with the labor market make existing dependencies increasingly unpalatable.[250]

Strategic Success

China's instrumental and relational success can serve as a foundation for future strategic success. First, through lock-in effects, it has generated greater leverage for coercion. Indeed, by dominating "the digital pipes that carry the data,"[251] China can threaten to impede the flow of data to compel certain outcomes. Additionally, given that Huawei and other Chinese firms rely

---

[246] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 5.

[247] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

[248] Hungerland and Chan, "Assessing China's Digital Silk Road," pp. 8–9.

[249] Bradsher and Nossiter, "In Nigeria, Chinese Investment Comes with a Downside."

[250] Bradsher and Nossiter, "In Nigeria, Chinese Investment Comes with a Downside"; Hungerland and Chan, "Assessing China's Digital Silk Road."

[251] Balogun, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind."

on hefty loans from the Export-Import Bank of China, their infrastructure projects can create opportunities for debt-trap diplomacy vis-à-vis Nigeria,[252] which has been endemic to its BRI.

Additionally, China can leverage the infrastructure for other strategic and military applications. For example, the Export-Import Bank of China acquired a stake in the Nigerian satellite communications company NIGCOMSAT. This creates opportunities for inter-satellite linking with Chinese satellites, thereby allowing the People's Liberation Army to access a greater reserve of satellite data for military operations.[253] Additionally, fiber-optic and broadband networks, such as the new undersea cable and RuralStar, may allow Beijing to install surveillance systems, which is commensurate with prior warnings from the United States.[254] And finally, Nigeria's increasing reliance on Chinese drones for both civilian and military applications may represent a testing ground for PLA autonomous capabilities.

Although it remains to be seen whether and how actively Beijing will exploit these sources of advantage, their greater strategic leverage creates opportunities for future coercion vis-à-vis Nigeria while refining new vectors for geopolitical competition vis-à-vis the United States.

Looking Forward

Given the recent departure of major U.S. tech firms, the United States' position in Nigeria continues to worsen. While China has struggled to penetrate major markets, such as Europe and Japan, Nigeria is a young and populous country that will continue to yield economic and strategic dividends. As a result, and commensurate with established trends pertaining to China's DSR strategy, we should expect further investments and collaboration—until or unless some of the potential sources of frustration with China's predatory practices boils over into political action against Beijing.

If the United States is to compete more effectively in Nigeria, it needs to create a more permissive environment for sustained presence by large and small U.S. firms alike. It should consider leveraging such tools as DFC and its own Nigerian Export-Import Bank to invest in Nigerian infrastructure projects, incentivize U.S. companies to pursue new areas of collaboration, and ultimately make U.S. products more competitive. These efforts should also complement the existing inroads that venture capital firms have made into Nigeria's digital economy.

The Philippines

Lead finding: The Philippines demonstrates that digital competition outcomes are determined not by geopolitical preference alone but by the interaction of infrastructure needs, market

---

[252] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 10.

[253] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 5.

[254] Hungerland and Chan, "Assessing China's Digital Silk Road," p. 9.

structure, deployment capacity, and financing. Even in a country with active security tensions with China and strong U.S. alignment, Chinese-linked firms secured a significant foothold in telecommunications because they met specific operational requirements that alternatives could not match at comparable scale, cost, speed, and integrated delivery.

Digital networks competition in the Philippines is neither zero-sum nor cleanly divided between the United States and China. Rather, the competition unfolds unevenly across the digital stack with different actors exerting influence at different layers. Chinese firms are most embedded in the telecommunications network, particularly through vendor relationships and the rollout of DITO Telecommunity as a third operator with Chinese ties in 2021, while U.S. and allied actors play more-prominent roles in subsea connectivity, cloud infrastructure, satellite services, and infrastructure financing. Recent Philippine policy reforms in investment screening and cybersecurity have sought to shape the conditions under which foreign actors participate in these layers.

Two features make the Philippines analytically useful. First, security tensions with China are salient in domestic politics, particularly maritime disputes in the South China Sea, debates over Chinese-linked investment in telecommunications infrastructure, and unfavorable public opinion of China. These dynamics have heightened attention within both the legislative and executive branches to the risks associated with foreign participation in strategic sectors. Policy decisions, including increased scrutiny of foreign investments and the Philippines' withdrawal from the BRI in 2023, illustrate a desire to reduce exposure to Chinese-linked systems. Yet efforts to reduce reliance on Chinese technology face practical constraints, in part because existing vendor dependencies, cost, and the need for rapid infrastructure deployment constrain available alternatives.

Second, the Philippines' network choices are shaped by geographic and implementation constraints that make rapid, nationwide connectivity necessary, costly, and technically complex. As an archipelagic state of more than 7,000 islands, the country faces high deployment costs and persistent challenges in achieving nationwide connectivity. These conditions necessitate reliance on a mix of technologies, including fiber, wireless, and satellite, as well as on external partners and financing to extend coverage to remote areas.[255] Policymakers and operators must navigate trade-offs among cost, speed of deployment, and security considerations, producing a fragmented digital ecosystem in which influence is distributed unevenly across layers rather than dominated by any single external actor.

Philippine policy has increasingly treated digital networks as critical infrastructure requiring both modernization and security oversight. The Department of Information and Communications Technology (DICT) plays the central planning role, including through the National Digital Connectivity Plan (NDCP). Published in February 2026, the NDCP frames digital connectivity

[255] Johan, "Fiber in the Philippines Is Improving and Catching Up with Its Regional Peers."

as an essential public good and lays out targets through 2028, including achieving full connectivity in public schools, creating 130,000 free Wi-Fi sites, and connecting geographically isolated communities.[256] The plan recognizes broadband affordability as a critical challenge, noting that the Philippines has some of the highest broadband costs in the Association of Southeast Asian Nations. Its goal of achieving a 40- to 80-percent reduction in broadband costs suggests that affordability and fiscal feasibility will be central drivers of infrastructure decisionmaking going forward. The National Telecommunications Commission, Department of Trade and Industry, and emerging national security review processes have distributed authority across agencies.

Philippine policy has increasingly treated digital networks as critical infrastructure requiring both modernization and security oversight. Formal rules have tightened in two specific ways relevant to affecting external participation in digital infrastructure. A revision of Republic Act No. 11659 in 2022 allowed 100-percent foreign ownership of key sectors, including telecommunications, and introduced national security screening for critical infrastructure, allowing the president to prohibit foreign investments in strategic industries.[257] This combination of liberalization and screening reflects an attempt to attract capital while retaining control over high-risk investments. Executive Orders No. 127 (2021) and No. 58 (2024) and the National Cybersecurity Plan further emphasize resilience, interagency coordination, and secure digital infrastructure.[258]

Competing Engagement Strategies

China

Chinese engagement is concentrated in telecommunications infrastructure. The market was historically dominated by PLDT/Smart Communications and Globe Telecom,[259] both relying on mixed vendors, including Huawei alongside Nokia.[260] The introduction of DITO Telecommunity in 2019 and commercially launched in 2021 brought China Telecom as a 40-percent equity holder,[261] with Huawei and ZTE playing central roles in network deployment. Despite security

---

[256] Philippine Department of Information and Communications Technology, *National Digital Connectivity Plan*.

[257] PwC, "Republic Act No. 11659."

[258] Duterte, Expanding the Provision of Internet Services Through Inclusive Access to Satellite Services, Amending Executive Order No. 467 (s. 1998) for the Purpose; Marcos, Adopting the National Cybersecurity Plan 2023–2028, and Directing the Implementation Thereof; Philippine Department of Information and Communications Technology, *National Cyber Security Plan 2023–2028*.

[259] Pateña, "PLDT Partners with Huawei to Improve Wireless Services Delivery."

[260] Nokia, "Nokia Selected by Globe Telecom to Modernize BNG Network to Improve Broadband Experience in the Philippines."

[261] Morales and Lema, "China-Backed Telecom Firm Says Won't Spy on Philippines."

concerns, the government facilitated DITO's entry through spectrum allocation and regulatory support, reflecting a priority to increase competition and expand coverage.

DITO's selection can be explained less as a geopolitical alignment decision and more as a response to binding market and policy constraints. The government had an explicit objective to introduce a third operator to break the duopoly associated with high prices and uneven service quality.[262] Three interconnected factors shaped the outcome, although DITO was competing with only two other bidders:[263] (1) cost and speed, in which DITO offered the most cost-competitive bid and ability to scale infrastructure quickly; (2) integrated turnkey delivery: the combination of China Telecom equity, Huawei and ZTE equipment, and a coordinated rollout reduced coordination risk compared with fragmented procurement approaches; and (3) market structure: the policy requirement to stand up a viable third operator created incentives to favor bids capable of delivering end-to-end solutions. Security concerns were acknowledged in legislative debates but were managed through ongoing oversight rather than exclusion, illustrating a broader pattern in which economic and deployment constraints shape outcomes even in politically sensitive sectors.

Beyond telecommunications, Chinese influence is more limited. Huawei Cloud entered the Philippine market in 2024 but faces established competition from U.S. hyperscalers. Cross-country analysis suggests that Chinese AI models have achieved only modest market share gains (0 to 5 percent), indicating a relatively limited presence in higher-value segments.

United States and Allies

U.S. and allied engagement is strongest in subsea connectivity, cloud infrastructure, satellite, and infrastructure financing. Subsea cable systems, including Jupiter,[264] Apricot,[265] and the Pacific Light Cable Network (PLCN),[266] involve multiple stakeholders, including Google and Meta, embedding the Philippines within broader regional networks. The PLCN case demonstrates how external governance mechanisms constrain available options: In 2020, U.S. authorities denied approval for the Hong Kong landing point on national security grounds while allowing Taiwan and Philippine segments to proceed under mitigation agreements.[267] In contrast to the DITO case, in which Philippine authorities actively enabled Chinese participation to meet

[262] Oxford Business Group, "The Entrance of a Third Major Telecoms Provider Set to Break the Duopoly in the Philippines."

[263] Camus, "Third Telco Bidding Aftermath."

[264] Submarine Cable Networks, "JUPITER."

[265] Koley, "Announcing Apricot."

[266] Submarine Cable Networks, "PLCN."

[267] 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"; Submarine Cable Networks, "PLCN."

domestic objectives, the subsea domain demonstrates how U.S. licensing requirements can shape routing and participation decisions even when the Philippines is not the primary decisionmaker.

In cloud and data infrastructure, U.S. providers dominate through platform ecosystems and enterprise integration. AWS's Manila Local Zone (2023),[268] alongside expansions by Microsoft, Google, and Equinix's 2024 data center acquisition,[269] reflects a model driven by global scale and network effects. Satellite connectivity introduces a parallel pathway bypassing terrestrial constraints: The Philippines' early adoption of Starlink in 2023,[270] enabled by Executive Order No. 127 (2021), which opened the satellite market, reflects both structural demand and policy openness to U.S.-based providers.

Infrastructure financing operates as a crosscutting mechanism. In March 2024, U.S. Secretary of Commerce Raimondo led a Presidential Trade and Investment Mission generating more than $1 billion in investment pledges from 22 U.S. companies spanning digital infrastructure, logistics, and energy.[271] This initiative underscores how sustained diplomacy and coordinated public-private engagement can anchor U.S. influence in the digital stack. KKR committed approximately $400 million to Philippine tower assets in 2024,[272] and World Bank financing supports broadband expansion. These investments demonstrate that control over capital and implementation capacity can shape outcomes as much as technology choice itself. Chinese models, by contrast, often bundle financing with infrastructure delivery.

Success Assessment

Instrumental Success

Chinese firms have established a foothold in telecommunications through vendor relationships and DITO's rollout, but their influence remains largely concentrated in this layer. U.S. and allied actors have achieved stronger positions in cloud infrastructure, subsea connectivity, and satellite services. The overall system remains diversified, with limited evidence of systemic dependency or lock-in. Information remains limited on the full effects of the new screening mechanisms in practice, making it difficult to assess whether they have materially altered the composition of foreign participation.[273]

---

[268] Amazon Web Services, "Announcing the General Availability of AWS Local Zones in Manila."

[269] "Data Center Firm Equinix Enters the Philippines, Eyes on Southeast Asia."

[270] Hilario, "NTC Greenlights Starlink VAS Provider Registration."

[271] Flores, "US Companies to Announce Investments of over $1Bln in the Philippines."

[272] Morales, "Philippines Gets $5 Bln in Investment Pledges from German, US Companies"; World Bank Group, "More Than 20 Million Filipinos to Benefit from Improved Broadband Internet Connectivity."

[273] For descriptions of the evolution of this new approach, see Yee, "How the Philippines Screens Foreign Investments"; Bataller, "What the 2026 SIPP Reveals About the Philippines' Future"; and Kelmer Group, "Philippines Targets P4.5 Trillion in Investments."

Relational Success

U.S. and allied actors benefit from alignment with Philippine cybersecurity frameworks, security standards, and integration into global digital ecosystems. Chinese participation in telecommunications infrastructure faces growing scrutiny tied to security concerns and unfavorable public opinion. However, Chinese providers met specific operational requirements, such as cost, speed, and integrated delivery, that sustained their role in telecommunications despite the broader political environment. The relationship is pragmatic on both sides.

Strategic Success

Neither side has achieved dominance across the digital stack. The Philippines' digital ecosystem remains fragmented, with influence distributed unevenly across layers rather than consolidated under any single external actor. AI represents one of the least consolidated layers and a potential entry point for sustained U.S. investment. The absence of entrenched positions in AI-related infrastructure means that outcomes in this layer will likely be determined by platform adoption, talent development, and regulatory choices rather than by legacy vendor relationships.

Looking Forward

AI may represent one of the least consolidated layers of the Philippines' digital ecosystem and, therefore, a potential entry point for external influence. Unlike telecommunications, in which Chinese-linked firms secured early footholds, or cloud infrastructure, in which provider ecosystems are already taking shape, AI adoption appears to remain nascent and centered on workforce development, pilot government use cases, and enterprise integration. Evidence from cross-country analysis suggests that Chinese AI models have expanded globally but achieved only modest market share gains in the Philippines (0 to 5 percent),[274] indicating a relatively limited presence as of this writing. AI adoption in the Philippines remains a fluid and contestable area in which future trajectories are likely to be shaped by skills pipelines, data-access frameworks, and ecosystem partnerships rather than by early-stage infrastructure lock-in.

Even in a country with significant security tensions with China and growing alignment with the United States, this case study shows that outcomes are not determined by geopolitical preference alone. They are shaped by the interaction of infrastructure needs, market structure, affordability and financing availability, and institutional capacity. Digital competition is less about choosing sides than about overwhelmingly shaping critical nodes of interdependence. Where Chinese providers remain embedded, particularly in telecommunications, it is because they met specific operational requirements related to cost, speed, and integrated delivery. Efforts to compete therefore require both trusted and more-advanced alternatives and commercially viable solutions at comparable scale and timelines.

---

[274] Wang and Siler-Evans, *U.S.-China Competition for Artificial Intelligence Markets*.

Serbia

Lead finding: Serbia illustrates that formal regulatory alignment with Western standards and actual infrastructure outcomes can diverge sharply when Chinese financing aligns with centralized domestic decisionmaking and when China provides geopolitical benefits—in this case, Kosovo-related diplomatic support—that Western engagement cannot substitute. Conditionality without enforcement and signaling without financing have shaped governance frameworks while leaving the underlying digital infrastructure tied primarily to Chinese providers.

Serbia illustrates how third countries make decisions in the context of the U.S.-China digital competition, demonstrating that outcomes are shaped not only by technological considerations but by broader political and economic factors. Over the past decade, Chinese firms, particularly Huawei,[275] have become deeply embedded across Serbia's telecommunications networks,[276] surveillance systems,[277] and data architectures,[278] through projects associated with the DSR. At the same time, Serbia remains formally committed to EU accession, has increasingly aligned its regulatory framework with EU digital standards, and signaled a partial shift toward including Western vendors in 5G procurement. U.S. engagement, by contrast, has been more limited and inconsistent. The result is a system in which regulatory alignment points West while much of the underlying digital infrastructure is tied primarily to Chinese providers.

Decisions on the digital stack are driven by the interaction of external incentives (including financing and conditionality), domestic political economy structures, and broader strategic relationships. China's model of combining state-backed financing, rapid deployment, and low conditionality aligns closely with Serbia's centralized decisionmaking and preference for flexible procurement. Western tools have had limited impact on infrastructure outcomes in the absence of credible financing and enforcement mechanisms.

These dynamics are reinforced by Serbia's broader strategic relationship with China, including cooperation in energy, defense, and diplomacy, which embeds digital infrastructure decisions within a wider set of political and economic ties.

---

[275] International Trade Administration, "Serbia Country Commercial Guide."

[276] Vasovic, "Serbia Chooses Links with China to Develop Economy, Telecoms Despite U.S. Warning Campaign."

[277] Jankovic and Standish, "Leaked Files Reveal Serbia's Secret Expansion of Chinese-Made Surveillance."

[278] Dragojlo, "China's Huawei Opens Tech Centre, Consolidating Presence in Serbia."

Competing Engagement Strategies

China

China's engagement in Serbia operates within a highly centralized telecommunications sector dominated by state-owned Telekom Srbija, which accounts for approximately 44 percent of mobile subscribers and 94 percent of fixed-line connections.[279] This concentration creates a governance structure in which political considerations can outweigh commercial or security concerns in vendor selection. Infrastructure outcomes are shaped less by market competition than by state preferences, creating conditions favorable to Chinese state-backed firms that can coordinate with centralized decisionmakers.

China's role in Serbia's digital infrastructure has developed within this centralized framework, supported by financing mechanisms that align with domestic priorities. Engagement deepened following Serbia's 2015 BRI memorandum of understanding and the 2016 Sino-Serbian Comprehensive Strategic Partnership,[280] which formalized cooperation across multiple sectors. Huawei emerged as a key partner in the modernization of Telekom Srbija's network, while Chinese state-backed financing facilitated project implementation.[281] As of 2023, Serbia owed approximately €2.37 billion to the Export-Import Bank of China, reflecting a broader pattern in which Chinese loans provide faster and less conditional alternatives to EU funding.[282] This model is particularly compatible with Serbia's preference for rapid deployment and executive-led decisionmaking.

Although Serbia has formally aligned its digital governance with European standards by adopting a GDPR-inspired data protection law in 2018 and a National AI Strategy in 2019 and harmonizing with the EU's NIS2 directive, enforcement remains limited, with low fines and underdeveloped oversight.[283] This gap allows infrastructure decisions to follow a different logic than governance commitments might suggest.

These dynamics are evident in Serbia's approach to 5G deployment. The country completed its 5G spectrum auction in November 2025 and launched commercial services in December 2025, several years behind regional peers.[284] Although Telekom Srbija announced procurement from European vendors, including Ericsson and Nokia, there is no clear indication that Chinese suppliers have been fully excluded from the broader network ecosystem. Existing assessments

---

[279] Miquee and Buffon, "Research Update."

[280] Serbian Ministry of Foreign Affairs, "China."

[281] Vasovi, "Serbia Chooses Links with China to Develop Economy, Telecoms Despite U.S. Warning Campaign."

[282] Trivić, "The Belt and Road Initiative and Its Impact on Serbia."

[283] Račanović, "Serbia's Artificial Intelligence Revolution."; Vlajkovic and Saric, "Bridging the Gap Between Serbian Regulations and the GDPR"; JPM Law Office, "Serbia."

[284] Kehoe, "5G in the Balkans."

point to continued cooperation with Huawei, suggesting that Serbia has pursued a strategy of partial diversification rather than full alignment with any single vendor bloc.

The Kosovo dimension reinforces China's position. China's nonrecognition of Kosovo and support for Serbian sovereignty under United Nations Security Council Resolution 1244 gives China leverage outside the digital domain that shapes digital decisions.[285] Where China provides something the West cannot substitute, such as diplomatic cover on a sovereign dispute, alignment costs for Western initiatives remain prohibitively high regardless of what those initiatives offer on their own terms.

United States and Allies

The most visible U.S. engagement has been the Clean Network initiative (2020), which sought commitments to exclude untrusted Chinese vendors.[286] Serbia signed the Washington Agreement in September 2020, committing in principle to exclude Huawei and ZTE, but did not translate this into binding domestic legislation. It continued to deepen cooperation with Huawei, including hosting a new innovation center and publicly reaffirming the company's importance. The 5G auction was delayed for several years, preserving flexibility rather than making a definitive choice. The initiative signaled policy preferences without providing financial alternatives, and the agreement established commitments without enforcement tools. The primary U.S. financial tool has been EXIM's $50 million commitment under the China and Transformational Exports Program, the first such financing extended to a European telecommunications operator. Beyond this, U.S. engagement has been sporadic, with the bilateral relationship shaped more by Kosovo-related diplomacy than a broader digital strategy. The EXIM loan remains the only instance in which U.S. engagement directly coincided with infrastructure decisions, and even its causal weight in the 5G outcome remains unestablished. Serbia faces a different calculus than its regional neighbors: Excluding Chinese vendors risks disrupting relationships with a key diplomatic partner on Kosovo, a major infrastructure investor and a broader political and security partner.

Western actors hold stronger positions in other layers. The fiber backbone is predominantly Western, with EXA Infrastructure's 2025 acquisition of a Serbian fiber corridor creating a unified route through the region.[287] In AI and data, France's Eviden secured a €50 million contract for Serbia's National AI Factory in 2025, indicating that competition remains open in higher-value segments of the stack.[288]

---

[285] Vladisavljev, "Why China Is Serbia's New Main Ally in the Kosovo Independence Dispute."

[286] Rithmire and Han, "The Clean Network and the Future of Global Technology Competition."

[287] EXA Infrastructure, "EXA Infrastructure to Purchase Longhaul Duct Assets from Conexio."

[288] Bull, "Eviden Signs a 50-Million-Euro Contract to Build Serbia's National AI Factory."

However, Huawei maintains a commercial presence in Serbia's State Data Center in Kragujevac alongside such firms as Oracle Cloud,[289] and its equipment remains embedded in Telekom Srbija's fiber-to-the-home network from the 2016 ALL-IP contract.[290] EU accession has traditionally been Serbia's primary external governance anchor, but its influence on infrastructure outcomes has been uneven. Although Serbia opened accession negotiations in 2014, progress has been slow and democratic backsliding has persisted. The EU's Reform and Growth Facility, which allocates €6 billion to Western Balkan states through performance-based,[291] tranche-linked funding tied to implementing specific reforms (including alignment with the EU's 5G Cybersecurity Toolbox[292]), represents the most substantive new Western mechanism. Serbia's first disbursement was approved in January 2026, although whether this conditionality will extend to legacy Chinese infrastructure remains to be seen.

Success Assessment

Instrumental Success

Chinese firms maintain strong positions across legacy telecommunications, surveillance infrastructure, and elements of data infrastructure, creating switching costs that complicate efforts to shift toward alternative vendors. The Huawei-deployed broadband infrastructure, smart city surveillance systems, and presence in the State Data Center collectively generate lock-in effects. Western actors have made inroads at specific layers, notably in the fiber backbone, 5G procurement from Ericsson and Nokia, and AI infrastructure, but these build on an infrastructure base that continues to include substantial Chinese involvement.

Relational Success

China's relational advantage stems from its broader strategic partnership with Serbia, particularly its diplomatic support on Kosovo, cooperation in energy and defense, and elite ties cultivated over more than a decade. This provides a form of leverage that Western actors cannot replicate through digital engagement alone. The Sino-Serbian Comprehensive Strategic Partnership, formalized in 2016, embedded digital cooperation within a wider architecture of political and economic ties. The EU has shaped formal governance structures through accession conditionality, but enforcement remains limited and has not altered procurement incentives. U.S. bilateral engagement has been episodic and Kosovo-dominated rather than strategically oriented

[289] Serbian Office for Information Technologies and eGovernment, "Government Data Centre in Kragujevac."

[290] IntelliNews, "Telekom Srbija and Huawei Launch €150mn Project to Develop Landline Network in Serbia."

[291] Directorate-General for Enlargement and Eastern Neighbourhood, "Reform and Growth Facility for the Western Balkans."

[292] Reform Monitor, "European Commission Approves First Disbursement of Reform and Growth Facility Funds to Serbia."

toward digital competition. High-level engagement has been sporadic, with the relationship largely shaped by Kosovo-related diplomacy rather than a broader strategic agenda.

Strategic Success

The result is a hybrid system in which regulatory alignment points West while underlying infrastructure remains tied to Chinese providers. Adopting Western regulatory frameworks has not translated into corresponding infrastructure outcomes. In Serbia, centralized decisionmaking, access to Chinese financing, and limited enforcement capacity have allowed Chinese and Western elements to coexist within the same system. China's embedded positions, combined with its nonsubstitutable diplomatic leverage on Kosovo, produce a strategic environment in which Western initiatives face prohibitively high alignment costs regardless of what those initiatives offer on their own terms. Neither side has achieved full dominance, but China holds the stronger structural position across the stack as a whole.

Looking Forward

Whether Serbia's partial diversification toward European vendors in 5G represents a durable shift or a tactical accommodation remains uncertain. The EU's Reform and Growth Facility introduced performance-based conditionality that could, if enforced, extend to legacy Chinese infrastructure rather than applying only to new deployments. However, centralized decisionmaking, the Kosovo dynamic, and limited enforcement capacity all favor continuity. Space-based connectivity remains the least developed and most open layer, representing a potential future arena of competition in which early regulatory and commercial decisions may shape long-term alignment. The broader lesson is that conditionality without enforcement and signaling without financing have shaped governance frameworks while leaving the underlying digital infrastructure tied to Chinese providers. Addressing these dynamics both within and beyond the digital sector will shape the scope for future shifts in infrastructure alignment.

Undersea Cables

Lead finding: The undersea cable market represents an unambiguous U.S. and allied success, demonstrating that a coordinated combination of financial tools, regulatory instruments, and diplomatic pressure can exclude Chinese providers from critical global infrastructure—even when they offer significantly lower bids—because U.S. market leverage and legal jurisdiction created switching costs that Chinese state subsidies could not overcome.

Undersea cables merit their own case study as an especially unique combination of physical and digital infrastructure. They are transnational in nature—in that they connect multiple countries and are often owned by consortia of multinational corporations—and therefore they do

not belong neatly within the parameters of a country-specific case study like the others in this report.

Infrastructure Baseline

The market for undersea cables is multifaceted. Given the high cost of large cable projects—ranging in the hundreds of millions of dollars for transcontinental cables[293]—each cable is often funded and owned by a consortium of telecommunications and cloud computing providers, who use most of the bandwidth for their own commercial data purposes while leasing out excess capacity to other firms.[294] By contrast, the undersea cable supply and installation market is far more consolidated and is largely dominated by France's ASN, the United States' SubCom, Japan's NEC, and, to a lesser extent, China's HMN Tech.[295]

Western firms command the market for undersea cables at both the ownership and supply levels of analysis. As of 2024, digital titans, such as Amazon, Google, Meta, and Microsoft, own or lease approximately half of global undersea bandwidth.[296] For cable suppliers, the comparison is similarly striking. Of the larger global cable projects for which there are data, the three Western suppliers possess a commanding lead in every important metric, as shown in Table C.1.

Table C.1. Comparison of Key Metrics in Undersea Cable Supply and Installation Market

Supplier	Number of Systems	Percentage of Systems	Total Distance of Cables (km)	Percentage of Total Distance	Number of Cable-Laying Vessels
ASN	145.04	37.53	577,878	39.42	5
SubCom	70.96	18.36	496,900	33.90	7
NEC	51.11	13.23	223,018	15.21	2 (planned)
HMN Tech	39	10.09	69,172	4.72	2

SOURCE: Features data from TeleGeography, "Submarine Cable Map"; Submarine Telecoms Forum, *Submarine Telecoms Industry Report 2025–2026*; Alcatel Submarine Networks, "ASN Fleet"; NEC Corporation, "NEC Signs Long-Term Charter Contract with Global Marine Systems Limited for Optical Submarine Cable-Laying Ship"; and Dempsey and Keohane, "Japan Set to Make Subsea Cables a National Security Issue with Support for New Fleet."

With support from Beijing, HMN Tech initially made significant inroads into the industry but has suffered a series of critical setbacks over the past few years.[297] Perhaps the best example is the loss of the South East Asia–Middle East–Western Europe 6 cable project (SeaMeWe-6) to SubCom in 2022 despite several preexisting advantages, such as a lower bid ($475 million

[293] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[294] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 2.

[295] TeleGeography, "Submarine Cable Map."

[296] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 2.

[297] Submarine Telecoms Forum, *Submarine Telecoms Industry Report 2025–2026*.

compared with SubCom's $600 million), a favorable consortium of investors (including three Chinese state-owned enterprises that preferred HMN Tech), and an initial decision by the consortium in 2020 to choose HMN Tech. Beyond this high-profile incident, HMN Tech also lost a cable project that would have connected Nauru, the Federated States of Micronesia, and Kiribati because of a joint effort by the United States, Australia, and Japan to fund a cable along the same route (now called the East Micronesia Cable). And U.S. pressure has resulted in the cancellation of four cables that would have linked the United States to Hong Kong—including the PLCN and the Bay to Bay Express Cable System[298]—and may produce a similar result for the joint Chile-China cable project in 2026.[299] In this case study, we explore the reasons for this sudden change of fortune.

Competing Engagement Strategies

China

Similarly to many Chinese infrastructure and industrial efforts, Beijing's strategy for entering the undersea cable market was primarily defined by strong and sustained state support. HMN Tech was founded in 2008 under the name Huawei Marine Networks as a joint venture between Huawei Technologies and Global Marine Systems, before Hengtong Optic-Electric purchased a controlling interest in 2020.[300] It initially provided smaller cables in "underserved markets such as Papua New Guinea and the Caribbean,"[301] but it eventually began securing larger projects, such as the 15,500-mi "Peace Cable" across Asia, Africa, and Europe, which cost $425 million.[302] This meteoric rise was fueled by Chinese subsidies, which allowed HMN Tech to submit bids that were 20 percent to 30 percent lower than those of their Western rivals.[303] By commanding a greater share of the undersea cable market, Beijing sought to advance its DSR initiative, expand the reach of Chinese telecommunications and cloud service providers, and ultimately influence the exchange of data in the digital age.

However, despite the rapid growth of HMN Tech, Chinese telecommunications firms never secured enough leverage to create an enduring advantage in this market. In terms of suppliers, while the quality of Chinese telecommunications products (such as 5G) has improved, their offerings have still lagged behind comparable U.S. and allied efforts in traditional sectors, such

---

[298] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[299] Orellana, "Chinese Cable Project Causes Rift Before Chile Presidential Transition."

[300] Wenrong, "Hengtong Optoelectronics Completed the Acquisition of 81% of Huawei Marine's Shares, with an Expenditure of About 1.6 Billion Yuan"; INNOVATE Corporation, "INNOVATE Corp. Completes Sale of Remaining Equity Stake in HMN International."

[301] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[302] *Wall Street Journal*, "The Trillion-Dollar Battle for Fiber-Optic Supremacy."

[303] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 6.

as undersea cables.[304] And most importantly, as Washington began pressuring other companies and countries to exclude HMN Tech through a combination of sanctions and incentives, China and its firms lacked the market leverage to withstand this sustained campaign. For example, in the case of SeaMeWe-6, the United States' proposed sanctions against HMN Tech promised to undermine the value of the cable, thereby making SubCom a more compelling choice despite its higher bid. By contrast, when China Telecommunications Corporation and China Mobile Limited threatened to leave the SeaMeWe-6 consortium if it did not select HMN Tech, the loss of their relatively small share of the investment funds was not sufficiently compelling. The consortium was ultimately able to account for the loss of their tens of millions of dollars by increasing existing investments and including two new companies from Malaysia and Indonesia.[305] Therefore, U.S. threats were especially convincing because of their strong economic and commercial leverage relative to China. The future of China's campaign to control undersea cables is now murky, and HMN Tech may require substantial state support to remain a viable competitor in the future.

United States and Allies

By contrast, Western governments have shared a better understanding of their long-standing advantages in undersea cables and have actively protected these advantages in the face of Beijing's challenge. Indeed, despite having installed a vast majority of global undersea cables, ASN, NEC, and SubCom were increasingly threatened by HMN Tech's low bids over the past decade. As a result, their governments arguably borrowed from Beijing's industrial playbook and intervened to secure these companies through a variety of means, including France's 2024 acquisition of 80 percent of ASN's equity because of its role as a "strategic company"[306] and Japan's decision to subsidize NEC's purchase of two cable installation vessels.[307]

The U.S. government has been particularly active in the competition over undersea cables. Similarly to France and Japan, it boosted its own cable supplier, SubCom. In the case of SeaMeWe-6, these efforts included the provision of EXIM loans, which allowed SubCom to lower its initial SeaMeWe-6 bid from around $750 million to $600 million; the offer of U.S. Trade and Development Agency (USTDA) technical grants, at a total of $3.8 million, to five telecommunications companies in countries along the cable's route; and the threat of sanctions,

---

[304] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 6.

[305] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[306] Nokia, "Nokia Completes Its Sale of Leading Submarine Networks Business, ASN (Alcatel Submarine Networks), to the French State"; Pinaud, "'Strategic' Submarine Telecom Cable Manufacturer ASN Nationalized by France."

[307] Dempsey and Keohane, "Japan Set to Make Subsea Cables a National Security Issue with Support for New Fleet."

which undermined the value of HMN Tech's bid.[308] This combination of the proverbial carrot and stick allowed SubCom to prevail.

But U.S. ambitions extend beyond SubCom, as Washington seeks to curb Chinese influence in the undersea cables market and in the broader digital infrastructure ecosystem. For example, in 2020, Executive Order 13913 formalized Team Telecom—an interagency group of officials from the Departments of Justice, Defense, and Homeland Security and advised by the Departments of State, Treasury, and Commerce, in addition to other federal agencies—and empowered it to review "certain Federal Communications Commission (FCC) applications and licenses for national-security and law-enforcement risks."[309] With this authority, Team Telecom has worked to exclude Chinese penetration into the U.S. telecommunications industry, including the construction of any cables connecting China or Hong Kong to the United States.[310] Moreover, U.S. officials have used diplomatic pressure to convince other countries and their companies to drop Chinese projects and equipment, including a more recent cable project that would connect Chile to China.[311] Ultimately, the United States has leveraged its profound advantages for instrumental, relational, and strategic success.

Success Assessment

Instrumental Success

In comparison with other telecommunications infrastructure, undersea cables are incredibly costly and require specialized expertise to install and maintain. Every bid is an opportunity to generate lock-in effects over long time horizons. By forcefully intervening in high-profile cable projects, such as SeaMeWe-6, U.S. officials demonstrated a willingness to both lock in SubCom as a critical supplier for Western digital tech titans and, more importantly, lock out HMN Tech from the most impactful data highways of the future.

Moreover, the United States has demonstrated a profound understanding of the instrumental leverage provided by its role as a hub of global economic activity and its legal and regulatory regimes that govern the local exchange of strategic commodities. Team Telecom and the FCC have been successful in excluding Chinese firms from undersea cables and related infrastructure projects that connect to the United States, thereby guarding against espionage and national security concerns while ensuring the compliance of firms that do business with the United States.[312] And for projects beyond the United States' borders, the threat of sanctions on HMN

---

[308] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[309] National Security Division, "Team Telecom."

[310] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables"; Oriishi, "What Has the U.S. Government Gained by Formalizing Team Telecom?"

[311] Batschke, "US Ambassador Defends Travel Bans on 3 Chilean Officials as a 'Sovereign Decision.'"

[312] Federal Communications Commission, "FCC Acts to Accelerate Submarine Cable Buildout & Security."

Tech makes it very difficult—and potentially cost-prohibitive—for major tech companies, such as Amazon, Meta, and Microsoft, to use Chinese-built cables.[313] As a result, multinational corporations are increasingly wary of HMN Tech and would prefer to use cables and equipment produced by the United States and its allies.

China is attempting to exploit its own leverage for cables that connect to its mainland or to Hong Kong—for example, by blocking the Southeast Asia–Japan 2 cable over concerns of espionage from NEC.[314] But the United States and its allies have exerted greater influence over longer transcontinental cables in recent years.

Relational Success

Traditionally, U.S. companies have struggled to compete with the systematically lower bids of their Chinese counterparts. Even in the case of SeaMeWe-6, EXIM loans only helped SubCom lower its bid from around $750 million to $600 million while HMN Tech lowered its bid from $500 million to $475 million. However, the United States maintains advantages for securing relational success that can account for this disadvantage in cost competition.

First, the United States has a history of building capacity among its partners, thereby contributing to greater technological sovereignty over time. In the case of SeaMeWe-6, technical assistance proved decisive.[315] USTDA offered training grants valued at a total of $3.8 million to five telecommunications companies along the cable's route—indeed, "Telecom Egypt and Network i2i Limited, a company owned by India's Bharti Airtel Limited, got $1 million apiece . . . [and] Djibouti Telecom, Sri Lanka Telecom and Dhivehi Raajjeyge Gulhun of the Maldives each received $600,000."[316] Moreover, in 2023, the Indo-Pacific Quad pledged $5 million in CABLES program funding to facilitate technical assistance and capacity-building on undersea cables.[317] However, as of 2026, the White House website for CABLES is down, which suggests that the program may no longer exist.

Second, Washington has relied on diplomacy to build trust and legitimacy, especially among strategically compatible allies. For SeaMeWe-6 and similar projects, State Department officials warned other countries about the risks of Chinese espionage in undersea cables. And to ensure greater legitimacy, the United States has collaborated with like-minded allies to raise awareness on this issue set, including by working with Australia and Japan to fund the East Micronesia Cable and by committing to undersea cable security alongside Quad and G7 partners.[318]

---

[313] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[314] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[315] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 6.

[316] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[317] Botting and Jordan-Zoob, "How the US and Its Partners Can Ensure the Worlds' Data Super-Highways Remain Reliable, Secure, Open & Free"; Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 10.

[318] Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables"; Botting and Jordan-Zoob, "Competing Visions for the Future of the Internet."

As a result, HMN Tech is no longer a trusted brand among core U.S. allies in Europe, Japan, and Australia. And for other partners that may not share the same concerns about Chinese espionage, there are incentives to work more closely with U.S. and Western firms.

Strategic Success

Undersea cables represent major chokepoints in the global flow of information and can be vulnerable to a variety of disruptions.[319] However, by excluding HMN Tech from installing future cables, the United States and its allies have both guarded their influence over these chokepoints and undermined the reach of Chinese telecommunications companies that would otherwise invest in large cable projects.

While various tools of "seabed warfare"[320] are still available to Beijing—including espionage, disruption, and sabotage—they require specialized equipment and risk attribution.[321] China may seek to leverage its world-leading shipbuilding capacity to provide repair fleets in the future,[322] which could represent a vector for these covert toolsets, but they are not as potent as installing the cable directly. And these toolsets would only be helpful in strict national security applications, vice the broader objectives of China's ambitious DSR initiative.

Moreover, as Western tech firms continue to build more, and more resilient, networks—ranging from new undersea cables to satellite and wireless communications—they will actually *decrease* the salience and importance of any particular chokepoint. China's ability to influence undersea cable projects, whether through ownership, supply, or covert means, may be less important in the future. But this trend also opens new arenas for competition over telecommunications, and the United States cannot be complacent with its lead in more traditional undersea cables.

Looking Forward

Thus far, the United States and its allies have retained their advantage. Western tech titans own the most important undersea cable projects of the future and continue to employ U.S., French, and Japanese cable providers. Meanwhile, HMN Tech's once-stunning growth has stunted; such companies as China Telecom and China Mobile may struggle to exert their influence on cable investment consortia; and fewer cables may connect other countries to China in the future.

---

[319] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 3; Gambrell, "Undersea Cables Cut in the Red Sea, Disrupting Internet Access in Asia and the Mideast"; Aitken, "Microsoft Warns of Service Issues After Subsea Cables Cut in the Red Sea."

[320] Brooke-Holland, "Seabed Warfare."

[321] Aitken, "Undersea Cables Are Vulnerable to Sabotage—but This Takes Skill and Specialist Equipment."

[322] Runde, Murphy, and Bryja, *Safeguarding Subsea Cables*, p. 3.

But there are reasons for concern. In the case of the Chile-China cable project, the United States leveraged sanctions against Chilean officials once other diplomatic efforts failed, resulting in backlash from the outgoing Chilean administration and a request to remove the U.S. ambassador to Chile.[323] While the incoming administration is more skeptical of the project and may ultimately comply with the U.S. position,[324] this case serves as a cautionary tale that too much pressure, especially in the absence of stronger incentives, can cause relational and potentially strategic harm, especially for such a partner as Chile that does not enjoy the same degree of strategic compatibility with the United States.

The U.S.-China competition over undersea cables underscores the importance of maximizing leverage through cost feasibility, regulatory control, and strategic compatibility. China's HMN Tech succeeded early by offering steeply discounted bids through state-backed subsidies but ultimately failed to convert these successes into durable influence. The United States and its allies, meanwhile, combined such financial tools as EXIM loans and USTDA grants with the persuasive power of legal, regulatory, and diplomatic instruments to steer projects toward trusted Western suppliers. Moving forward, U.S. strategy should focus on continuing to deploy these complementary carrot-and-stick mechanisms to both increase the relative financial, political, and opportunity costs of working with Chinese firms and bolster the reputation of Western firms as trusted partners. Table C.2 summarizes our insights across the case studies.

[323] Orellana, "Chinese Cable Project Causes Rift Before Chile Presidential Transition."

[324] Batschke, "Kast Takes Office as Chile Marks Its Sharpest Shift to the Right Since Dictatorship."

Table C.2. Comparison of Insights Across Case Studies

Case Study	Key Milestones and Procurement Decisions	Factors Governing Success (Advantage)	Outcome
Costa Rica	• Huawei secured the first 3G contract with ICE (2009). • Costa Rica issued a decree barring non-signatories to the Budapest Convention on Cybercrime from participating in 5G networks (2023). • The United States and Costa Rica released a joint statement committing to Open RAN and joint collaboration (2024).	Primary • Cost and economic feasibility (U.S.) • Technology capabilities and quality (U.S.) • Digital governance and institutions (U.S.) • Ecosystem advantages (U.S.) Secondary • Regulatory, legal, and policy environments (U.S.)	• *Instrumental:* Costa Rica has anchored its 5G and cybersecurity architecture in Western suppliers. • *Relational:* U.S. aid was viewed as reliable in the wake of debilitating ransomware attacks on Costa Rica. • *Strategic:* The United States and allies have greater advantages in Costa Rica but have not entirely excluded Chinese technology from Costa Rican infrastructure. • *Outcome:* Durable Western alignment exists in a country that had once featured early footholds by Chinese vendors.
Nigeria	• Chinese companies invested more than $16 billion in Nigerian telecommunications (by 2018). • The Export-Import Bank of China acquired a stake in Nigerian satellite comms company NIGCOMSAT (2018). • U.S. tech titans, such as Meta, Microsoft, and IBM, reduced their presence (2024–2025).	Primary • Cost and economic feasibility (PRC) Secondary • On-the-ground presence and local training and workforce development programs (PRC) • Lock-in effects (PRC) • Elite co-optation (PRC) • Regulatory, legal, and policy environments (PRC)	• *Instrumental:* Chinese firms are embedded in Nigerian digital infrastructure, generating lock-in effects. • *Relational:* China offers better deals, consistent relationships, and greater capacity-building. • *Strategic:* The PRC has greater leverage for coercion and new opportunities for geopolitical competition. • *Outcome:* Chinese dominance exists across digital infrastructure layers, leaving only venture capital–scale U.S. engagement where infrastructure-scale investment is required.
Serbia	• Serbia signed a BRI memorandum of understanding (2015). • Serbia and the PRC announced their Sino-Serbian Comprehensive Strategic Partnership, formalizing cooperation across multiple sectors (2016). • Serbia formally aligned digital governance with European standards via a GDPR-inspired data protection law (2018) and a National AI Strategy (2019). • Serbia completed its 5G spectrum auction,	Primary • Political and strategic alignment and compatibility (PRC) • Cost and economic feasibility (PRC) • Ecosystem advantages (PRC) • Digital governance and institutions (PRC) Secondary • Regulatory, legal, and policy environments (U.S./Europe) • Elite co-optation (PRC) • On-the-ground presence and local	• *Instrumental:* Chinese firms maintain strong positions across legacy telecommunications, surveillance infrastructure, and data infrastructure; while Western actors have made inroads in the fiber backbone, 5G, and AI infrastructure, they build on Chinese-provided infrastructure. • *Relational:* The PRC maintains leverage from its broader strategic partnership with Serbia, particularly via its diplomatic support on the Kosovo issue, cooperation in energy and defense, and elite ties. • *Strategic:* The result is a hybrid system in which regulatory alignment points West while

Case Study	Key Milestones and Procurement Decisions	Factors Governing Success (Advantage)	Outcome
	emphasizing procurement from European vendors without excluding Chinese vendors (2025).	training and workforce development programs • Lock-in effects (PRC)	underlying infrastructure remains tied to Chinese providers. • *Outcome:* Conditionality without enforcement and signaling without financing have shaped governance frameworks while leaving the underlying digital infrastructure tied primarily to Chinese providers.
Philippines	• DITO Telecommunity is rolled out, with Chinese ties (2021). • The Philippines withdrew from the BRI (2023). • The Philippines' DICT rolled out its NDCP, laying out targets for wireless connectivity through 2028 (2026).	Primary • Cost and economic feasibility (PRC) • Ecosystem advantages (PRC) • Digital governance and institutions (PRC/U.S.) • Political and strategic alignment and compatibility (U.S.) • Technology capabilities and quality (U.S.) Secondary • Regulatory, legal, and policy environments (U.S.)	• *Instrumental:* Chinese firms have established a foothold in telecommunications while U.S. and allied actors have achieved stronger positions in cloud infrastructure, subsea connectivity, and satellite services. • *Relational:* The United States and allies benefit from alignment with Philippine cybersecurity frameworks, security standards, and global integration, but the PRC has performed well on telecommunications contracts. • *Strategic:* Neither competitor has achieved dominance across the digital stack. • *Outcome:* Despite the Philippines' active security tensions with China and strong U.S. alignment, Chinese-linked firms have secured a significant foothold in telecommunications.
Undersea cables	• U.S. pressure has resulted in the cancellation of four cables that would have linked the United States to Hong Kong (since 2020). • HMN Tech lost a cable project (now called the East Micronesia Cable) to the United States, Australia, and Japan (2021). • SubCom beat HMN Tech for the SeaMeWe-6 cable project (2022).	Primary • Political and strategic alignment and compatibility (U.S.) • Technology capabilities and quality (U.S.) • Cost and economic feasibility (PRC) Secondary • Regulatory, legal, and policy environments (U.S.) • On-the-ground presence and local training and workforce development programs (U.S.)	• *Instrumental:* U.S. officials locked in SubCom and locked out HMN Tech from critical cable projects. • *Relational:* U.S. training grants and diplomacy overcame SubCom's inability to compete with HMN Tech on cost. • *Strategic:* The United States and allies guarded their influence over key chokepoints and undermined the reach of Chinese firms. • *Outcome:* Unambiguous U.S. and allied success results, capitalizing on U.S. market leverage and legal jurisdiction that Chinese state subsidies could not overcome.

Abbreviations

3GPP	3rd Generation Partnership Project
AI	artificial intelligence
ASN	Alcatel Submarine Networks
AWS	Amazon Web Services
BRI	Belt and Road Initiative
CBERS	China-Brazil Earth Resources Satellite
DFC	U.S. International Development Finance Corporation
DICT	Department of Information and Communications Technology
DSR	Digital Silk Road
EU	European Union
EXIM	Export-Import Bank of the United States
FCC	Federal Communications Commission
fintech	financial technology
G7	Group of Seven
G7+	Group of Seven Plus
GDP	gross domestic product
GDPR	General Data Protection Regulation
GEO	geostationary orbit
GNSS	global navigation satellite system
GPS	Global Positioning System
GPU	graphics processing unit
ICE	Instituto Costarricense de Electricidad
ILRS	International Lunar Research Station
IoT	Internet of Things
LEO	low earth orbit
LLM	large language model
MEO	medium earth orbit
NASA	National Aeronautics and Space Administration
NDCP	National Digital Connectivity Plan
NEC	Nippon Electric Company
PLCN	Pacific Light Cable Network
PNT	positioning, navigation, and timing
PRC	People's Republic of China
R&D	research and development
RAN	radio access network

SeaMeWe-6	South East Asia–Middle East–Western Europe 6
SEP	standard-essential patent
SMS	Short Message Service
TAM-1	Trans Americas Fiber System
TT&C	telemetry, tracking, and command
USTDA	U.S. Trade and Development Agency

References

Unless otherwise indicated, the authors of this annex provided the translations of bibliographic details for the non-English sources. To support conventions for alphabetizing, sources in Chinese are introduced with and organized according to their English translations. The original rendering in Chinese appears in brackets after the English translation.

Aitken, John, "Undersea Cables Are Vulnerable to Sabotage—but This Takes Skill and Specialist Equipment," *The Conversation*, July 7, 2025.

Aitken, Peter, "Microsoft Warns of Service Issues After Subsea Cables Cut in the Red Sea," *Newsweek*, September 6, 2025.

Alcatel Submarine Networks, "ASN Fleet," webpage, undated. As of January 29, 2026: https://www.asn.com/our-fleet/

Allan, Bentley, *Regaining Geopolitical Advantage: How to Focus U.S. Foreign Policy for Clean Energy*, Carnegie Endowment for International Peace, February 2025.

Álvarez, Mariana, "Costa Rica Will Be the First Country in Central America to Have an Artificial Intelligence Strategy," United Nations Educational, Scientific and Cultural Organization, February 28, 2023.

Amazon Web Services, "Announcing the General Availability of AWS Local Zones in Manila," June 19, 2023.

Ammachchi, Narayan, "Washington's Warning to Costa Rica: Keep Your 5G Networks China-Free," Nearshore Americas, April 17, 2024.

Arha, Kaush, *Trusted Connectivity: A Framework for a Free, Open, and Connected World*, Atlantic Council, August 2021.

Arha, Kaush, "The G7's $600 Billion Response to China's Belt and Road Initiative Is Here. This Is How to Make Sure It Succeeds," *New Atlanticist* blog, Atlantic Council, November 8, 2022. As of September 1, 2026: https://www.atlanticcouncil.org/blogs/new-atlanticist/the-g7s-600-billion-response-to-chinas-belt-and-road-initiative-is-here-this-is-how-to-make-sure-it-succeeds/

Balbontin, Rodrigo, "Backfire: Export Controls Helped Huawei and Hurt U.S. Firms," Information Technology and Innovation Foundation, October 27, 2025.

Balogun, Folake, "China Tightens Grip on Nigeria's Tech Landscape as the U.S. Trails Behind," *Business Day*, October 28, 2025.

Bataller, Diana Elaine, "What the 2026 SIPP Reveals About the Philippines' Future," Deloitte, undated.

Batschke, Nayara, "US Ambassador Defends Travel Bans on 3 Chilean Officials as a 'Sovereign Decision,'" Associated Press, February 23, 2026.

Batschke, Nayara, "Kast Takes Office as Chile Marks Its Sharpest Shift to the Right Since Dictatorship," Associated Press, March 11, 2026.

Bazmi, Noor, "China Hits U.S. Optical Fiber Suppliers with Rate Hikes in Trade Tension Escalation," MSN, September 4, 2025.

Ben-Itzhak, Svetla, "Network Analysis of International Cooperation in Space 1958–2023: Evidence of Space Blocs," *Journal of Peace Research*, Vol. 62, No. 3, 2025.

Berman, Noah, Lindsay Maizland, and Andrew Chatzky, "Is China's Huawei a Threat to U.S. National Security?" Council on Foreign Relations, February 8, 2023.

Beszeditz, David, *Chinese Space Cooperation in Latin America: Implications for United States Space Security*, thesis, Naval Postgraduate School, September 2021.

BNamericas, "Costa Rica Investigates Alleged Irregularities in Huawei Contract," August 14, 2020.

Botting, Alex, and Inés Jordan-Zoob, "Optical Core Infrastructure: The Hidden Highway of Connectivity," Wilson Center, February 28, 2024.

Botting, Alex, and Inés Jordan-Zoob, "Competing Visions for the Future of the Internet: China's Strategy to Control the Highways of Connectivity," Wilson Center, May 9, 2024.

Botting, Alex, and Inés Jordan-Zoob, "How the US and Its Partners Can Ensure the Worlds' Data Super-Highways Remain Reliable, Secure, Open & Free," Wilson Center, July 15, 2024.

Boullenois, Camille, Malcolm Black, and Daniel H. Rosen, *Was Made in China 2025 Successful?* Rhodium Group and U.S. Chamber of Commerce, May 5, 2025.

Bowe, Alexander, *China's Pursuit of Space Power Status and Implications for the United States*, U.S.-China Economic and Security Review Commission, April 11, 2019.

Brackup, Julia, Sarah Harting, and Daniel Gonzales, *Digital Infrastructure and Digital Presence: A Framework for Assessing the Impact on Future Military Competition and Conflict*, RAND Corporation, RR-A877-1, 2022. As of August 25, 2026: https://www.rand.org/pubs/research_reports/RRA877-1.html

Brackup, Julia, Sarah Harting, Daniel Gonzales, and Brandon Corbin, *Alternative Futures for Digital Infrastructure: Insights and Considerations for the Department of Defense*, RAND Corporation, RR-A1859-1, 2023. As of August 25, 2026: https://www.rand.org/pubs/research_reports/RRA1859-1.html

Bradley, Chris, Michael Chui, Kevin Russell, Kweilin Ellingrud, Michael Birshan, and Suhayl Chettih, *The Next Big Arenas of Competition*, McKinsey Global Institute, October 2024.

Bradsher, Keith, and Adam Nossiter, "In Nigeria, Chinese Investment Comes with a Downside," *New York Times*, December 5, 2015.

Brock, Joe, "U.S. and China Wage War Beneath the Waves—over Internet Cables," Reuters, March 24, 2023.

Brooke-Holland, Louisa, "Seabed Warfare: Protecting the UK's Undersea Infrastructure," UK Parliament House of Commons Library, May 24, 2023.

Bruer, Alexandra, and Doug Brake, *Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy and Policy*, Information Technology and Innovation Foundation, November 8, 2021.

Bull, "Eviden Signs a 50-Million-Euro Contract to Build Serbia's National AI Factory," press release, April 10, 2025.

Burningham, Grant, "Why Microsoft and Facebook Are Building a Superfast Trans-Atlantic Cable," *Newsweek*, last updated June 15, 2016.

Cadell, Cate, and Marcelo Perez del Carpio, "A Growing Global Footprint for China's Space Program Worries Pentagon," *Washington Post*, November 21, 2023.

Camus, Miguel R., "Third Telco Bidding Aftermath: Your Questions Answered," *Business Inquirer*, November 12, 2028.

Carrai, Maria Adele, "Is America Losing the Global South? Assessing the Dynamics of Sino-American Rivalry in Infrastructure Diplomacy," *Orbis*, Vol. 67, No. 4, 2023.

Casaccia, Lorenzo, "Why Qualcomm Is the True Leader in 5G—a Story of Foundational Inventions," *OnQ Blog*, Qualcomm, December 15, 2022. As of September 1, 2026: https://www.qualcomm.com/news/onq/2022/12/why-qualcomm-is-the-true-leader-in-5g

Chambers, Rob W., *China's Space Program: A New Tool for PRC "Soft Power" in International Relations*, thesis, Naval Postgraduate School, March 2009.

Chaudhary, Archana, Ragini Saxena, P. R. Sanjai, and Saritha Rai, "China's Huawei, ZTE Face India 5G Network Exclusion: Report," Al Jazeera, August 14, 2020.

Chee, Foo Yun, "EU Plan to Phase-Out High-Risk Tech Draws Fire from China's Huawei," Reuters, January 21, 2026.

Chilukuri, Vivek, and Ruby Scanlon, *Countering the Digital Silk Road*, Center for a New American Security, October 15, 2025.

"China Home to 3.92 Million 5G Base Stations," *China Daily*, July 24, 2024.

Cloudscene, "North America," webpage, undated. As of January 29, 2026: https://cloudscene.com/region/datacenters-in-north-america

Colback, Lucy, "Why It Is Vital That You Understand the Infrastructure Behind AI," *Financial Times*, July 6, 2025.

Costa Rica Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, *Plan Nacional de Desarrollo de las Telecomunicaciones 2022–2027: Costa Rica; Hacia la disrupción digital inclusiva*, 2022.

Costa Rica Ministry of Foreign Trade, *Roadmap for Strengthening the Semiconductor Ecosystem in Costa Rica*, March 2024.

Council of the European Union, "ChatGPT in the Public Sector—Overhyped or Overlooked?" April 24, 2023.

Council on Foreign Relations, "Assessing China's Digital Silk Road Initiative," undated. As of August 8, 2025: https://www.cfr.org/china-digital-silk-road/

Croshier, Rose, *Opportunities for US-Africa Space Cooperation and Development*, Center for Global Development, Policy Paper 256, March 2022.

CSA Group, "Costa Rica (SUTEL)—National Frequency Allocation Plan Update," webpage, July 2021. As of January 25, 2026: https://www.csagroup.org/global-certification-regulatory-update/costa-rica-sutel-national-frequency-allocation-plan-update/

Cyber and Infrastructure Security Agency, *Overview of Risks Introduced by 5G Adoption in the United States*, July 31, 2019.

"Data Center Firm Equinix Enters the Philippines, Eyes on Southeast Asia," Reuters, July 22, 2024.

De Luca, Stefano, *The Path to 6G*, European Parliament, PE 757.633, January 2024.

de Vries, Alex, "The Growing Energy Footprint of Artificial Intelligence," *Joule*, Vol. 7, No. 10, October 2023.

Dempsey, Harry, and David Keohane, "Japan Set to Make Subsea Cables a National Security Issue with Support for New Fleet," *Financial Times*, September 15, 2025.

Directorate-General for Enlargement and Eastern Neighbourhood, "Reform and Growth Facility for the Western Balkans," European Commission, webpage, undated. As of September 2, 2026: https://enlargement.ec.europa.eu/funding-technical-assistance/reform-and-growth-facility-western-balkans_en

Dragojlo, Sasa, "China's Huawei Opens Tech Centre, Consolidating Presence in Serbia," Balkan Insight, September 15, 2020.

Duterte, Rodrigo R., Expanding the Provision of Internet Services Through Inclusive Access to Satellite Services, Amending Executive Order No. 467 (s. 1998) for the Purpose, Executive Order No. 127, s. 2021, Office of the President of the Philippines, March 10, 2021.

Edl, Andras, "Developing Space Programs and Cooperation in Latin America," *Academic and Applied Research in Military and Public Management Science*, Vol. 21, No. 3, 2022.

Edquist, Harald, Peter Goodridge, and Jonathan Haskel, "The Internet of Things and Economic Growth in a Panel of Countries," *Economic of Innovation and New Technology*, Vol. 30, No. 3, 2021.

Ellis, R. Evan, "China-Latin America Space Cooperation: An Overview," *The Diplomat*, February 16, 2024.

Ellis, R. Evan, "China's Successes and Struggles in Costa Rica," *The Diplomat*, August 2, 2025.

Endeshaw, Dawit, "Ethiopia's State Telecom Launches 5G Services in Capital," Reuters, May 10, 2022.

Ericsson, "5G Explained," webpage, undated. As of August 31, 2026: https://www.ericsson.com/en/5g

Ericsson, "Liberty and Ericsson Switch on First 5G Standalone Network for Mobile Services in Costa Rica and Central America," press release, July 15, 2025.

"EU Moves to Force the Phase-Out of Chinese Suppliers from Key Infrastructure, FT Reports," Reuters, January 16, 2026.

European Commission, "Costa Rica," webpage, undated. As of January 25, 2026: https://international-partnerships.ec.europa.eu/countries/costa-rica_en

European Space Agency, "New ESOC GNSS Station in Costa Rica," webpage, undated. As of January 25, 2026: https://esoc.esa.int/content/new-esoc-gnss-station-costa-rica

EXA Infrastructure, "EXA Infrastructure to Purchase Longhaul Duct Assets from Conexio," press release, October 23, 2025.

EXIM—*See* Export-Import Bank of the United States.

Export-Import Bank of the United States, "EXIM Board of Directors Approves Preliminary Commitment to Support Development of 5G Network in Costa Rica," June 9, 2023.

Faller, Craig S., "Posture Statement of Admiral Craig S. Faller, Commander United States Southern Command," testimony before the U.S. House Armed Services Committee, U.S. Southern Command, May 1, 2019.

Fedasiuk, Ryan, Emily Weinstein, and Anna Puglisi, *China's Foreign Technology Wish List*, Center for Security and Emerging Technology, May 2021.

Federal Communications Commission, "FCC Acts to Accelerate Submarine Cable Buildout & Security: Action Boost America's Leadership in AI and Next-Gen Technologies," August 7, 2025.

Feldgoise, Jacob, Catherine Aiken, Emily S. Weinstein, and Zachary Arnold, "Studying Tech Competition Through Research Output: Some CSET Best Practices," blog post, Center for Security and Emerging Technology, April 2023. As of September 1, 2026: https://cset.georgetown.edu/article/studying-tech-competition-through-research-output-some-cset-best-practices/

Ficili, Ilenia, Maurizio Giacobbe, Giuseppe Tricomi, and Antonio Puliafito, "From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI," *Perspectives in Intelligent Sensors and Sensing Systems*, Vol. 25, No. 6, 2025.

Financial Times, "AI Power Demand Could Stifle Industry's Growth: FT Energy Source," video, August 19, 2024. As of August 31, 2026: https://www.youtube.com/watch?v=rcIqrT5rIzw&t=4s

Flores, Mikhail, "US Companies to Announce Investments of over $1Bln in the Philippines," Reuters, March 11, 2024.

Freedom House, "Costa Rica: Key Developments, June 1, 2023–May 31, 2024," webpage, undated. As of January 25, 2026: https://freedomhouse.org/country/costa-rica/freedom-net/2024

Frimpong, Paul, *China's Modernization: Catalyzing Sustainable Growth in Developing Countries*, Africa-China Centre for Policy & Advisory, February 2, 2024.

Fujitsu and Rakuten Mobile, "Rakuten Mobile Partners with Fujitsu to Accelerate 5G Network Expansion," press release, March 3, 2025.

Funaiole, Matthew P., Dana Kim, Brian Hart, and Joseph S. Bermudez, Jr., "Eyes on the Skies: China's Growing Space Footprint in South America," Hidden Reach Issue No. 1, Center for Strategic and International Studies, October 4, 2022.

Gambrell, Jon, "Undersea Cables Cut in the Red Sea, Disrupting Internet Access in Asia and the Mideast," Associated Press, September 7, 2025.

Gargeyas, Arjun, "Digital and Energy Infrastructure Are Fueling Important Progress. Integrating Them Can Maximize the Benefits," Digital Impact Alliance, June 12, 2025.

Giannopapa, Christina, Athanasios Staveris-Poykalas, and Spyros Metallinos, "Space as Enabler for Sustainable Digital Transformation: The New Space Race and Benefits for Newcomers," *Acta Astronautica*, Vol. 198, September 2022.

GIP Digital Watch, "Costa Rica's Digital Transformation Strategy (2023–2027)," September 2022.

Goujon, Reva, Ben Reynolds, Ciel Qi, Lauren D. Piper, and John Larsen, *Fighting Hubris in AI Strategy: A Layer-by-Layer Dissection of AI Tech Stack Competition*, Rhodium Group, August 2026.

GPS, "Space Segment," webpage, undated. As of January 29, 2026: https://www.gps.gov/space-segment

Greig, Jonathan, "US Commits $25 Million to Costa Rica for Conti Ransomware Recovery," *The Record*, March 29, 2023.

Hart, Melanie, and Jordan Link, *There Is a Solution to the Huawei Challenge*, Center for American Progress, October 14, 2020.

Hilario, Edgard, "NTC Greenlights Starlink VAS Provider Registration," *Manila Bulletin*, May 27, 2022.

Hungerland, Nils, and Kenddrick Chan, "Assessing China's Digital Silk Road: Huawei's Engagement in Nigeria," working paper, London School of Economics and Political Science, November 2021.

IDB Invest, "IDB Invest, Liberty Costa Rica Launch Digital Infrastructure Sustainability-Linked Bond," January 26, 2023.

Ijaseun, David, "Why More Multinational Firms May Exit Nigeria—Report," Business Day, January 12, 2024.

INNOVATE Corporation, "INNOVATE Corp. Completes Sale of Remaining Equity Stake in HMN International," press release, March 7, 2023.

Intel, "Intel, Biden-Harris Administration Finalize $7.86 Billion Funding Award Under US CHIPS Act," press release, November 26, 2024.

IntelliNews, "Telekom Srbija and Huawei Launch €150mn Project to Develop Landline Network in Serbia," October 6, 2016.

International Energy Agency, "AI Is Set to Drive Surging Electricity Demand from Data Centres While Offering the Potential to Transform How the Energy Sector Works," April 10, 2025.

International Institute for Strategic Studies, "DeepSeek's Release of an Open-Weight Frontier AI Model," *Strategic Comments*, Vol. 31, April 2025.

International Trade Administration, "Serbia Country Commercial Guide: Digital Economy," last updated December 2, 2025. As of September 2, 2026: https://www.trade.gov/country-commercial-guides/serbia-digital-economy

Jagtiani, Sharinee L., *Risky Configuration: China's Footprint in Germany's Technology Stack*, German Marshall Fund of the United States, September 2025.

Jaiyeola, Temitayo, "American Company, IBM, Exits Nigeria in Latest Tech Exodus," *Business Day*, February 5, 2025.

Jankovic, Jelena, and Reid Standish, "Leaked Files Reveal Serbia's Secret Expansion of Chinese-Made Surveillance," Radio Free Europe/Radio Liberty, August 12, 2025.

Jiang, Kun, Wolfgang Keller, Larry D. Qui, and William Ridley, "International Joint Ventures and Internal Technology Transfer vs. External Technology Spillovers: Evidence from China," *Journal of International Economics*, Vol. 150, July 2024.

Johan, Affandy, "Fiber in the Philippines Is Improving and Catching Up with Its Regional Peers," Ookla, July 22, 2024.

Johnson, Clete, "Next Steps to Close the Gap with China on Licensed Spectrum for Commercial 5G," Center for Strategic and International Studies, February 12, 2024.

Johnson, Matthew, "Smart Device Empire: Beijing's Expansion Through Everyday Digital Infrastructure," Jamestown Foundation, July 25, 2025.

Joint SDG Fund, "Transforming Territories in Costa Rica with Digital Innovation and Women's Leadership," August 25, 2025.

Jones, Andrew, "China Files ITU Paperwork for Megaconstellations Totaling Nearly 200,000 Satellites," *SpaceNews*, January 12, 2026.

JPM Law Office, "Serbia: New Law on Information Security (Part I)," December 24, 2025.

Jung, Eric, "The 'Chip 4 Alliance' and Taiwan-South Korea Relations," *Global Taiwan Brief*, Global Taiwan Institute, Vol. 8, No. 18, September 20, 2023.

Kai Loung, Vincent Yong, Razali Ngah, Joseph Owusu, Chua Tien Han, Samuel Tweneboah-Koduah, and Jafri Din, "Key Technologies and Future Trends of 5G Wireless Network Applications," paper presented at the 6th International Conference on Signal and Image Processing, 2021.

Kehoe, Luke, "5G in the Balkans: Serbia's Mobile Renaissance as New Spectrum Fuels Competitiveness," Ookla, February 18, 2026.

Kelmer Group, "Philippines Targets P4.5 Trillion in Investments: The New SIPP 2026–2028 and What It Means for Foreign Businesses," July 31, 2026.

Klinger, Julie Michelle, "A Brief History of Outer Space Cooperation Between Latin America and China," *Journal of Latin American Geography*, Vol. 17, No. 2, July 2018.

Klinger, Julie Michelle, and Temidayo Isaiah Oniosun, *China's Space Collaboration with Africa: Implications and Recommendations for the United States*, United States Institute of Peace, Special Report 524, September 2023.

Koley, Bikash, "Announcing Apricot: A New Subsea Cable Connecting Singapore to Japan," blog post, Google Cloud, August 16, 2021. As of March 19, 2026: https://cloud.google.com/blog/products/infrastructure/new-apricot-subsea-cable-brings-more-connectivity-to-asia

Kumar, Suneel, "China's Digital Expansionism in Africa and the US Counter-Strategies," *Insight on Africa*, Vol. 16, No. 2, 2024.

LAPOP Lab, "AmericasBarometer Data Playground," webpage, Center for Global Democracy, Vanderbilt University, undated. As of August 28, 2025: https://www.vanderbilt.edu/lapop/data-playground-eng.php

Lee-Makiyama, Hosuk, and Robin Baker, *How Huawei Weathered the Storm: Resilience, Market Conditions or Failed Sanctions?* European Centre for International Political Economy, 2024.

Lewis, James Andrew, *How 5G Will Shape Innovation and Security*, Center for Strategic and International Studies, December 16, 2018.

LexisNexis, "Who Is Leading the 5G Patent Race? 5G Report—January 2026," January 2026.

Li, Xiaodao, "Comparing the Power Resources Critical to International Rulemaking in Outer Space: China and the United States," *Advances in Space Research*, Vol. 72, No. 6, 2023.

Liu, Zongyuan Zoe, "Tracking China's Control of Overseas Ports," Council on Foreign Relations, last updated July 15, 2026. As of August 31, 2026: https://www.cfr.org/articles/china-overseas-ports

Londoño, Ernesto, "From a Space Station in Argentina, China Expands Its Reach in Latin America," *New York Times*, July 18, 2018.

López, Laura Delgado, "Orbital Dynamics: The Domestic and Foreign Policy Forces Shaping Latin American Engagement in Space," Center for Strategic and International Studies, July 2024.

Lorci, Enescan, *Shaping the Digital Order: China's Role in Technology Standards and the Implications for Taiwan*, Global Taiwan Institute, February 5, 2025.

Luong, Ngor, *Forging the 5G Future: Strategic Imperatives for the US and Its Allies*, Atlantic Council, September 4, 2024.

MacroPolo, "The Global AI Talent Tracker," version 3, last updated 2025. As of July 6, 2025: https://archivemacropolo.org/interactive/digital-projects/the-global-ai-talent-tracker/

Mahmood, Mou, Prangon Chowdhury, Rahbaar Yeassin, Mahmudul Hasan, Tanvir Ahmad, and Nahid-Ur-Rahman Chowdhury, "Impacts of Digitalization on Smart Grids, Renewable Energy, and Demand Response: An Updated Review of Current Applications," *Energy Conversion and Management: X*, Vol. 24, October 2024.

Marcos, Ferdinand R., Jr., Adopting the National Cybersecurity Plan 2023–2028, and Directing the Implementation Thereof, Executive Order No. 58, Office of the President of the Philippines, April 4, 2024.

Martin, Julien, *Analyzing the Economic Impact of Each Additional 100MhZ of Mid-Band Spectrum for Mobile*, National Economic Research Associates, January 23, 2025.

Massa, Isabella, *Export Finance Activities by the Chinese Government*, European Parliament, PE 433.862, September 2011.

McKinsey & Company, "What Is the Internet of Things (IoT)?" last updated May 28, 2024.

McWaters, Jesse, "5G and the Politics of Change: Could Nationalism Erode Innovation and Economic Growth?" Mastercard, March 9, 2021.

Miquee, Justine, and Xavier Buffon, "Research Update: Telekom Srbija a.d. Beograd and Senior Unsecured Bond Rated Preliminary 'BB-'; Outlook Stable," S&P Global, October 2024.

Morales, Neil Jerome, "Philippines Gets $5 Bln in Investment Pledges from German, US Companies," Reuters, March 13, 2024.

Morales, Neil Jerome, and Karen Lema, "China-Backed Telecom Firm Says Won't Spy on Philippines," Reuters, September 17, 2020.

Morris, Iain, "Huawei Overtakes Nokia Outside China as Open RAN 'Stabilizes,'" Light Reading, August 27, 2025.

Nadarajah, Hema, "China: A Global Power's Celestial Ambitions," Asia Pacific Foundation of Canada, May 9, 2024.

Nadin, Rebecca, and Elena Kiryakova, *China's Growing Space and Communications Presence in Africa*, ODI Global, December 2024.

NASA—*See* National Aeronautics and Space Administration.

National Aeronautics and Space Administration, "Global Reach—NASA International Cooperation," undated. As of September 12, 2026: https://www.nasa.gov/wp-content/uploads/2023/07/nac-day1-3-international-collaboration.pdf

National Security Division, "Team Telecom," webpage, U.S. Department of Justice, last updated September 20, 2023. As of March 19, 2026: https://www.justice.gov/nsd/team-telecom

NATO Cooperative Cyber Defence Centre of Excellence, "Costa Rica Ransomware Attack (2022)," webpage, last updated March 20, 2023. As of January 26, 2026: https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)

NEC Corporation, "NEC Signs Long-Term Charter Contract with Global Marine Systems Limited for Optical Submarine Cable-Laying Ship," press release, October 17, 2022.

Negussie, Feven, "The Discourse on Sino-African Relations," *Columbia Political Review*, February 18, 2019.

Nemko Digital, "AI Regulation in Costa Rica: Emerging Policy & Compliance," webpage, undated. As of January 25, 2026: https://digital.nemko.com/regulations/ai-regulation-costa-rica

Neuberger, Anne, "China Is Still Winning the Battle for 5G—and 6G: America Must Do More to Compete with Huawei," *Foreign Affairs*, May 1, 2025.

Next G Alliance, "National 6G Roadmap," webpage, undated. As of August 8, 2025: https://nextgalliance.org/working_group/national-6g-roadmap/

Nokia, "Nokia Selected by Globe Telecom to Modernize BNG Network to Improve Broadband Experience in the Philippines," press release, June 13, 2024.

Nokia, "Nokia and RACSA Deploy First 5G Network in Costa Rica," press release, October 10, 2024.

Nokia, "Nokia Completes Its Sale of Leading Submarine Networks Business, ASN (Alcatel Submarine Networks), to the French State," press release, January 3, 2025.

Nucci, Antonio, "AI Infrastructure Explained," blog post, Aisera, undated. As of September 1, 2026: https://web.archive.org/web/20250823213708/https://aisera.com/blog/ai-infrastructure/

Office of the Spokesperson, "Joint Statement on Enhancing Digital Economy Cooperation Between the United States of America and the Republic of Costa Rica," U.S. Department of State, April 11, 2024.

Open RAN Policy Coalition, "Open RAN Policy Coalition Launches to Advance Open and Interoperable Solutions to Expand the Global Advanced Wireless Supply Chain," press release, May 6, 2020.

Orellana, Francisca, "Chinese Cable Project Causes Rift Before Chile Presidential Transition," United Press International, March 3, 2026.

Oriishi, Anna, "What Has the U.S. Government Gained by Formalizing Team Telecom? Team Telecom and the FCC's Dual Security Approach," *Journal of Cybersecurity*, Vol. 11, No. 1, 2025.

"The Output Value of Our Country's Satellite Navigation Industry Reached 575.8 Billion Yuan" [我国卫星导航产业产值达5758亿元], Xinhua News [新华网], May 18, 2025.

Oxford Business Group, "The Entrance of a Third Major Telecoms Provider Set to Break the Duopoly in the Philippines," undated.

Pateña, Aerol John, "PLDT Partners with Huawei to Improve Wireless Services Delivery," Philippines News Agency, January 2, 2018.

Patterson, Rebecca, Susan Bryant, Ken Gleiman, and Mark Troutman, *Winning Without Fighting: Irregular Warfare and Strategic Competition in the 21st Century*, Cambria Press, 2024.

Philippine Department of Information and Communications Technology, *National Cyber Security Plan 2023–2028*, February 2024.

Philippine Department of Information and Communications Technology, *National Digital Connectivity Plan*, 2026.

Pilz, Konstantin F., Robi Rahman, James Sanders, and Lennart Heim, "Trends in AI Supercomputers," Epoch AI, April 23, 2025.

Pinaud, Oliver, "'Strategic' Submarine Telecom Cable Manufacturer ASN Nationalized by France," *Le Monde*, November 5, 2024.

Pollet, Mathieu, "China's Huawei Dominates Telco Jamboree Despite European Bans," *Politico Europe*, March 4, 2026.

Pollpeter, Kevin, "To Be More Precise: BeiDou, GPS, and the Emerging Competition in Satellite-Based PNT," China Aerospace Studies Institute, May 20, 2024.

President's National Security Telecommunications Advisory Committee, *Internet of Things (IoT) Advisory Board (IoTAB) Report*, National Institute of Standards and Technology, October 2024.

PwC, "Republic Act No. 11659," webpage, March 2022. As of March 19, 2026: https://www.pwc.com/ph/en/tax/issues/ra-11659-public-service-act.html

Račanović, Bojana, "Serbia's Artificial Intelligence Revolution," Chambers and Partners, August 13, 2023.

"Reading Between the Lines of the Dueling US and Chinese AI Action Plans," *New Atlanticist* blog, Atlantic Council, August 7, 2025. As of September 1, 2026: https://www.atlanticcouncil.org/blogs/new-atlanticist/reading-between-the-lines-of-the-dueling-us-and-chinese-ai-action-plans/

Reform Monitor, "European Commission Approves First Disbursement of Reform and Growth Facility Funds to Serbia," January 16, 2026.

Ridgeway, Beth, "NASA, USAID Launch SERVIR Central American Hub," National Aeronautics and Space Administration, December 6, 2024.

Rithmire, Meg, and Courtney Han, "The Clean Network and the Future of Global Technology Competition," Harvard Business School, April 2021.

Roulette, Joey, Eduardo Baptista, Sarah El Safty, and Joe Brock, "China Builds Space Alliances in Africa as Trump Cuts Foreign Aid," Reuters, February 11, 2025.

Roulette, Joey, Cassell Bryan-Low, and Tom Balmforth, "Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia," Reuters, July 25, 2025.

Runde, Daniel F., Austin Hardman, and Clara Bonin, *Responding to China's Growing Influence in Ports of the Global South*, Center for Strategic and International Studies, October 30, 2024.

Runde, Daniel, Erin Murphy, and Thomas Bryja, *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition*, Center for Strategic and International Studies, August 2024.

Saha, Shubhangi, "Software Defined Wireless Network: The Rise, the Evolution, the Future," *International Journal of Engineering Research & Technology*, Vol. 12, No. 6, June 2023.

Samuthira Pandi, V., Gadyam Somasundaram Uthayakumar, D. Aishwarya, S. Kathikeyan, S. Kamatchi, and N. Gopinath, "Revolutionizing Connectivity: Unleashing the Power of 5G Wireless Networks Enhanced by Artificial Intelligence for a Smarter Future," *Results in Engineering*, Vol. 22, June 2024.

Satariano, Adam, and Paul Mozur, "The Global A.I. Divide," *New York Times*, June 21, 2025.

Scanlon, Ruby, and Bill Drexel, *Countering the Digital Silk Road: Brazil*, Center for a New American Security, April 2025.

Schindler, Seth, Ilias Alami, Jessica DiCarlo, Nicholas Jepson, Steve Rolf, Mustafa Kemal Bayırbağ, Louis Cyuzuzo, Meredith DeBoom, Alireza F. Farahani, Imogen T. Liu, et al., "The Second Cold War: US-China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks," *Geopolitics*, Vol. 29, No. 4, 2024.

Serbian Ministry of Foreign Affairs, "China," webpage, undated. As of September 2, 2026: https://www.mfa.gov.rs/en/foreign-policy/bilateral-cooperation/china

Serbian Office for Information Technologies and eGovernment, "Government Data Centre in Kragujevac: The Most Modern and Efficient Data Storage Centre in the Region," webpage, undated. As of September 2, 2026: https://www.ite.gov.rs/tekst/en/34/government-data-centre-in-kragujevac.php

Shao, Ming Pu, "ITU and 3GPP," Networks at ITP, New York University, 2000.

Sokhean, Ben, "Cambodia, China Ink MoUs to Boost Innovation, AI, and Energy Cooperation," *Khmer Times*, April 21, 2025.

Spaargaren, Jerome, *The World's Leading 5G Patent Owners*, Patently, 2025.

Space-Track.org, "Query Builder," webpage, January 30, 2026. As of January 30, 2026: https://www.space-track.org/#queryBuilder

Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2025*, Stanford University, 2025.

State Council Information Office of the People's Republic of China [中华人民共和国国务院新闻办公室], "China's BeiDou Navigation Satellite System in the New Era," November 2022.

State Council of the People's Republic of China, *New Generation Artificial Intelligence Plan*, trans. by Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, Stanford Cyber Policy Center, August 1, 2017.

State Council of the People's Republic of China, "China Issues Guideline to Accelerate 'AI Plus' Integration Across Key Sectors," August 27, 2025. As of September 1, 2026: https://english.www.gov.cn/policies/latestreleases/202508/27/content_WS68ae7976c6d0868f4e8f51a0.html

Statista, "Artificial Intelligence—Worldwide," webpage, undated. As of July 6, 2025: https://www.statista.com/outlook/tmo/artificial-intelligence/worldwide

Statista, "Internet of Things—Worldwide," webpage, undated. As of August 8, 2025: https://www.statista.com/outlook/tmo/internet-of-things/worldwide

Statista, "Network Infrastructure," webpage, undated. As of August 8, 2025: https://www.statista.com/outlook/tmo/data-center/network-infrastructure/worldwide

Stokes, Mark, Gabriel Alvarado, Emily Weinstein, and Ian Easton, *China's Space and Counterspace Capabilities and Activities*, Project 2049 Institute and Pointe Bellow, March 30, 2020.

Strider and Special Competitive Studies Project, *China's AI Infrastructure Surge: How PRC Data Centers and AI Models Bridge Military Ambitions and Global Connections*, June 2025.

Submarine Cable Networks, "JUPITER," webpage, undated. As of March 19, 2026: https://www.submarinenetworks.com/en/systems/trans-pacific/jupiter

Submarine Cable Networks, "PLCN," webpage, undated. As of March 19, 2026: https://www.submarinenetworks.com/en/systems/trans-pacific/plcn

Submarine Cable Networks, "TAM-1," webpage, undated. As of January 25, 2026: https://www.submarinenetworks.com/en/systems/brazil-us/tam-1

Submarine Telecoms Forum, *Submarine Telecoms Industry Report 2025–2026*, October 30, 2025.

SubOptic, "How Many Submarine Cables Are There, Anyway?" May 22, 2025.

Tele Info Today, "Costa Rica Advances 5G Deployment with Tender Evaluation," undated.

TeleGeography, "Submarine Cable Frequently Asked Questions," webpage, undated. As of January 26, 2026: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

TeleGeography, "Submarine Cable Map," map, last updated January 15, 2026. As of January 26, 2026: https://www.submarinecablemap.com/submarine-cable/unitirreno

Thompson, Kieran, "Japan's 5G Ambitions with the Quad," Lowy Institute, July 18, 2024.

Thussu, Daya Kishan, "China's Deepening Digital Presence in the Global South," *Commonwealth Journal of International Affairs and Policy Studies*, Vol. 114, No. 4, 2025.

TicosLand, "Costa Rica Launches Pioneering 5G Testbed," June 24, 2025.

TicosLand, "ICE Advances Landmark 5G Tender as Bidding Closes," October 28, 2025.

Ting-Fang, Cheng, and Lauly Li, "Huawei Says It Is Training 300,000 Tech Students a Year amid U.S. Clampdown," *Nikkei Asia*, December 31, 2024.

Trivić, Slobodan, "The Belt and Road Initiative and Its Impact on Serbia: A Delicate Balance," in Andrea Bogoni and Brian F. G. Fabrègue, eds., *The Dragon at the Gates of Europe: Chinese Presence in the Balkans and Central-Eastern Europe*, Blue Europe, 2023.

Trotti, Christian, "A New Playbook for Irregular Warfare: How the United States Can Win Without Fighting," Irregular Warfare Initiative, January 21, 2025.

U.S. Department of Defense, *Department of Defense 5G Strategy Implementation Plan: Advancing 5G Technology & Applications Securing 5G Capabilities*, 2020.

U.S. Department of Energy, *Energy for Space: Department of Energy's Strategy to Advance American Space Leadership (FY 2021–FY 2031)*, January 2021.

U.S. Department of Homeland Security, "Securing the Internet of Things," webpage, last updated July 19, 2022. As of August 8, 2025: https://www.dhs.gov/securingtheIoT

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.

U.S. Department of State, "The Clean Network," webpage, undated. As of January 29, 2026: https://2017-2021.state.gov/the-clean-network/

U.S. Department of State, "Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids for Peaceful Purposes," webpage, last updated July 2026. As of September 1, 2026: https://www.state.gov/bureau-of-oceans-and-international-environmental-and-scientific-affairs/artemis-accords

U.S. Embassy in Senegal, "Senegal Joins the Artemis Accords," press release, July 25, 2025.

U.S. Government Accountability Office, *International Infrastructure Projects: China's Investments Significantly Outpace the U.S., and Experts Suggest Potential Improvements to the U.S. Approach*, September 2024.

U.S. Government Accountability Office, "China's Foreign Investments Significantly Outpace the United States. What Does That Mean?" *WatchBlog*, October 16, 2024. As of August 31, 2026: https://www.gao.gov/blog/chinas-foreign-investments-significantly-outpace-united-states.-what-does-mean

U.S. International Development Finance Corporation, "Supporting Resilient Telecommunications Infrastructure in the South Pacific," webpage, undated. As of September 1, 2026: https://web.archive.org/web/20250622092424/https://www.dfc.gov/investment-story/supporting-resilient-telecommunications-infrastructure-south-pacific

"US Looks to Invest in Foreign Energy Projects to Promote Exports, USTDA Says," Reuters, March 13, 2025.

U.S. Southern Command, "Partnership with Costa Rica to Establish Cyber Security," press release, August 22, 2023.

Varol, Cihan, *Enhancing and Adapting Security Risk Assessment Strategies on Critical Infrastructure Utilizing IoT Devices Using NIST Cybersecurity Framework 2.0*, Institute for Homeland Security, Sam Houston State University, 2024.

Vasovic, Aleksandar, "Serbia Chooses Links with China to Develop Economy, Telecoms Despite U.S. Warning Campaign," Reuters, August 13, 2020.

Vladisavljev, Stefan, "Why China Is Serbia's New Main Ally in the Kosovo Independence Dispute," *SAIS Review of International Affairs*, October 9, 2022.

Vlajkovic, Marija, and Andrija Saric, "Bridging the Gap Between Serbian Regulations and the GDPR: Serbia's Data Protection Strategy Unveiled," Schönherr Rechtsanwälte GmbH, September 27, 2023.

Wall Street Journal, "The Trillion-Dollar Battle for Fiber-Optic Supremacy," video, August 5, 2024. As of August 31, 2026: https://www.youtube.com/watch?v=7Koyi-MuEY8&t=3s

Wang, Austin Horng-En, and Kyle Siler-Evans, *U.S.-China Competition for Artificial Intelligence Markets: Analyzing Global Use Patterns of Large Language Models*, RAND Corporation, RR-A4355-1, 2026. As of August 25, 2026: https://www.rand.org/pubs/research_reports/RRA4355-1.html

Warner, Jason, and Toyosi Ajibade, "China's Smart Cities in Africa: Should the United States Be Concerned?" Center for Strategic and International Studies, November 18, 2024.

Wei, Lingling, Amrith Ramkumar, and Robbie Whelan, "America's Chip Restrictions Are Biting in China," *Wall Street Journal*, November 11, 2025.

Weinbaum, Cortney, Christopher G. Pernin, Camille Reeves, Libby Weaver, and Shanshan Mei, *Challenges When Collaborating with China on Space Research and Technology: Common Practices and Risks*, RAND Corporation, RR-A4104-2, 2026. As of September 1, 2026: https://www.rand.org/pubs/research_reports/RRA4104-2.html

Wenrong [文荣], "Hengtong Optoelectronics Completed the Acquisition of 81% of Huawei Marine's Shares, with an Expenditure of About 1.6 Billion Yuan" ["亨通光电完成收购华为海洋81%股权, 支出约16亿元"], Submarine Cable Networks, June 6, 2020.

White House, "Fact Sheet: Advancing Technology for Democracy," March 29, 2023.

White House, "White House Unveils America's AI Action Plan," July 23, 2025.

Williams, Laurence, Benjamin K. Sovacool, and Timothy J. Foxon, "The Energy Use Implications of 5G: Reviewing Whole Network Operational Energy, Embodied Energy, and Indirect Effects," *Renewable and Sustainable Energy Reviews*, Vol. 157, April 2022.

Wooden, Andrew, “Huawei Makes RAN Gains in Several Global Regions,” Telecoms.com, February 20, 2026.

World Bank Group, “More Than 20 Million Filipinos to Benefit from Improved Broadband Internet Connectivity,” press release, October 10, 2024.

Wu, Xiaodan, “The International Lunar Research Station: China’s New Era of Space Cooperation and Its New Role in the Space Legal Order,” *Space Policy*, Vol. 65, August 2023.

Xie, Yu, and Yongai Jin, “Global Attitudes Toward China: Trends and Correlates,” *Journal of Contemporary China*, Vol. 31, No. 133, 2022.

Xing, Liudong, “Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience,” *IEEE Internet of Things Journal*, Vol. 8, No. 1, January 2021.

Yadav, Poonam, Qi Li, and Richard Mortier, *IOT Network Behaviours and Dependencies*, Centre for Digital Built Britain, November 2018.

Yap, Chuin-Wei, “State Support Helped Fuel Huawei’s Global Rise,” *Wall Street Journal*, December 25, 2019.

Yee, William Yuen, “How the Philippines Screens Foreign Investments,” *Lawfare*, December 12, 2024.

Yeoh, Kenson, and Dingding Chen, “China-US Competition: Who Will Win the Digital Infrastructure Contest?” *The Diplomat*, December 21, 2022.

Yigzaw, Sina, “Ethiopia’s Diplomatic Horizon: Navigating Between Tradition and Pragmatism,” Horn Review, July 8, 2025.

Zeng, Tengchan, Omid Semiari, Walid Saad, and Mehdi Bennis, “Joint Communication and Control for Wireless Autonomous Vehicular Platoon Systems,” *IEEE Transactions on Communications*, Vol. 67, No. 11, November 2019.

Zhang, Mingze, Ming Hu, Jing Yang, Wutang Jing, Jin Guo, Hui Cai, and Yuntao Ma, “A Pilot Study on the Clinical Feasibility of 5G Remote Robot-Assisted Gastrectomy,” *World Journal of Surgical Oncology*, Vol. 23, April 2025.