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

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.

Research Report

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-A4569-1

About This Report

In this report, we examine what determines success in the U.S.-China competition for influence over global digital networks. We define the competition for digital networks, 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. Using the findings of that analysis, as well as a set of discussions with government officials and private-sector representatives, we conclude by identifying nine factors that govern outcomes in the competition and advancing corresponding recommendations for U.S. strategy.

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.

Summary

The commanding heights of the international system in the 21st century will exist in the digital realm: the digital networks and the broader ecosystem of hardware, software, artificial intelligence (AI) models, and standards that support them. Nations that shape the digital infrastructure connecting the international system will exercise disproportionate influence over the patterns of economic growth, the structure of security relationships, and the evolution of governance norms. Accordingly, competition for influence over digital networks—physical connectivity infrastructure, wireless networks, AI infrastructure, and space-based systems—now sits at the heart of the U.S.-China rivalry.

One leading vehicle for China's digital influence is the Digital Silk Road (DSR), a component of the Belt and Road Initiative estimated to have generated more than $79 billion in digital infrastructure projects since 2015.[1] The DSR is not a single document or strategy but an adaptive, evolving framework encompassing such elements as physical infrastructure (5G networks, fiber-optic cables, data centers); space-based navigation and communications; digital commerce, e-payments, and digital currency platforms; norms and standards campaigns; and smart city ecosystems in developing nations. Across the cases that we examined, China's most consistently observed competitive advantage is its ability to bundle these elements into integrated, subsidized, turnkey packages, which combine hardware, software, financing, training, and diplomatic engagement into offers that individual Western firms, bidding on their own, struggle to match.

In our analysis, we did not aim to provide a comprehensive accounting of digital networks in third countries or to assess the relative U.S. and Chinese standing in them. Instead, we sought to identify the *key determinants of competitive success* across major digital network categories. In this report, we provide an initial, qualitative assessment, drawn from four complementary lines of research, and its findings are best read as informed judgments about which considerations recur, not as measured effects. The answer, we found, varies significantly across different elements of digital infrastructure and, within any one element, across the countries making the choice.

Study Approach

To tackle the core research questions of this study, we first defined the scope of the subject, drawing from a robust body of literature on both network power in general and digital networks in particular. Because these networks comprise dozens of components and dependencies, we mined the literature for a series of selection criteria that would scope the analysis toward the most consequential areas of digital competition. The following four components scored highest across these technical, economic, and security metrics and therefore serve as the primary focus of our study: (1) physical

[1] Chan, *China's Digital Silk Road*, p. 7.

connectivity and infrastructure, (2) wireless and Internet of Things networks and standards, (3) AI infrastructure and data ecosystem, and (4) space systems. If the United States or China were to gain a truly dominant position across any one or several of these primary components, that outcome would have echo effects across many other areas of their rivalry. Although we did not conduct a net assessment of current U.S. and Chinese positions in this digital competition, we did review available data on their relative influence in each of those four areas (included as Appendix A in an annex to this report, available at www.rand.org/t/RRA4569-1). The resulting analysis is designed to be relevant to a broad national security audience and especially analysts, officials, and scholars who study the U.S.-China relationship.

We then moved to answer the core research question of the study: Which factors or variables are most essential for success in this contest? We brought four lines of analysis to bear on this question. First, we derived lessons from general research into the available public literature. Second, we undertook deeper research into the four priority areas listed above (these analyses appear in full in Appendix B in the annex). Third, we conducted discussions with U.S. and international government officials and private-sector leaders with experience in digital networks. Fourth, we built on available country and issue cases in the literature with five new ones, which examined digital network competition in Costa Rica, Nigeria, the Philippines, and Serbia and in the issue area of subsea cables. These cases appear in full in Appendix C in the annex; the findings are integrated throughout the report.

We selected these cases in a three-phase process. We first identified a larger number of countries in which meaningful digital network competition is underway. We then eliminated countries for which in-depth cases had already been accomplished, specifically those covered in a recent study by the Center for a New American Security.[2] Finally, we selected a set of countries for research that was designed to capture variation in geography, economic development, existing infrastructure, and geopolitical orientation. Each case study followed a common template: an account of Chinese and U.S. or allied engagement strategies, an assessment of outcomes against the three dimensions of success developed in Chapter 2, and a forward look; each closed with its own independent roster of factors that appeared to govern outcomes in that setting. The four domain assessments in Appendix B vary more in structure because the analytical problems they address differ substantially, but each was likewise read against the same conception of success and was required to produce the same kind of roster.

Accordingly, this report proceeds as follows: Chapter 1 explores the literature and articulates the rationale for examining these research questions. Within this important strategic context, Chapter 2 articulates our conceptualization of digital networks and the ways in which states vie for influence within them. Chapter 3 offers the core findings on the main research question of the study—the factors governing success in this competition. We brought these together by reviewing the major findings from each part and identifying common themes in the factors most consistently associated with outcomes. Chapter 3 describes that synthesis and its limits in more detail. Chapter 4 summarizes our findings from that research and suggests a way ahead for U.S. strategy for digital networks.

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

Factors Most Consistently Associated with Competitive Success

We identify five primary factors and four secondary factors that recurred most consistently across the domains, cases, and interviews we examined and that appear to shape which side gains advantage in digital network competitions. The distinction between the two groups reflects how often and how emphatically our sources nominated each factor. Chapter 3 outlines these in detail, and they are listed below.

Primary Factors

- *Cost and economic feasibility:* The basic price tag of fully installed digital systems and associated technologies for the recipient country.
- *Ecosystem advantages:* The ability of major digital powers to bundle various components of networks together, specifically including end-to-end solutions in such areas as 5G or AI.
- *Political, strategic, and business culture alignment:* A recipient country's alliance relationships, values, or business norms and standards.
- *Technology capabilities and quality:* The relative technological sophistication and effectiveness of the digital network components on offer.
- *The level of digital governance and institutions:* The degree to which the recipient country has strong or weak rules, laws, norms, and institutions governing the purchase and operation of digital network components.

Secondary Factors

- *Lock-in effects:* The tendency of early technology commitments to lock a recipient country into one technology ecosystem, standards regime, or supplier.
- *Regulatory and legal environments:* Specific regulations and laws that may allow or constrain some technology offerings.
- *On-the-ground presence:* U.S., Chinese, or other diplomats; private-sector representatives; researchers; or others establishing a long-term presence in the recipient country.
- *Elite co-optation:* The use of bribery, corruption, or, in some cases, legal means for generating elite support for specific digital offerings.

Key Findings and Strategic Implications

Having identified those nine factors, we drew on the research in our study to offer wider findings. Key insights include the following:

- Despite the significant progress China has made, *the United States and its close allies continue to enjoy many advantages*, including technological quality and geopolitical alignment, in several key areas of digital network rivalry.

- *Integrated packages of digital offerings provide essential competitive advantage*. China's leading competitive advantage is not any single technology but its ability to gather elements of a comprehensive offering into off-the-shelf technology ecosystems.
- *China's pattern of behavior reflects an effort to achieve ecosystem lock-in*. Across the cases we reviewed, Beijing has sought not merely to win market share or achieve discrete advantages but to create various forms of lock-in that make it difficult for customers to leave its ecosystem. This characterization reflects our assessment of the pattern of behavior rather than a stated Chinese objective. That pattern does not always hold; lock-in has proven far stronger in telecommunications and cable systems than in AI, in which open-weight models leave more room to switch.
- *Cost and financing are leading tools employed by Beijing for competitive advantage*. Across all four domains, the single most consistently cited factor in determining the adoption decisions of developing countries is not technology quality, security, or political alignment: It is financing. However, this does not hold universally. In the subsea cable competitions we examined, Chinese bids that were 20 to 30 percent below Western offers still lost, defeated by regulatory leverage and the threat of sanctions.
- *Speed matters*. China deploys rapidly and builds dependency over time; the United States often arrives late or not at all.
- *Most recipient countries have so far attempted to hedge rather than choose*. Outside a handful of advanced democracies, few third countries align exclusively with either ecosystem. They mix Chinese hardware with Western software, reserve Chinese systems for less sensitive applications, and court both sides to preserve leverage, a modularity that suggests that China may not need the wholesale vendor dominance that decided earlier technological competitions, only sufficient presence across enough layers.
- *Issues of narratives, reputation, and legitimacy play a significant, if secondary, role in shaping third-country choices*. The United States wants third parties to see this as a contest between democracy and autocracy, between reliable technology and insecure systems, and between sovereign autonomy and dependence on China's whims. China, meanwhile, deploys the narratives of South-South cooperation, noninterference, partnership of equals, and win-win development.
- *The "soft side" of the network competition, in standards setting and governance architecture, is a critical long-term factor*. This is true across all four domains we examined in depth.

Recommendations for U.S. Strategy

We found that the United States has lost ground in third-country digital markets, decisively in 5G and more gradually elsewhere, even as it and its allies retain strong positions and world-leading technologies across most other domains of the competition. We attribute that erosion, in substantial part, to the absence of a coherent, well-resourced, and integrated strategy. As we identified the factors that produce success in the competition, our research also revealed gaps in current U.S. policy and strategy. We propose five priorities for U.S. policymakers to help close those gaps:

1. *Develop a formal national strategy and coordinating office for the digital competition.* The United States needs a single empowered body (potentially in the White House Office of Science and Technology Policy) to align public and private efforts, thereby replacing the existing fragmented, agency-siloed approach, and to develop truly synergistic, coordinated solutions for third countries that address the challenge of China's ecosystem advantages.
2. *Address the financing gap.* The United States should create dedicated digital network financing programs through the U.S. International Development Finance Corporation and the Export-Import Bank of the United States, or a new purpose-built vehicle, designed to match China's concessional terms as closely as possible. Financing alone may not close the price gap because China's cost advantages also derive from scale, labor, and a protected home market, but it is the element most directly within U.S. control. Where single-country terms cannot match Chinese offers, pooled allied financing—as in the East Micronesia Cable System, jointly funded with Australia and Japan—has proven the more realistic instrument.
3. *Leverage allied synergies.* A coordinated U.S.–European Union–Japan approach that pools resources, shares technology offerings, and presents unified financing packages would substantially multiply U.S. competitive capacity.
4. *Build on-the-ground presence.* The United States should establish a new cadre of digital service officers embedded in key partner countries to support contract wins, train local workforces on Western platforms, and cultivate long-term relationships with ministries and firms.
5. *Renew norm-building coalitions.* The United States should build on the Clean Network initiative to establish and maintain a coalition of countries committed to open, interoperable, and secure digital standards, without demanding the exclusivity that most hedging states will refuse.

The United States and its allies confront a critical decade in the digital network competition, when a combination of key decisions by third parties and the emergence and market effect of novel technologies have the potential to push this competition in new directions. We conclude on a cautiously optimistic note: The United States retains genuine competitive advantages in innovation, technology quality, multilateral trust, and private-sector dynamism. Relatively modest but targeted improvements to the structure and resourcing of U.S. competitive strategy could make a significant difference, but time is of the essence.

Contents

About This Report iii
Summary iv
Tables x

CHAPTER 1 ..... **1**
The Growing Importance of Digital Networks 1
The Precedent: Network Effects in the Computer Revolution 3
China's Digital Silk Road 3
The Stakes 5
Who Is Winning? A Snapshot of the Contest for Digital Networks Today 8
The Study Approach 9

CHAPTER 2 ..... **11**
Conceptualizing Digital Networks 11
Components of Digital Networks 11
Priority Elements of Digital Networks 13
Defining Success 17
Initial Findings and Lessons: Sectoral Assessments 20

CHAPTER 3 ..... **24**
Identifying the Factors That Shape Success in the Digital Network Competition 24
Review of Case Study Findings 28
Primary Factors 33
Secondary or Context-Specific Factors 41
Overall Lessons: A Contest Led by the Match of Technology Offerings and Local Needs 45

CHAPTER 4 ..... **47**
Designing a U.S. Strategy for Success 47
Navigating the U.S.-China Competitive Landscape 48
Developing and Assessing a U.S. Strategy for Digital Network Competition 51

Abbreviations 58
References 59
About the Authors 64

Available at www.rand.org/t/RRA4569-1

ANNEX

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

Tables

Table 2.1. Categories and Elements of Success in the Digital Network Competition 18
Table 3.1. Conceptualizing the Factors 26
Table 3.2. Factors Associated with Success: Domain Case Studies 29
Table 3.3. Factors Associated with Success: Country and Functional Issue Cases 30
Table 3.4. Determinants of Outcomes in Digital Network Competition: Factors Most Consistently Observed Across the Evidence 32
Table 4.1. Categories and Elements of Success in the Digital Network Competition 52

Chapter 1

The Growing Importance of Digital Networks

Throughout history, great powers have competed by trying to dominate whatever material good or capability sits at the root of systemic advantage. For centuries, that meant territory: colonies that unlocked resources, revenue, and captive markets. Then came the scramble for trade routes, the arteries of global commerce. In the industrial era, nations competed for the resources and materials that drove modern economies. And more recently, the battleground shifted again: Scientific and technological knowledge became the ultimate prize, and the nations that could shape global innovation systems gained tremendous competitive advantage.

It now seems clear that the commanding heights of the international system in the 21st century will exist in the digital realm. Nations that shape the digital infrastructure connecting the international system will exercise disproportionate influence over the patterns of economic growth, the structure of security relationships, and the evolution of governance norms. The competition for digital networks may therefore ultimately prove decisive in determining which country achieves the ultimate advantage in the international order—not because digital dominance alone ensures victory but because the scope and depth of influence it provides extends across virtually every other domain of competition. Accordingly, competition for influence over digital networks, including physical connectivity infrastructure, wireless networks, artificial intelligence (AI) infrastructure, and space-based systems, now sits at the heart of the U.S.-China rivalry.

China has explicitly highlighted the importance of international digital competition. In its recent 15th Five Year Plan, the Chinese Communist Party calls for building "a global network of digital cooperation partnerships" in such areas as e-commerce, digital payments, smart cities, and data centers.[3] Former U.S. Department of War official Anne Neuberger has described the significance of this contest:[4] "Thus far, much of the digital infrastructure that has undergirded the modern world was invented, developed, and deployed in the United States," she notes. She further notes,

> If the United States were to lose this advantage for good, the consequences would be immense. A China that dominates global digital networks would be able to surveil them at will. It would also be positioned to lead in AI, training AI models on data

[3] Dorman, "Clear Course for Digital China."

[4] The Department of War is designated the Department of Defense under Public Law 81-216, National Security Act Amendments of 1949.

> that traverses Chinese companies' networks and controlling AI applications that rely on high-speed networking.[5]

A growing body of research examines various dimensions of digital network competition: defining the scope of these networks, documenting China's sustained pursuit of influence within them, and tracking competitive dynamics. Yet a critical question for U.S. strategy remains underexplored: *What factors will determine success in the contest for influence in third countries' digital architectures?* Which capabilities, investments, or general trends will be the decisive factors in the United States or China gaining a position of relative advantage?

We sought to address that gap with this study. Its purpose was not to provide a comprehensive accounting of digital networks in third countries or to assess the relative U.S. and Chinese standing in them. We did not examine the details of the technologies, from 5G communications to satellites to subsea or subterranean cables, that form the material basis of these networks. Instead, our goal was to conduct an initial assessment that identifies the key determinants of competitive success across major categories of digital networks. The resulting analysis was designed to be relevant to a broad national security audience and especially analysts, officials, and scholars who study the U.S.-China relationship.

Understanding these determinants will inform the design of strategic initiatives, guide investment priorities, and shape policy choices across multiple agencies. The answer, we found, varies significantly across different elements of digital infrastructure. The factors that determine success in submarine cable construction differ from those relevant to 5G network deployment. The overall picture is complex, depending on both crosscutting factors relevant across multiple domains and domain-specific variables unique to technological areas. Nonetheless, we identified nine overarching factors that seem to be the most important determinants of digital competitions in third countries across the domains we examined. Chapter 3 describes these in detail.

Beyond that set of factors, our research finds that, despite the significant progress China has made in telecommunications through Huawei networks and its growing position in third-country space and AI endeavors, the United States and its close allies continue to enjoy many advantages, including technological quality and geopolitical alignment, in several key areas of digital network rivalry. But China is working to erode those advantages through an integrated, partly state-directed campaign to seize advantage, built around its centerpiece initiative of the Digital Silk Road (DSR). Despite the centrality of digital networks to geopolitical competition, the United States still lacks a cohesive, well-resourced strategy to respond.[6] While China pursues digital influence through coordinated, sustained initiatives spanning infrastructure financing, standards promotion, and technology transfer, U.S. efforts remain fragmented across agencies, resource-constrained, and often more defensive than anticipatory. The United States, in short, is losing market share in third countries' digital infrastructure—as well as associated forms of engagement and influence that stem from direct participation in those networks—despite maintaining an edge in many areas of product quality, innovation, and reliability.

---

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

[6] Cilukuri and Scanlon, *Countering the Digital Silk Road*, p. 62.

The Precedent: Network Effects in the Computer Revolution

U.S. leadership of the computer revolution in the late 20th century produced network effects that offer instructive parallels for understanding contemporary digital competition. *Network effects* arise when a technology, standard, or platform gains value with each additional user, creating advantages that can entrench dominance and raise barriers to competitors. What distinguishes network effects from other forms of competitive advantage is their compounding nature: Early leadership generates benefits that make subsequent leadership easier to maintain, creating path dependencies that can persist for generations.

Such network advantages flowed to the United States during the computer revolution for several reasons. First, linguistic standardization in programming languages favored English-speaking developers and oriented global software communities toward Western technological norms.[7] Dominance in open-source development meant that competitors building digital systems, including potential adversaries, became dependent on tools and platforms developed within U.S.-led communities, even as those competitors seek technological independence.[8] Firms that lead in technology development play a dominant role in setting standards for the industry, which became a lasting source of power. The governance structure embedded in software licensing frameworks derived from U.S. legal principles, granting the United States disproportionate influence over the terms of digital systems far beyond its borders.[9]

During this era, U.S. advantage across these mutually reinforcing vectors emerged primarily through innovation and commercial success rather than deliberate statecraft. The dominant U.S. position in the computer revolution was a by-product of technological leadership rather than a strategic asset requiring active defense. That is no longer the case. China has identified the key sources of relative influence in the digital sphere and is developing an integrated strategy to reverse those U.S. advantages. Its effort centers on the major global initiative known as the DSR.

China's Digital Silk Road

China has recognized the importance of mastering the networked digital future, and beginning in 2015 has promoted a comprehensive effort—though relatively unformed at first and still undefined in terms of its scope—to attract other countries to its digital network offerings. This is the DSR, a component of the larger Belt and Road Initiative (BRI).[10] The DSR has no foundational document or strategy laying out its elements. It appears to be an adaptive concept that has grown over time to encompass various initiatives and investments. The precise objectives of the initiative are not clear, apart from gradually winning more engagement from other countries.[11] But the DSR is a major

[7] Alejandro, "Why English-Based Programming Languages?"

[8] Pannier, *Software Power*.

[9] One example relates to legal frameworks governing cloud access. See Schwartz, "Legal Access to the Global Cloud."

[10] Shen, "Building a Digital Silk Road?"

[11] Oreglia, Ren, and Liao, "The Puzzle of the Digital Silk Road," p. 1.

element of China's global statecraft: As of 2021, one estimate suggested that China had spent more than $79 billion on projects dealing with digital networks and infrastructure.[12]

Observers have identified several major elements of the DSR based on Chinese practice.[13] These include the following:

- *Physical infrastructure*. China is working to become the dominant provider of the physical foundations of digital networks. One working paper noted, "Through the Digital Silk Road, China seeks to become a world leader in providing physical infrastructure in the digital sphere, which includes next-generation cellular networks, or 5G technology; fiberoptic cables used to transmit data over the Internet; and data centers used to store data."[14] China has undertaken digital infrastructure projects in dozens of countries.
- *Space-based navigation and communications satellites*. China is also investing heavily in satellites, ground control stations, and other elements of space communications and navigation options for countries to join. It has promoted the BeiDou system, for example, as an alternative to the Global Positioning System (GPS).[15]
- *Digital commerce*. China has sought to use the DSR initiative to expand the reach of its e-commerce, digital payment, and digital currency platforms, which are widely deployed in China but only beginning to achieve real penetration in third countries. In the process, China is seeking digital free trade zones with multiple countries and aiming to develop a digital yuan with international adoption.[16]
- *Norms and standards*. Alongside its DSR initiative, China has pursued a broad strategic agenda aimed at enabling China to shape technical standards of global products and services in the digital space.[17] Beijing fully appreciates the critical role of standards in setting the context for future digital network development and is working to ensure that it has a strong voice in that process; indeed, in recent years, DSR engagements have increasingly prioritized *soft connectivity*, or agreements on standards, norms, and software relationships.[18] In an overlapping and parallel effort, China is seeking, in part, to attract others to its concepts of digital sovereignty, sometimes by offering surveillance technology.

[12] Chan, *China's Digital Silk Road*, p. 7.

[13] For a definition of the DSR's elements, see Chan, *China's Digital Silk Road*, pp. 15–29.

[14] Cheney, "China's Digital Silk Road," p. 4.

[15] Cheney, "China's Digital Silk Road," p. 6.

[16] Chan, *China's Digital Silk Road*, pp. 66–90.

[17] Dekker, Okano-Heijmans, and Zhang, *Unpacking China's Digital Silk Road*, p. 2; He, "The Digital Silk Road and China's Influence on Standard Setting."

[18] Thibaut, Puyosa, and Komaitis, "AI Cooperation Under the Shadow of China's Digital Silk Road"; Goujon et al., *Fighting Hubris in AI Strategy*, pp. 33–34.

- *Smart cities*. A major offering in China's DSR toolbox is integrated sets of technologies that allow developing nations to realize ambitions for smart cities.[19] Many developing countries have displayed an interest in these ecosystems.

At least in theory, the concept of the DSR represents a holistic combination of all these aspects, among others, to create synergies that generate competitive advantage.[20] The idea is to assemble packages of technology infrastructure, trade agreements, finance guarantees, and informational offerings that create high value for third countries. DSR programs with third countries often involve such integrated packages of technologies and are linked to China's broader ecosystem of national tools of statecraft, from development finance to security relationships to classic diplomacy.

The DSR has already allowed China to achieve major, growing presence in key elements of global digital networks. With China now prioritizing what it terms *high-quality* growth—that is, national growth and development led by high-technology industries—it is even more tightly connecting its future global influence to high-tech partnerships, many of them built around digital networks.

The Stakes

The contest for leadership in global digital networks could have a significant effect on the larger U.S.-China competition. If the United States or China were to gain a truly dominant position across the main components of such networks, that outcome would have echo effects across many other areas of the rivalry. The specific causal ties between an outside role in developing and operating digital networks and degrees of influence are beyond the scope of this report. But there are strong reasons to believe that, if one nation becomes the leading provider of network components (much as the United States was the world's leading provider of computer software), significant influence and power would follow.

One reason to believe this is that modern societies are becoming thoroughly dependent on digital networks and the ecosystems that support them. The rise of Internet of Things (IoT) smart devices and systems is accelerating this transition. By 2025, there were more than 21 billion connected devices globally,[21] and many U.S. households have multiple smart devices, from thermostats to refrigerators to watches. IoT is no longer a niche phenomenon but is embedded in the texture of everyday life for advanced economies. The spread of such devices has created strategic vulnerabilities: The U.S. Government Accountability Office reported that U.S. critical infrastructure sectors rely heavily on IoT devices, which often have poor cybersecurity protocols.[22]

As advanced economies become more deeply dependent on smart, connected products in homes, hospitals, factories, energy grids, and transportation networks, the digital networks that underpin those products become strategic assets of the first order. A nation that controls the architecture,

---

[19] Ekman, *China's Smart Cities*; Warner and Ajibade, "China's Smart Cities in Africa"; Artha et al., *China's Smart Cities Development*.

[20] Dekker, Okano-Heijmans, and Zhang, *Unpacking China's Digital Silk Road*, p. 3.

[21] Sinha, "State of IoT 2025."

[22] U.S. Government Accountability Office, *Critical Infrastructure*.

standards, and security of those networks gains not merely commercial advantage but the potential ability to surveil, disrupt, or hold at risk the entire productive and social fabric of a digitally dependent adversary. Such leaders in digital networks might not routinely exercise such power for fear of alienating potential customers. But they could engage in covert information-gathering on a regular basis and will have a sword of leverage hanging over their digital partners. In the event of a crisis or conflict or even a severe geopolitical disagreement, the providers of digital services could (as China has recently done with rare earths) employ that leverage for geopolitical ends. There are numerous examples of such potential leverage and information acquisition, from the use of fiber-optic cables for intelligence-gathering to sudden embargoes on technology products critical to digital networks.[23]

Nations that control the architecture of 5G, AI platforms, and data transmission corridors will also put themselves in a position to capture the economic value generated by the industries built on them, from advanced manufacturing and autonomous systems to financial services and precision agriculture. So many elements of digital economies are linked together in mutually supporting ecosystems such that gaining a leading foothold in several areas of that economy can quickly spread to advantages in others. One analysis of the U.S.-China competition recently noted that "[t]rade and procurement decisions in sectors like information and communications technology" and some other sectors, such as energy and port logistics, "are not ordinary commercial transactions. They are investments into entire technological ecosystems where significant barriers to entry and exit mean that early supplier choices can lock in technological standards, maintenance chains, and market relationships for decades."[24]

Predominant positions in national digital networks also integrate outside powers into the recipient countries' societies, economies, and politics far more than most typical investments. They place the outside vendors at the very fulcrum of national life in ways that automobile factories or consulting firm engagements do not. Providers of telecommunications and data transmission infrastructure could gain access to data and information, both as a general commodity and about specific individuals and organizations. Cloud computing firms host critical information on their servers. Companies offering AI models can theoretically access all the queries made on their systems. And across all these and other components of digital networks, providers of key ecosystem components become essential to the continued economic, social, and political health of the countries in which they provide services.

Taking a leadership position in these networks has very practical implications in at least two ways: data and manufacturing capacity. Countries that dominate such networks will gain access to massive troves of data for training AI models, conducting espionage, and other purposes. Leaders in the field can dominate the manufacturing of hardware components of these ecosystems, from phones to cables to data centers to satellites. That manufacturing capacity, in turn, supercharges technological innovation, creating a positive feedback loop that countries that are shut out of these networks will not be able to match.

For national security more specifically, acquiring a position in a third country's digital ecosystem creates opportunities to observe, intercept, or manipulate data flows. Chinese-built infrastructure—such as Huawei base stations, subsea cable landing stations, satellites, and satellite ground systems—

[23] Gebhart, "Revitalizing the Export-Import Bank for Great Power Competition," p. 172.

[24] Gebhart, "Revitalizing the Export-Import Bank for Great Power Competition," p. 171.

offers the potential for espionage, data exfiltration, and backdoor access to sensitive communications. Because modern warfighting is inseparable from digital networks, major powers that are deeply integrated into other countries' digital networks could potentially impose real constraints on their partners' ability to join any contingency. Deep digital access could also empower cyber operations: If China shapes the digital networks of U.S. partners or allies, it might be able to use the access granted to public and private networks to discover exploits in U.S. government systems.

Whoever leads in deploying next-generation networks will also gain outsize influence over the technical standards, governance norms, and regulatory frameworks that set the conditions for global digital economies. Influence over standards can operate through several distinct mechanisms, including participation in standards-development organizations, such as the International Telecommunication Union (ITU) and 3rd Generation Partnership Project (3GPP), in which we assess China's influence to be growing in an effort to entrench favored norms around surveillance-friendly architectures and data localization, technical contributions and ownership of standards-essential patents, adoption in commercial products, and broader governance principles, such as competing visions of digital sovereignty. We recognize that these mechanisms could have different outcomes, but that level of analysis is outside the scope of this report.

There is substantial evidence—from China's actions, as well as public strategy documents, such as China's AI Plus initiative and its 15th Five Year Plan—that senior officials in Beijing see these potential sources of power and aim to use AI leadership, along with other elements of digital network power, for such purposes. One recent Rhodium Group report surveyed many sources of evidence on Chinese intentions and concluded,

> China's drive to lead the global debate on spectrum management reflects its broader ambition to shape the foundational infrastructure of the digital economy. By influencing how key frequency bands are allocated and used—particularly for 5G, 6G, and industrial applications—China aims to position its technologies, standards, and vendors as default choices in emerging markets. This not only secures long-term commercial advantages for Chinese firms but also strengthens Beijing's voice in setting the technical and governance norms that will underpin the next generation of global connectivity.[25]

For all these reasons, there is much at stake in the contest for leadership in global digital networks. This is far more than a bilateral contest for profits or market share; it is a competition to dominate the central technological ecosystem of the 21st century. This is not to say that a role in building, maintaining, and updating digital networks automatically confers a specific degree of power or influence. Those outcomes will differ dramatically from one sector to another and from one country to another. Countries could seek to insulate themselves from control or dependency in various ways. Nonetheless, for the reasons outlined above, there is strong reason to believe that gaining a leading role in digital network construction and operation could well convey important competitive benefits.

[25] Goujon et al., *Fighting Hubris in AI Strategy*, pp. 33–34.

Who Is Winning? A Snapshot of the Contest for Digital Networks Today

As noted above, our research did not focus primarily on a net assessment to determine who is winning the competition for digital networks. However, to understand the context and provide potential insight for our main goal—identifying factors critical to success—we did undertake a relatively brief review of the evidence on that score, surveying the current state of the competition across the four priority areas of the competition that we describe in Chapter 2: physical connectivity and infrastructure, wireless and IoT networks and standards, AI infrastructure and data ecosystem, and space systems. Appendix A offers these data.

The most important message of these data is that, despite substantial attention to Huawei's global lead in 5G networks and China's generally rising position in many areas of technology, across elements of all four areas, the United States and its allies continue to hold significant competitive advantages and strong sectoral positions. In 5G, the story is clearly one of Chinese leadership: Despite significant Western pushback—including Huawei being added to the U.S. Commerce Department's Entity List and bans on its technology across Five Eyes nations and much of Europe—Huawei remains the world's largest 5G provider. It is in use or likely to be adopted in more than 100 countries and has driven major U.S. players, such as Cisco and Motorola, entirely out of the industry. Yet even here, in the global marketplace outside China, Ericsson and Nokia retain reasonably significant positions in the radio access network (RAN) market: Ericsson is the top RAN vendor outside China overall, with Nokia third after Huawei. If post-5G technologies emerge in which U.S. and allied firms become competitive, the landscape for advantage would dramatically shift.[26]

In cloud computing and data centers (a core element of AI infrastructure and data ecosystems), the picture is considerably more favorable for the United States.[27] U.S. firms account for more than 46 percent of publicly listed data centers globally, compared with around 4 percent for China. Microsoft, Amazon Web Services, and Google together control nearly 62 percent of all availability zones among the nine leading cloud providers, compared with roughly 36 percent for their three Chinese counterparts combined. Similarly, in undersea cables, Western and Japanese firms dominate decisively: France's Alcatel Submarine Networks, the United States' SubCom, and Japan's Nippon Electric Company together account for nearly 90 percent of total deployed cable length, whereas China's HMN Tech has installed only about 5 percent despite representing around 10 percent of cable systems. Projections for new near-term cable installations reflect a continuation of this pattern.

In space systems, the picture is somewhat more mixed but still reflects significant U.S. advantages. U.S. firms lead in scale and maturity, especially in Starlink's dominance in low earth orbit broadband. China's BeiDou Navigation Satellite System has grown rapidly, however, and now serves more than 2 billion users. It is also a newer system that offers capabilities that, in some respects, exceed GPS, including built-in messaging and intersatellite links. China also has ambitious plans to deploy satellite

[26] See Morris, "Huawei Overtakes Nokia Outside China as Open RAN 'Stabilizes'"; Wooden, "Huawei Makes RAN Gains in Several Global Regions"; and the analysis in Appendix A.

[27] The figures in this paragraph are derived from Cloudscene data; more detailed citations and additional figures are available in Appendix A.

mega-constellations. So far, they remain largely aspirational, with actual deployment lagging well behind announced targets, but China has clearly signaled an intention to become the dominant provider of space-based digital services.[28]

In space and other areas of the competition—notably the race to become the leading provider of AI ecosystems for developing nations—the ultimate outcomes remain very much in doubt. The United States and its allies retain meaningful advantages across most of these domains, but China is investing heavily in various sources of advantage. In the AI competition, for example, U.S. frontier models are leading the development of AI capability, but Chinese open models are cheaper, more energy efficient, and highly attractive to users in developing countries.[29] China has demonstrated in 5G that subsidized, integrated offerings can achieve significant global penetration even in the face of coordinated Western opposition.

Our brief survey of the current standing in the competition drove home two broad points. First, across the primary areas of the contest, outcomes remain in flux, and the United States and its allies enjoy significant advantages. But second, evidence from current practice suggests that China is pursuing much more coordinated, integrated strategies across many variables governing success.[30] This context redoubles the importance of discovering the sources of competitive advantage in this contest and developing strategic responses to shape its future trajectory.

We need to stress the limits of the resulting findings. We have gathered detailed data and case study information on various aspects of the issue and sought out the best available expert opinion on China's intentions, likely trends in this field, and related issues. Nonetheless, several key aspects of digital network competition, from the true intentions of China's senior leaders to the evolution of key technology areas to the conduct of U.S. foreign policy, are characterized by significant uncertainty. Our findings represent the best judgment we could reach given the information that we could access.

The Study Approach

To tackle the core research questions of this study, we first defined the scope of the subject, outlining the main material and normative components of digital networks. Chapter 2 summarizes this work. We then sought to narrow the focus to a subset of the most-critical elements, developing criteria to assess significance and identifying four elements for deeper analysis, also described in Chapter 2. Analytically, this work was informed by research into all available open-source treatments of digital networks, cited throughout the report. Although generating a net assessment of the United States' and China's relative positions in digital networks was not the primary purpose of the research, we did conduct a broad survey of their standing as of this writing in mid-2026. Appendix A offers this analysis.

We then sought to answer the core research question of the study: Which factors or variables are most essential for success in this contest? We brought four lines of analysis to bear on this question.

---

[28] O'Callaghan, "China Has Applied to Launch 200,000 Satellites, but What Are They For?"

[29] Meinhardt et al., "Beyond DeepSeek."

[30] One recent discussion of overall Chinese techno-industrial strategies that speaks to areas beyond digital networks is McMorrow et al., "China Shock 2.0."

First, we derived lessons from general research into the available public literature, looking especially for factors that seemed to be decisive in shaping decisions by individual countries on digital network participation. We reviewed primarily think-tank reports and private-sector analyses, with some use of available scholarly resources and U.S. government publications. Because of the relatively limited direct literature on this topic, we reviewed all the direct sources we could find. Second, we undertook deeper research into the four priority areas identified in Chapter 2, specifically trying to determine what factors were critical to competitive position in each. These analyses appear in full in Appendix B; their findings and lessons are integrated throughout the report.

Third, we conducted discussions with roughly a dozen U.S. and international government officials and private-sector leaders with experience in digital networks to elicit their perspectives on the factors that have determined key choices. These were roughly divided between former U.S. government officials and private-sector officials. Because of the different focus areas of different components of digital networks, we did not follow a single formal interview protocol. The interviews were also done on a background basis to inform the research but are not cited directly. These interviews reflected a selection of perspectives, some from U.S. and private-sector officials with global responsibilities and awareness and a smaller number of officials with sector- or country-specific knowledge. Their purpose was to provide a sampling of on-the-ground perspectives; they did not represent a comprehensive survey of key sectors or regions.

Fourth, we built on available country and issue cases in the literature with five new ones, which examined digital network competition in Costa Rica, Nigeria, the Philippines, and Serbia and in the issue area of subsea cables. These cases appear in full in Appendix C; their findings are integrated throughout the report. We selected these cases in a three-phase process: We first identified a larger number of countries in which digital network competition is underway in significant ways. We then eliminated countries for which in-depth cases had already been accomplished, specifically those discussed in a recent study by the Center for a New American Security (CNAS).[31] Finally, we selected a set of countries for research that was designed to capture variation in geography, economic development, existing infrastructure, and geopolitical orientation.

Chapter 3 offers the core findings on the main research question of the study: the factors governing success in this competition. Those findings are derived from all four lines of analysis summarized above. We brought these together by reviewing the major findings from each part and identifying common themes in terms of the factors that emerged as determining outcomes. Chapter 4 summarizes our findings from that research and suggests a way ahead for U.S. strategy for digital networks. It outlines components of a needed strategy for the United States to avoid being left behind in this most essential of contests.

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

Chapter 2

Conceptualizing Digital Networks

Our ultimate purpose in this study was to discover the factors that determine success in the competition for position and influence in digital networks. To set the context for that analytical goal, we first had to define digital networks and then select critical areas of the competition around them for deeper analysis. This chapter summarizes the analysis we undertook to make those initial assessments. We reviewed a broad literature on such networks to understand the dozens of component areas that compose them, and we developed criteria to narrow them down to a set of four highly significant components for further analysis; we define and briefly discuss each.

To understand the sources of success in the competition, we also had to understand what success looks like. Using the research on digital networks and the literature on system and network dynamics, we developed a conceptualization of success for the competition built around three interrelated elements. This chapter also lays out that analysis. Finally, we outline several interim findings—broad themes that can help guide U.S. strategy for this competition—that emerged from this phase of the research. This analysis sets the stage for the primary focus of our research: identifying the factors that will determine who succeeds in this contest.

Components of Digital Networks

Digital infrastructure is not a single competitive domain but rather a stack of nested layers—technical, operational, and governance—that interact with each other in ways that compound in complexity. There are many ways to conceptualize the elements of digital networks: hardware and software elements, different technology sectors, functional layers, and governance frameworks, among others. Some of the major hardware and software elements of digital networks include the following:[32]

- global connectivity assets, including submarine fiber-optic cables, wireless infrastructure, and satellite constellations and user terminals
- compute and storage capabilities, including data centers, semiconductor supply chains, edge computing nodes, and micro-data centers

[32] We derived these categories from a general review of the literature on digital networks and then shared drafts with several industry and government interviewees for comment. Many of the sources we relied on for these findings are cited in the sector assessments in Appendix A. More-general sources on the competition include the following: Brackup, Harting, and Gonzales, *Digital Infrastructure and Digital Presence*; Shen, "Building a Digital Silk Road?"; Schindler et al., "The Second Cold War"; Cheney, "China's Digital Silk Road"; Klaus and Curtis, "The New Corridor Competition Between Washington and Beijing"; Yeoh and Chen, "China-US Competition"; Kumar, "China's Digital Expansionism in Africa and the US Counter-Strategies"; Shi-Kupfer and Ohlberg, *China's Digital Rise*; Liu, "Coalition Building and Sino–US Competition in the Digital Era"; Dong and Dan, "Digital Globalization and China-US Strategic Competition"; Reddy and Soni, *Is There Space for a Digital Non-Aligned Movement?*

- network management and control elements, such as software-defined networking controllers, cybersecurity architecture, and identity and trust services
- AI model development systems, including datasets, training clusters, and specialized hardware (e.g., graphics processing units [GPUs], tensor processing units)
- application and transaction ecosystems, including e-commerce platforms, ubiquitous software applications, and social media platforms
- standards and governance mechanisms, including technical standards and national and cross-border regulatory frameworks.

Many other technological, industrial, and governance capabilities support those components of digital networks. Manufacturing capacity for specific systems, from satellites to high-end computing racks in data centers, is essential for countries seeking the ability to offer end-to-end digital ecosystems to customers. State support for technology development and manufacturing competitiveness can make a critical difference in competitive standing in some domains. Financial and payment systems integrate with e-commerce platforms. From this broad variety of elements, we sought to identify a more limited number of domains for deeper analysis.

Digital networks encompass a vast array of technologies, platforms, and infrastructure elements, and not all components carry equal strategic weight. Some generate cascading dependencies and durable competitive advantages, while others remain contestable or marginal to broader geopolitical outcomes. Systematic assessment requires identifying which specific attributes render individual network elements as sources of sustained leverage in great-power competition. Among these many areas, we propose the following as the most critical for U.S.-China competition, based on an initial set of criteria.

Elements of digital infrastructures will have the highest competitive leverage when they demonstrate the following:[33]

- *Network effects:* Cases in which each additional user enhances value for all participants confer competitive leverage. Leverage potential is especially pronounced when usage scaling is combined with reinforcing mechanisms, such as data aggregation benefits, switching costs, or user lock-in. Early dominance in such environments proves difficult to dislodge, making initial market positioning strategically consequential.
- *Lock-in dynamics:* Components with low initial barriers to entry but high switching costs and ecosystem dependencies possess highly competitive leverage. Substantial obstacles to migration for users, whether individual consumers or enterprises, create durable market positions.
- *Chokepoint control:* Control of nodes that constitute critical bottlenecks in flows of data, commerce, or communication confers disproportionate influence and creates dependencies vulnerable to strategic leverage.

[33] These criteria are derived from a review of two broad bodies of literature. One deals with the sources of network power generally. Notably, sources of analysis in this domain include Grewal, *Network Power*; Jervis, *System Effects*; Meadows, *Leverage Points*. The other body of literature is the material on digital network competition cited throughout the report.

- *High barriers to entry:* Elements that require substantial upfront investment, specialized expertise, or exclusive access to the supply chain can effectively foreclose competition. Such barriers create durable advantages for incumbent players and limit the strategic options available to late entrants.
- *Pace of innovation:* Leverage is built in areas in which technological change is especially rapid and early leads can compound over time. Leverage is particularly significant where elements fuel virtuous cycles of innovation, talent development, capital attraction, and next-generation capabilities. In such dynamic environments, initial advantages tend to reinforce themselves, creating widening competitive gaps.
- *Standardization power:* For components for which the ability to establish or shape standards influences the broader technology adoption, control over standardization processes can lock in market positions and determine ecosystem trajectories.
- *Potential for market dominance:* For segments in which single players or small numbers of firms can dominate the market, concentrated market power enables disproportionate influence over dependent users, standards, and downstream innovation.
- *National security value:* Infrastructure and technologies with dual-use military applications or capabilities aligned with intelligence collection or information manipulation activities possess inherent strategic leverage beyond their commercial or civilian functions.

These criteria provide an analytical framework for assessing competitive significance rather than a mechanical scoring system. In practice, few elements will score highly across all dimensions, and comprehensive dominance is not necessary to confer strategic advantage. The goal is instead to identify patterns of leverage that emerge from the interplay of these factors. The relative weight of each factor will vary depending on the specific technology, market conditions, and geopolitical circumstances under examination. Moreover, the criteria themselves are not entirely independent: Network effects often reinforce lock-in dynamics, for instance, while high barriers to entry frequently correlate with the potential for market dominance.

In Chapter 3, we nominate factors that are critical in determining outcomes in the digital competition. That list is derived from case and interview evidence rather than this selection screen. These criteria helped us discover the most-significant domains of the competition; Chapter 3 outlines a separate list of the factors that determine success.

Priority Elements of Digital Networks

Using those eight criteria, we identified four components of digital networks for further analysis: physical connectivity and infrastructure, wireless and IoT connectivity and standards, AI infrastructure and data systems, and space systems. They represent combinations of the hardware and software building blocks of digital networks into broader issue areas. Each of these domains generates outsize strategic consequences through reinforcing mechanisms that make early advantages in third countries difficult to displace. Each scored highly across most of the criteria noted above.[34]

[34] We weighed candidates at the level of the six hardware and software categories set out above—connectivity assets, compute and storage, network management and control, AI development systems, application and transaction ecosystems,

We briefly summarize the four areas below. A more detailed analysis of these four priority areas and the factors influencing competitive success in each is provided in Appendix B, including the sources used to draw these conclusions. After summarizing each, we then conclude the chapter with key lessons and insights drawn from these domain analyses.

Physical Connectivity and Infrastructure

Traditional physical infrastructure merits attention in digital networks competition despite—or perhaps because of—its seeming distance from cutting-edge software innovations. Undersea and terrestrial fiber-optic cables transmit 95 to 99 percent of intercontinental data, creating natural chokepoints in global communications with high barriers to entry and concentrated market structures. Energy infrastructure similarly functions as a critical enabler, powering the computational demands of AI development and 5G networks while itself benefiting from digital augmentation. Transportation systems, although they contribute more indirectly to digital capabilities, remain essential conduits for trade and capital flows that sustain technology markets. In this domain, the United States retains first-mover benefits through decades of infrastructure statecraft. China, however, has strategically leveraged its second-mover position through the BRI, rapidly deploying hybrid digital-physical systems in developing countries despite persistent concerns about quality, dependency creation, and predatory practices.

These infrastructure elements embody two distinct theories of competitive success, each activating different mechanisms of leverage. As an enabler of digital innovation, physical infrastructure generates influence through relational pathways: supplying energy and data inputs that accelerate partner nations' development and pace of innovation, building local capacity and technical skills, and cultivating trust and legitimacy. Success through these pathways depends on cost competition, reliable provision of critical inputs, partnership models that empower rather than create dependencies, and sustained political commitment. As transmitters of strategic commodities, such as data and energy, however, the same infrastructure represents tangible chokepoints subject to traditional power dynamics: points of control that can be disrupted to manipulate signals or denied entirely to exclude rivals and ensure resilience against containment. The dual nature of physical infrastructure, simultaneously enabling digital innovation and controlling critical flows, makes it a priority element in which early positioning and market dominance can compound into enduring strategic advantage.

It is important to note that the remaining three elements of digital networks discussed below also include their own physical components. Because these physical components represent specialized components unique to their respective wireless and IoT, AI, and space stacks, however, they exhibit different dynamics from those of the more traditional physical infrastructure considered above.

---

and standards and governance—rather than against the much longer roster of specific technologies nested within each because no settled taxonomy of that finer grain yet exists in the literature, and reducing qualitative judgments of this kind to a numerical score would claim more precision than the analysis can support. Standards and governance did not emerge as a fifth domain of comparable weight to the other four; standardization power instead functions as an attribute that attaches to and shapes each of them, which is why we treat it as a crosscutting consideration, examine its clearest single-domain expression (3GPP governance) within wireless and IoT below, and discuss its bearing on the other three domains separately in Chapters 1 and 3 and in Appendix B.

Wireless and Internet of Things Networks and Standards

Wireless networks and IoT ecosystems bridge the physical and digital worlds through sensors, actuators, and wireless systems that transmit data to cloud-based systems, making them priority infrastructure in which multiple leverage mechanisms reinforce one another to create compounding competitive advantages. Encompassing cellular base stations, satellite arrays, sensor-embedded devices, and cloud platforms managing spectrum and data routing, these critical inputs generate dependencies with profound economic and security implications, though of several kinds. At its most fundamental level, early market positioning in 5G infrastructure can lock countries into vendor ecosystems for upgrades, maintenance, and protocol compatibility, a contractual and operational dependency legible in terms of the agreements themselves. Simultaneously, documented participation in standardization bodies, such as 3GPP, shapes which IoT devices can connect and which technical standards govern future deployments.

The competitive outcome in wireless and IoT networks, however, depends less on great-power capabilities than on how recipient countries navigate adoption decisions. Our research suggests that four interconnected factors, rather than bilateral competition metrics, tend to shape these outcomes. Economic feasibility establishes baseline possibilities, although geopolitical considerations can override economic calculations. Similarly, narrative resonance enables leaders to justify choices as expressions of national identity, with China's "partnership of equals" messaging and the United States' "democratic technology" arguments resonating differently depending on recipient countries' core concerns. A nation's structural capacity ultimately determines whether it retains flexibility or becomes locked into multigenerational vendor relationships, a process that requires coordinated institutions, regulatory frameworks, and technical expertise, which many countries lack. The 5G to 6G transition is Washington's opportunity to reverse China's dominance in wireless and IoT infrastructure, but success requires preemptive coordination of development finance and alliance structures to address all four factors simultaneously.

AI Infrastructure and Data Ecosystem

Much like wireless networks and IoT, technological leadership in AI model development does not automatically translate into global market dominance. The United States accounts for 75 percent of global GPU capacity, leads in foundation model development, and hosts all the leading frontier models.[35] However, it has yet to translate these capabilities into a firm, lasting and dominant presence in third-country digital ecosystems. Meanwhile, China's state-driven semiconductor investment, open-source strategy, and bundled packages have the potential to scale the adoption of such models as DeepSeek-R1 in those third countries.[36] The competitive landscape therefore reflects vulnerabilities that could shift over time.

---

[35] See the Epoch AI data on total GPU clusters and the Stanford University Institute for Human-Centered Artificial Intelligence country ranking metrics (Epoch AI, GPU Clusters; Stanford University Institute for Human-Centered Artificial Intelligence, "Which Countries Are Leading in AI?").

[36] Adoption of Chinese open-weight models around the world has surged in the past year. See Lambert and Brand, "The ATOM Report."

Success depends on whose systems become embedded in the global digital infrastructure, a process in which China has made considerable progress. Partnerships in Cambodia, Southeast Asia, Hungary, Brazil, and Central Asia layer AI systems atop existing Huawei and ZTE telecom networks, raising switching costs to levels that make it prohibitively expensive for governments to overhaul entire digital stacks, even when they are concerned about data autonomy and surveillance risks. Countries increasingly prioritize co-development, local integration, and skills transfer rather than simple technology adoption, thereby advantaging China's science and technology attachés, who provide continuous technical support, compared with the limited U.S. diplomatic presence and frequent policy shifts that undermine perceptions of reliability.

Strategically, outcomes hinge on recognizing that "good enough" AI systems that meet partner needs at scale and at lower cost can secure influence and create durable dependencies. Third countries typically hedge by adopting Chinese tools for affordability and deployment speed while seeking U.S. partnerships for defense and high-end applications, making zero-risk postures that demand Chinese divestment, without viable alternatives, self-defeating. Therefore, securing influence in sectors and geographies in which military, diplomatic, or economic stakes are highest will prevent Chinese systems from gaining privileged access to sensitive data or becoming embedded infrastructure in pivotal states.

Space Systems

Outer space has evolved from a domain of general discovery, exploration, and superpower prestige into the supporting environment for the world's foundational digital infrastructure. Satellites support essential services that governments and populations depend on daily, including broadband internet connectivity, earth observation for agriculture and climate monitoring, disaster response, navigation and timing systems that synchronize global banking and logistics, and smart city platforms that coordinate public services and security. For low- and middle-income countries in particular, access to space-based capabilities is not an aspirational goal but a practical necessity for economic development and governance. This transformation has made the space-based elements of digital networks a central arena of geopolitical competition: Whichever country provides the satellites, ground stations, data systems, and technical training that developing nations rely on stands to gain substantial and lasting influence over their digital infrastructure and, through it, their societies and politics.

China has approached this competition much as it has other areas of digital network competition—with a systematic, whole-of-government strategy designed to produce Chinese predominance in key technology areas and create dependencies that leave other countries relying on Beijing's goodwill for the security of their economies and societies. Beijing bundles space cooperation with infrastructure investment, state-backed financing at rates well below Western alternatives, technology transfer, and capacity-building into comprehensive packages that developing countries find difficult to refuse. These arrangements are designed, in part, to furnish Chinese firms and organizations with leading roles across the full program life cycle, from feasibility studies through satellite design, construction, launch, and ongoing operation of ground stations. The strategic objective goes beyond commercial advantage: China is constructing what amounts to a parallel global digital ecosystem anchored in Chinese technology and governed by Chinese standards, much as it has already done with 5G telecommunications.

As we noted above, the United States retains significant advantages in this competition. Some U.S. satellite and space launch firms continue to enjoy technological advantages over their Chinese competitors. The National Aeronautics and Space Administration (NASA) has more than 600 international partnerships, backed by decades of trust built through the provision of free public goods, such as GPS and weather data. Yet Washington lacks the institutional mechanisms, long-term planning capacity, and coordinated funding to offer a credible alternative to China's bundled investment packages. U.S. warnings about the security risks of Chinese space technology have not been matched with sufficient resources to compete with subsidized Chinese offerings or planning processes to generate true ecosystem-level competitive offers. Most developing countries have responded rationally to this asymmetry by hedging. In many cases, though, this posture effectively advantages China because even partial integration into Chinese space networks provides Beijing with data access, intelligence capabilities, and normative influence that accumulates over time regardless of whether those countries formally align with Beijing.

Defining Success

Having selected four areas of digital networks for more detailed assessment, we then had to define what success looked like. We can identify factors critical to competitive advantage only if we know how to understand success.

The question of what constitutes success for the United States in digital infrastructure competition cannot be reduced to simple binaries of market dominance or technological superiority. Rather, it turns on whether U.S. engagement fosters conditions that preserve third-country agency, sustain alignment with Western systems, and prevent the consolidation of asymmetric dependencies. Achieving these conditions requires attention to three analytically distinct but operationally interconnected dimensions. Table 2.1 outlines three primary ways of understanding competitive success: in instrumental, relational, and strategic terms.

Table 2.1. Categories and Elements of Success in the Digital Network Competition

Dimension	U.S. Success	Chinese Success
Instrumental • *Overall basis for success:* Is either country gaining a dominant position in a major component of digital networks that creates a technological lock-in or otherwise leaves countries with no easily available or affordable alternatives?	• Diverse and resilient supply chains (R) • Adoption of open standards and norms (S) • Sustainable and transparent development (R)	• Chinese standards, platforms, and suppliers dominate critical nodes (S) • Diversification pathways foreclosed (R)
Relational • *Overall basis for success:* Is either country building licit or illicit relationships with governments, private-sector firms, or other actors in the country that make it politically, bureaucratically, or otherwise infeasible for the country to back out of the relationship?	• United States and West as trusted partners (R) • Capacity-building benefits local populations and skill development (R) • Regulatory alignment results in closer bilateral ties (H)	• China viewed as more reliable (R) • Local populations develop skills aligned only with Chinese digital ecosystems (R) • Partners adopt data governance models compatible with Chinese approaches (H)
Strategic • *Overall basis for success:* Does either country's position in one or more elements of a country's digital networks provide related security and strategic information or leverage?	• Digital sovereignty for third countries (R) • Adversaries unable to extract intelligence through infrastructure control (R) • Partners possess capacity to resist coercion (R)	• Diminished U.S. Influence results in erosion of digital freedoms (R) • Strategic vulnerabilities enabled (e.g., espionage, data control, breaches) (R) • Beijing gains visibility into partner operations (H) • Partners vulnerable to coercion (R)

NOTE: Tags denote the actor to whom each outcome primarily accrues: (S) denotes the supplier and its firms; (R) denotes the recipient country; (H) denotes the supplier's home government. Several elements register at more than one level; the tag indicates the dominant one, at the authors' discretion.

The outcomes cataloged in the table do not all accrue to the same actor. Some are supplier outcomes (e.g., market position), others are recipient-country outcomes (e.g., diversity of supply), and a third set accrues to the supplier's home government and its allies (e.g., intelligence access, coercive leverage, and the broader geopolitical influence that, as argued in Chapter 1, tends to follow from a leading position in the infrastructure on which a society runs). Table 2.1 tags each element accordingly.

We deliberately fold these three units of analysis into a single definition, and the reasons follow what Washington is pursuing; a purely commercial scorecard would misdescribe the objective. The United States can gain ground in this contest without a U.S. firm winning the contract: When a third country diversifies toward European, Japanese, or domestic suppliers or acquires the regulatory capacity to hold any vendor to its commitments, the result serves the shared U.S. and allied aim of preventing coercive Chinese dependence while registering nowhere in U.S. market share. The

converse also holds. A U.S. commercial 5G win that left a partner tied to one vendor and stripped of alternatives would satisfy a market-share metric while cutting against the very sovereignty argument (in this example, Open RAN) that the United States makes to prospective partners. Denial and third-country autonomy are constitutive of U.S. success in this competition, which is why they belong in the definition.

Instrumental success operates at the level of market structure and technical architecture, and its elements accrue chiefly to suppliers and to the countries that buy from them. The United States achieves instrumental success when third countries' telecommunications, payment systems, and other digital assets are sourced from multiple vendors under transparent governance frameworks built on interoperable standards and structured to prevent any single supplier from gaining access to sensitive data or imposing insurmountable switching costs. By contrast, in a world in which China succeeds instrumentally, partner nations operate digital infrastructure built predominantly on Chinese technical standards, managed through Chinese platforms, and dependent on Chinese suppliers for maintenance and upgrades—a configuration that affords Beijing continuous visibility into economic transactions, social networks, and government operations while foreclosing realistic pathways to diversification.

Relational success concerns the distribution of trust, legitimacy, and institutional alignment, the one dimension in which all three units of analysis are in play because reputation attaches to firms, capacity accrues to local populations, and alignment ultimately registers between governments. U.S. success at this level entails an earned reputation for reliable, affordable, and nonintrusive engagement that contrasts favorably with Chinese alternatives. Over the long run, this translates into regulatory harmonization and human capital development that benefits local populations and deepens partner alignment with U.S. standards and norms.

Strategic success reflects the wider U.S. geopolitical goals in the competition—specifically, the protection of third-country digital and national autonomy against Chinese efforts to create coercive dependencies and gain widespread data and intelligence access. U.S. success in this sphere represents a world in which China is unable to extract intelligence, impose extreme economic costs, or gain operational advantages through control of third-country digital infrastructure, and partner nations possess the technical and institutional capacity to resist Chinese coercion. Such resilience manifests in third countries' ability to switch telecommunications vendors during geopolitical disputes, operate government services when foreign platforms impose restrictions, and sustain payment systems and economic activity when digital infrastructure is disrupted. It is this dimension, above all, that explains why market share alone is an inadequate yardstick for the competition.

These strategic vulnerabilities reflect relative rather than absolute standards, of course. If China is engaged in important ways in a country's digital ecosystems, it will have some opportunity for intelligence-gathering and data-gathering, as well as some potential for imposing coercive influence. No easily identifiable threshold exists to define when such influence becomes unacceptable. A good example of this uncertainty surrounds the debates over TikTok's U.S. presence: How much influence over users, and how much ability to extract user data, is too much?[37]

---

[37] For a summary of the debate, see, for example, "Your Expert Guide to the Debate over Banning TikTok"; Lee, "TikTok May Not Be Chinese-Owned Anymore, but There Still Is a Privacy Problem"; and the very useful dialogue in the Supreme Court case of *TikTok Inc. v. Garland*.

Adding to the complexity is the fact that the three dimensions are interrelated. Even the strongest bilateral relationships cannot deliver strategic resilience if the underlying technical architecture locks partners into a dependency relationship that forecloses switching. Strategic success thus emerges from the interaction between technical capacity and political alignment. The former determines what partners *can* do in times of peace or crisis, while the latter determines what they *will* do—and only when both are present does digital infrastructure become a source of resilience.

This brief discussion ought to make clear that there are no simple answers to these questions and, thus, no straightforward way of assessing the degree of strategic success achieved in digital network competition. The United States and other leading democratic powers in Europe and Asia can retain the majority market share in some sectors of these networks while China becomes the dominant provider in others. Even within one area, such as telecommunications, China can gain high levels of instrumental success without advancing its relational goals.

Still, it is possible to identify critical metrics of success or failure that will characterize the digital network competition and offer a basis for identifying those factors most associated with competitive advantage. Table 2.1 outlines such metrics, both in terms of general principles of success and specific outcomes. The portrait of competitive advantage outlined in that table served as our basic guideline as we looked to specific issue areas and country cases.

Initial Findings and Lessons: Sectoral Assessments

We reviewed all four of these domain assessments for common themes that help make sense of the digital network competition and lay the groundwork for our identification of factors critical to success in this contest. Our analysis, based on our review of the literature and our discussions with government officials and private-sector leaders, suggested several major findings and insights.

Success comes in large measure from offering compelling, integrated packages of digital offerings. In all these domains, China's leading competitive advantage is arguably not any single technology or tool of statecraft but its ability to gather various parts of a comprehensive offering into off-the-shelf technology ecosystems (and, as we will stress, to subsidize their cost). Infrastructure packages under the BRI combine feasibility studies, construction, financing, and labor. In telecommunications, China's packages incorporate 5G terminals, hardware, and workforce training and, in some cases, links them to smart city platforms. China has begun to bundle several components of AI ecosystems: access to open-source models, cloud computing, software, training, and applications designed specifically for the target country's marketplace. In space, it combines satellite design, launch services, ground station construction, and engineer training into single agreements.

U.S. private-sector and governmental offerings, on the other hand, are generally more siloed, one-off programs that, in some cases, confront recipient countries with a confusing melee of agencies, financing mechanisms, companies, and technologies that do not add up to a compelling value proposition. There are exceptions to this, such as the U.S. efforts to combine Export-Import Bank of the United States (EXIM) loans with U.S. Trade and Development Agency grants to shape subsea cable choices and the formation of the Team Telecom interagency group to coordinate U.S. competitive efforts in that sector. But overall, this structural asymmetry is arguably the single most consequential competitive disadvantage the United States faces across the entire digital infrastructure

competition. It cannot be solved by improving any one component without addressing the organizational architecture that produces fragmentation in the first place.

Our analysis suggests that China's strategies risk producing ecosystem lock-in. In each of these domains, as in the competition overall, China's goal—or, at a minimum, the practical effect of its integrated packages—is not merely to win market share or achieve discrete advantages but to create various forms of lock-in that make it difficult for customers to leave its ecosystem. This is our assessment of the pattern of China's behavior rather than a stated Chinese objective. In telecommunications, for example, Huawei and ZTE equipment offerings are used as the front edge of wider network infrastructure sales and upgrade and maintenance agreements that make switching that much more difficult. BeiDou integration serves to generate positioning, navigation, and timing (PNT) dependencies that propagate across banking, logistics, and military systems. Chinese AI offerings are optimized for Chinese chips and data center design. In these ways, China seeks strategic success as defined above—creating dependency and coercive leverage are just as important as carving out a measurable position in partner countries' digital networks.

Cost and financing are leading tools employed by Beijing for competitive advantage. Across all four domains (physical infrastructure, wireless networks, AI, and space programs), the single most consistently cited factor determining the adoption decisions of developing countries is not technology quality, security, or political alignment: It is financing. China offers concessional loans, direct support, and subsidized technology costs to make its digital technology the best financial deal on offer and often the only financially feasible choice. Throughout the literature and our interviews, the same theme cropped up repeatedly: Many developed and developing countries, and many of their private-sector firms, would rather work with U.S., European, or Japanese counterparts, but the financial attraction of Chinese digital products was simply too good to pass up. Unless the United States can develop financing vehicles that allow it to compete with China's concessional terms, it will continue to lose market share and see China achieve more of its strategic goals.

Third countries are making rational cost-benefit decisions. In some cases, China engages in elite capture, sometimes through direct corruption and bribery, to win digital network competitions. More often, however, it uses the variety of tools outlined above to assemble packages that simply offer a better value proposition than other options. Potential customers, whether developed or developing nations or firms within them, understand the risks, but they ultimately make calculated decisions based on their own interests and priorities. Developing nations, for example, focus on cost, speed of deployment, and turnkey solutions—priorities that give China a tremendous competitive advantage in many cases. These tend to override security fears, which are typically perceived as theoretical and long-term considerations. Many countries also choose to deliberately hedge, working with China on some digital technologies and the United States on others, in part to maximize their leverage.

Issues of narratives, reputation, and legitimacy play a significant, if secondary, role in shaping third-country choices. The United States and China are now engaged in a battle to frame the digital network competition in terms that tilt it in their direction. The United States wants third parties to see this as a contest between democracy and autocracy, between reliable technology and insecure systems, and between sovereign autonomy and dependence on China's whims. China, meanwhile, deploys the narratives of South-South cooperation, noninterference, partnership of equals, and win-win development. Apart from a handful of advanced democracies, China's narrative is gaining currency,

partly because many developing countries are sensitive to postcolonial themes and view U.S. and European warnings as an effort to lock in Western hegemony in a new economic space. These narrative differences are partly reflected in the structure of agreements, with China offering economic concessions, turnkey solutions, co-development, and training (at least at first) while the United States offers mainly exports of individual technologies.

It does not help in this regard that the United States is increasingly perceived as an unreliable, inconsistent, and reactive partner. The Snowden revelations, Starlink's decision to suspend service in Ukraine for a time, and recent U.S. coercive moves against partners and allies mean that the United States does not enjoy its historic advantage over China as a more trustworthy partner.[38] Meanwhile, the U.S. fragmentation of policymaking across many departments and agencies, the volatility introduced by sudden congressional moves and electoral cycles, and the reliance on private actors who pursue commercial rather than strategic logic all impair the United States' ability to present itself as a reliable partner. China's state-directed model produces more consistent, predictable partner behavior despite the nature of its system.

The "soft side" of the network competition, in standards setting and governance architecture, is a critical long-term factor. This is true across all four domains that we examined in depth. Such normative and institutional aspects of technological competitions have, in the past, proven critical to establishing long-term advantage, as in the computer revolution. In our assessment, China appears to recognize this area as a classic U.S. stronghold and is seeking to upset that situation. Chinese telecommunications firms have submitted thousands of technical applications to the 3GPP and ITU. China is actively seeking to reshape elements of space law to establish the International Lunar Research Station as an alternative normative framework to the Artemis Accords. Research studies have documented many ways in which the United States retains advantages in existing standards bodies and regulatory frameworks, but China is working diligently to overturn them.

The best technology does not always win the contest for adoption. Across all four domains, superior technology does not automatically translate into competitive advantage. U.S. and allied undersea cables and U.S. AI models and space capabilities generally retain a technological lead over Chinese alternatives. Increasingly, however, China appears to be neutralizing these technical advantages with cheaper alternatives, financing offers, and off-the-shelf packages that hit all the main requirements of many developing countries. Especially in the AI domain but potentially in space as well, "good enough" technology may be able to compete with technically better U.S. offerings.

The United States and its allies confront a critical decade in the digital network competition. Historically, the most significant competitive opportunities in techno-industrial rivalries tend to arise during technological transitions, when existing commitments and dependencies are loosening and the defining technologies of the emerging era have not yet been defined. Many such transitions are soon to be underway across these four domains: from 5G to 6G, from a space architecture limited to a few players to one in which dozens of countries deploy space-based digital network assets, from the use of basic software and simple machine learning to the AI revolution. As these transitions occur, new defining technologies will be chosen and locked in, new winners and losers identified. In some cases,

[38] See, for example, Shahani, "A Year After Snowden, U.S. Tech Losing Trust Overseas," and Ortiz Freuler, "'Kill Switch Shield' and the Recurring Erosion of Trust in US Tech."

once those choices become locked in, they will be accompanied by dense, mutually supporting ecosystems that become very difficult to escape. The United States faces an urgent competitive imperative to improve the appeal of its offerings before the structural dependencies that define the next generation of digital infrastructure are set in concrete.

Chapter 3

Identifying the Factors That Shape Success in the Digital Network Competition

In Chapter 2, we defined what success looks like in this competition; in this chapter, we identify the factors that appear to produce such success. The core research question for this study focused on the sources of advantage in the competition for digital networks. What factors lead to third countries choosing U.S. or Chinese technology, infrastructure, models, or services? What characteristics of each side's technologies are most compelling?

As noted in Chapter 1, we sought to answer this question through five overlapping lines of research. In this project, after defining the elements of the competition for digital networks, we

- gathered data on the situation in the digital competition as it stood in late 2025 and early 2026
- conducted in-depth research on four components of digital network competition: physical connectivity and infrastructure, wireless and IoT connectivity and standards, AI infrastructure and data systems, and space systems
- conducted four country case studies, looking at the evolution of the digital competition in Costa Rica, Nigeria, the Philippines, and Serbia and one functional case study on subsea cables
- reviewed existing research and reporting on the DSR and the digital contest in specific countries
- conducted roughly a dozen interviews with current and former U.S. government officials and representatives of leading private-sector firms engaged in the digital competition.

The latter four endeavors generated candidate factors directly; the first supplied context on where the competition currently stands. Those four streams correspond to the four columns of Table 3.4 later in this chapter, and the framework itself was induced from that evidence. The one commitment we carried into the research was the conception of success laid out in Chapter 2, which articulated what outcomes to look for but not what produced them. Each of the nine domain, country, and issue studies was written to close with its own independent roster of governing factors, and those rosters were fixed before any attempt at synthesis; Tables 3.1 and 3.2 later in this chapter present them as we wrote them. The studies were not, however, written in isolation from one another. The four country studies and the subsea cable case followed a common template, which included sections describing competing engagement strategies, an assessment against the three dimensions of success from Table 2.1, and a forward look. By contrast, the domain assessments in Appendix B necessarily varied more in structure because the analytical problem posed by seabed warfare differs from the one posed by open-

weight model diffusion. However, each was read against the same conception of success, and that shared endpoint is what makes the two tables comparable.

Synthesis then proceeded by cross-case comparison. We tabulated the factor rosters from all nine studies alongside the themes emerging from the interviews and the literature and grouped semantically equivalent nominations under common headings. Contradictory evidence was retained, and several of the more instructive findings in this report are of that kind. For example, cost emerged as the most frequently nominated factor, yet Chinese bidders 20 to 30 percent cheaper still lost the subsea cable contests. We flag such tensions where they arise rather than absorbing them into the general pattern.

What emerged from that comparison was a set of nine factors that appear to play critical roles in determining long-term outcomes in this competition. We grouped them into two general baskets: (1) factors that recurred with the greatest consistency and weight across our cases, sectors, and interviews, which we term *primary*, and (2) factors that proved important but appeared more selectively, or chiefly as amplifiers and consequences of the first group, which we term *secondary*. The result is a combination of supply-side and demand-side influences on outcomes: The major powers offering components of digital networks can shape choices through the technological sophistication and cost of their products by seeking local influence with key decisionmakers and by integrating pieces of a larger ecosystem into a turnkey solution. Recipient countries have legal, regulatory, institutional, strategic alignment, and national development goals and characteristics that influence their choices.

These nine factors operate at different stages of competition and can serve alternative roles within a state's digital strategy. Some are contextual conditions in the recipient country (i.e., the environment) that shape which offer prevails, such as political and strategic alignment, the regulatory environment, and the maturity of digital infrastructure and institutions. Others are characteristics of the offers themselves (i.e., the means), such as cost and technology quality. And some are mechanisms through which a provider builds durable advantage (i.e., the ways)—such as ecosystem integration, lock-in effects, on-the-ground presence, and elite co-optation—which, once achieved, can generate path dependencies that shape future competition.

Table 3.1 lays out the nine factors across these primary and secondary, supply-side and demand-side, and roles-based dichotomies. Our country case studies in Appendix C provide greater illustrative detail on the interplay between these factors.

Table 3.1. Conceptualizing the Factors

Consistency and Weight of Factor	Contextual Conditions in Recipient Country (Environment)	Characteristics of Technology Offerings (Means)	Mechanisms for Building Sustained Advantage (Ways)
Primary	**Political and strategic alignment and compatibility** • *Supply side:* Competitors advance narratives to capitalize on shared geopolitical interests and cultural values. • *Demand side:* Recipient countries determine their choices based in part on self-determined ideas of norms, values, and strategic alliances. **Uneven digital governance and institutions** • *Supply side:* Competitors orient their strategies to the recipient country's institutions; better governance requires more competitive bids, while weaker governance can be exploited. • *Demand side:* For recipient countries, effective institutions and governance can make and implement choices freer from external control, while uneven governance can lead to dependencies.	**Cost and economic feasibility** • *Supply side:* Providers attempt to compete by cost, sometimes with state-backed financing. • *Demand side:* Recipient countries often look first and foremost for the best deal; and sometimes lack the financial capacity to afford other options. **Technology capabilities and quality** • *Supply side:* Providers attempt to compete by quality of products, which depends on its broader innovation ecosystem. • *Demand side:* Recipient countries face trade-offs between the state-of-the-art and "good enough" technology while reflecting on their technical capacity to absorb products.	**Ecosystem advantages** • *Supply side:* Competitors assemble various elements of statecraft (e.g., public-private actions) to create systemic advantages. • *Demand side:* Government officials, private-sector leaders, and publics in recipient countries consider the potential for quick and substantial gains across domains.

Consistency and Weight of Factor	Contextual Conditions in Recipient Country (Environment)	Characteristics of Technology Offerings (Means)	Mechanisms for Building Sustained Advantage (Ways)
Secondary	**Regulatory, legal, and policy environments** • *Supply side:* Competitors can use legal and regulatory power to "lock out" others' investments within their borders while setting standards to influence other countries. • *Demand side:* Recipient countries' regulatory, legal, and policy environments can constrain their choices among digital networks.		**Lock-in effects** • *Supply side:* Competitors seek to offer products that raise switching costs in the future. • *Demand side:* Recipient countries face a trade-off between short-term interoperability or economies of scale and long-term dependencies. **On-the-ground presence and local training and workforce development programs** • *Supply side:* Competitors build relationships and create a stronger basis for private-sector partnerships. • *Demand side:* Recipient countries gravitate toward offers that allow them to raise the proficiency of their workforces. **Elite co-optation** • *Supply side:* Competitors can foster a network of local, loyal clients via corruption. • *Demand side:* Recipient institutions may make leaders more or less susceptible to co-optation by foreign powers.

However, it is important to note that these factors do not neatly lend themselves to a general theory of success that can cut across every case. Indeed, several factors span more than one role. Financing is both a feature of an offer and a lever for building an ecosystem. Standards participation functions as both a mechanism and, once entrenched, an outcome. We treat these factors together because each shapes adoption decisions. We flag these differing roles not to reclassify the factors but to show how each contributes: at a different point in the same competition and serving different purposes within a state's digital competition strategy. Additionally, although primary factors generally appear more often and carry more weight than secondary factors, not every factor appears in every case. Consequently, there can be different permutations of factors that each lead to success, as demonstrated in Appendix C.

These realities bear on how much causal weight the framework can carry. For instance, financing underwrites ecosystem bundling; governance capacity conditions procurement; political alignment shapes the regulatory environment; and local presence deepens ecosystem integration. Because the factors are mutually constituting in this way, our evidence can establish that they recur together across settings, but it cannot isolate the independent contribution of any one of them to a given outcome. Additionally, because the factors do not always manifest in the same ways, we cannot determine which ones are sufficient on their own, which ones are necessary but not sufficient, and which ones are unnecessary but enabling. We therefore describe what our cases most consistently reveal, and we resist the stronger claim that these variables separately explain why particular decisions were made.

One of our findings complicates the analysis further: The answer to this question differs by sector. Different combinations of factors determine outcomes in the distinct areas of digital network competition. We highlight some of these differences below. But our research still validates the importance of several common variables across these domains of competition.

As noted in Chapter 1, it is important to stress the limitations on our findings. We reviewed existing literature, case studies, our interviews, and other sources. Each source nominated factors critical to digital competition outcomes. In many cases, these emerge directly from case experience or the testimony of U.S. or private-sector officials who have been on the front lines of competing with Chinese technology firms and government offerings. But the mix of variables that will determine the outcome of individual future competitions for network influence and access remains uncertain. Our findings are strong but not generalizable in an unqualified way. We are confident that the menu of factors we offer stands out from our qualitative survey, but other factors could play a role in future cases as well.

Review of Case Study Findings

In addition to our general review of literature and interviews, the primary source of our findings came from nine specific sectoral, country, and issue case studies: four of the most significant domains of digital competition, as articulated in Chapter 2; four country cases (Costa Rica, Nigeria, the Philippines, and Serbia); and one specific functional issue case (subsea cables). The full analyses of the domains of competition appear in Appendix B; the full country and issue cases appear in Appendix C. All those assessments identify specific factors of success. Table 3.2 summarizes the factors highlighted in the domain analyses. Table 3.3 lists the factors that emerged from the country and subsea cables cases. We derived the overall set of factors (listed later in this chapter in Table 3.4) primarily from these lists.

Table 3.2. Factors Associated with Success: Domain Case Studies

Domain of Competition	Factors Governing Success
Physical connectivity and infrastructure	• Financing, including the use of investment and concessionary projects to increase the attractiveness of offerings • Integrated programs that offer multiple components of an infrastructure or technology stack in coordinated efforts • Credibility and a reputation for trustworthiness in executing projects • Chokepoint control over the exchange of key resources or data in ways that convey leverage • Navigation of third-country institutional and regulatory frameworks shaping participation in infrastructure projects (e.g., permitting processes) • Resilience, redundancy, and the ability to defend and reconstitute infrastructure on disruption
Wireless and IoT networks	• Offering vertically integrated, turnkey packages of capabilities and solutions • Cost and economic feasibility • Governance structures and standards that shape the ecosystem for wireless adoption • Lock-in factors, including reliance on providers of new technology for updates and capacity-building and the sometimes-limited infrastructure capacity of third countries • Trust factors, including data and information security • Political-strategic alignment of the third country with the provider • Speed of deployment to address the urgent needs of developing countries for technological advancement • Narrative resonance that aligns with the needs of the third countries
AI infrastructure and data ecosystem	• Offering vertically integrated, turnkey packages of capabilities and solutions • Cost and economic feasibility • Regulatory and technical alignment of the third country's digital networks with the providing state's AI and data center offerings • Trust factors, including concerns over data sovereignty, surveillance risks, and the security of sensitive data processed through foreign AI systems • Sustained support, co-development partnerships, capacity-building, and workforce development, including through a consistent on-the-ground presence • Energy infrastructure readiness and the capacity to sustain large-scale data center operations through reliable and scalable power generation • Speed and practicality of deployment, including the ability to deliver operationally adequate solutions at scale to countries with limited existing infrastructure • Technology leadership in ways that attract third-party engagement
Space systems	• Regulatory and standards alignment with the recipient country • Offering vertically integrated, turnkey packages that bundle space cooperation with broader economic incentives • Trust around information security and the dual-use nature of space infrastructure • Alignment to the needs and goals of the recipient country; cooperative approaches that meet the needs of partners, including multilateral approaches • Lock-in factors regarding dependency on technology networks • Capacity-building efforts and technology transfer

Table 3.3. Factors Associated with Success: Country and Functional Issue Cases

Case Study	Factors Governing Success
Costa Rica	• Cost and financing competitiveness, including the role of concessionary lending and large-scale public financing • Technical standards and architecture mandates, such as Open RAN and 3GPP compliance, as sustainable mechanisms for managing security risks and avoiding the diplomatic costs of outright vendor bans • Recipient-country institutions, governance frameworks, and rule of law that enable transparent procurement, enforcement, and switching when incumbents fail to meet compliance standards (e.g., Chinese noncompliance) • Credibility and reliability in project execution, in which poor delivery can erode a provider's position and create openings for competitors • Crisis events, such as major cyberattacks, that reshape political priorities and create momentum for diversification • Bundled offerings combining financing, capacity-building, training, and strategic advisory support
Nigeria	• Cost of major programs • On-the-ground presence, including commercial representatives during the sales period and training and sustainment activities after deployment • Lock-in effects of technology ecosystems • Elite capture through long-term relationship cultivation • Status of domestic institutions and regulatory environment
The Philippines	• Cost, affordability, and speed of deployment, particularly where rapid nationwide coverage is a binding policy objective • Turnkey delivery models that reduce coordination risk • Recipient-country market structure and policy imperatives that shape partner selection, including the need to address incumbent market failures • Recipient-country regulatory frameworks shaping the conditions of foreign participation without preemptively excluding specific actors • Security concerns and trust factors, although they may be outweighed by operational imperatives • Existing vendor dependencies and technology lock-in effects that constrain the ability to shift providers
Serbia	• Geopolitical alignment issues (in this case, conflicting ones) • Domestic regulatory environment • Cost of competing offerings as manipulated by subsidies • Potential for rapid deployment • Elite ties and long-term relationship-building, partly as a function of on the ground presence
Subsea cables	• Geopolitical alignment and diplomatic pressure from major powers over political reliability issues • Cost driven by state subsidization of projects • Technical quality of competing offerings • Domestic regulatory environments used to manipulate the competitive environment (such as Federal Communications Commission [FCC] regulatory enforcement by the United States) • On-the-ground presence—long-term human capital development • Chokepoint control over global data flows, with redundancy and resilience to disruption

We also reviewed the categories of success in digital network competition laid out in Table 2.1 for clues to the sorts of factors that would be critical in achieving those outcomes for either the United States or China. Our conception of success highlights several possible kinds of tools, capabilities, or qualities that could be important. They include

- anything that makes one side's physical systems more inherently attractive for third-country projects in clear material or technological terms
- factors that give one side a clear advantage in setting norms and standards for digital networks
- technological, political, or structural factors that tend to create lock-in on one provider's offerings
- strong relationships with recipient country governments and decisionmakers
- factors related to the trust and confidence that third parties have in digital providers
- bureaucratic, legal, or regulatory aspects of the third party's digital policies and aspirations that create alignments or roadblocks to working with specific providers.

Those considerations parallel many of the themes laid out in Tables 3.2 and 3.3. They begin to point in common directions and establish a shared vision of the factors that shape success.

Using these assessments, complemented by our general research and interviews, we identified nine total factors of success that seem common across many domains and cases. As described previously, we divided them into *primary factors*—those nominated most often and most emphatically across the four lines of evidence and most frequently described as pivotal to a decision—and *secondary factors*, which appear more sporadically and typically operate as amplifiers, constraints, or downstream consequences of the primary drivers rather than as independent determinants.

Table 3.4 summarizes all nine factors, indicating the sources of support for each one's importance. In the table, we rate how strongly each of our four sources of evidence supports each of the factors: very strongly, somewhat strongly, or less strongly. These ratings record the weight of evidentiary support, not the magnitude of a factor's effect. A "very strong" rating means that the factor was named in most or all relevant instances within that line of evidence and treated there as decisive or near decisive; "somewhat strong" means that it recurred but usually as a contributing consideration; and "less strong" means that it surfaced in a minority of instances or chiefly as a background condition. As noted above, that evidence is qualitative and admits uncertainties about future cases but is, in all cases, at least somewhat direct and empirical. The sections below describe the factors in detail.

Table 3.4. Determinants of Outcomes in Digital Network Competition: Factors Most Consistently Observed Across the Evidence

Factor	Significance in Research Findings			
	Country and Issue Cases	Sector Cases	Interviews	General Research
Primary factors				
Cost and economic feasibility	Very strong	Very strong	Very strong	Very strong
Ecosystem advantages	Very strong	Very strong	Very strong	Very strong
Political and strategic alignment and compatibility	Very strong	Very strong	Somewhat strong	Somewhat strong
Technology capabilities and quality	Somewhat strong	Very strong	Somewhat strong	Somewhat strong
Uneven digital governance and institutions	Very strong	Somewhat strong	Very strong	Somewhat strong
Secondary factors				
Lock-in effects	Somewhat strong	Somewhat strong	Less strong	Somewhat strong
Regulatory, legal, and policy environments	Somewhat strong	Somewhat strong	Somewhat strong	Somewhat strong
On-the-ground presence and local training and workforce development programs	Somewhat strong	Somewhat strong	Less strong	Less strong
Elite co-optation	Somewhat strong	Somewhat strong	Less strong	Somewhat strong

NOTE: Darker colors indicate stronger relationships.

The distinction between primary and secondary factors reflects both the frequency of their appearance across our evidence base and the weight that our sources assigned them. Primary factors are those that recipient country officials, U.S. government officials, industry participants, and case study authors returned to repeatedly when explaining why a decision went the way it did—with cost and geopolitical alignment above all. Secondary factors, by contrast, tend to operate as amplifiers, enablers, or downstream consequences of the primary drivers. Lock-in effects, for example, typically emerge after an initial commitment shaped by cost or ecosystem bundling; regulatory environments constrain the field of competition but rarely appear in our cases as the decisive consideration on their own. The secondary factors are important in that they can be decisive in specific contexts, and their cumulative effect reinforces patterns established by the primary drivers. The two categories are thus better understood as a gradient of observed prominence.

Primary Factors

Our research highlighted five determinants of success that surfaced most consistently across our cases, interviews, and literature review and that our sources most often identified as shaping third-country adoption decisions. Each of these factors was described in at least one setting as sufficient on its own to tip a country's choice toward one provider over another, even if our research does not allow us to predict which ones will be most decisive in any specific future case or to disentangle their effects where several operated at once. They are (1) cost and economic feasibility, (2) ecosystem advantages (particularly China's ability to link several tools of statecraft to achieve certain results), (3) political and strategic alignment and compatibility, (4) technology capabilities and quality, and (5) uneven digital governance and institutional contexts that either create or foreclose opportunities for outside influence. The sections below describe each of these variables.

Cost and Economic Feasibility

In the cases, interviews, and existing research surveyed for this analysis, this first variable—the basic cost of the relative U.S., Chinese, or other digital offerings for a third party—was often nominated the single most decisive factor governing choices among digital network offerings. These countries (or firms within them, which are sometimes the ones making decisions to partner) are looking first and foremost for the best deal. That judgment involves several distinct elements, but cost is often first in line, in part because of the financial limitations of developing countries and companies. Financing is treated here as an element of cost; as discussed below, it also operates as a mechanism for building ecosystem advantage (see the next section, "Ecosystem Advantages") and recurs as a distinct finding in Chapter 4.

This factor has been most evident in telecommunications, in which Huawei has long offered a cheaper and technologically equivalent or even superior alternative to European firms. Country case studies, interviews, and the broader literature on digital competition all point to cost considerations as a dominant reason for Huawei's attractiveness. Chinese firms have also offered strikingly lower bids for undersea cables,[39] although cost considerations have not yet tilted the playing field decisively toward Beijing in that domain because of the lock-in effect of cable installation. It is not yet as decisive an influence in other areas, but it is becoming increasingly important in the AI field, in which Chinese open models offer less expensive alternatives to U.S. counterparts.[40]

Underpinning these cost advantages is a stark asymmetry in state-backed financing. In 2023, China's export credit financing totaled $39 billion, compared with $2.7 billion for the United States. That same year, Xi Jinping called for the Export-Import Bank of China and China Development Bank to each assemble a $48 billion fund to support investment in DSR projects in particular.[41] This

[39] Chan, *China's Digital Silk Road*, pp. 96–97.

[40] Daniels and Dohmen, "China's Overlooked AI Strategy"; Morieson, "How China Is Betting Cheap AI Will Get the World Hooked on Its Tech"; Kynge, "Low-Cost Chinese AI Models Forge Ahead, Even in the US, Raising the Risks of a US AI Bubble"; Irwin-Hunt, "US–China AI Model Costs Diverge."

[41] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 19.

disparity in public financial firepower gives Beijing a structural ability to subsidize offerings across the digital stack at price points that competitors relying primarily on private capital find difficult to match.

China's cost advantages do not all come from state subsidies. Chinese goods are often cheaper at the factory gate because of scale, labor costs, and exchange rates. A well-known category is direct and indirect state subsidies to Chinese firms in everything from energy costs to tax holidays to guaranteed purchases and low-cost loans.[42] Chinese investment organizations also grant concessionary loans to buyers of Chinese technology to further reduce the cost. China uses its immense and significantly protected domestic market to develop new products; its firms become accustomed to cutthroat competition that demands reducing price in every way possible. Lower-cost Chinese labor, even in high-skill professions, helps keep cost down. And finally, Chinese cost advantages come, in part, from its extensive ecosystems: the ways in which multiple firms, and sometimes the Chinese government itself, assemble broad packages of elements that represent an incredibly combined bargain. These packages can include low-cost core components, concessionary financing, and related elements of a technology stack. Multiple interviewees reported confronting "full end-to-end offers" from Chinese competitors, often cleverly tailored to the needs of specific countries.

One increasingly important issue, especially in the emerging area of AI technology stack competition, is the role of venture capital (VC) funding in shaping the financial context for digital network projects. Traditionally, the U.S. VC ecosystem is much stronger than China's. When digital projects in third countries, such as Nigeria, can attract U.S. VC funding, that provides a relative advantage to the United States. Increasingly, however, VC funding in developing nations, especially in Asia, is searching out Chinese partnerships.[43] As early as 2020, Chinese technology companies and VC funds had collectively invested an estimated $4 billion in Indian startups alone, backing 18 of India's 30 unicorns (private firms that have grown to a value of more than $1 billion) at the time. If Chinese capital can achieve that degree of penetration in a market as strategically contested as India's, the potential for similar dynamics in smaller, less scrutinized markets across Southeast Asia and the Global South is considerable.[44]

Although lowering costs provides critical competitive leverage, it is not the only way to compete. A state can also increase the cost of a competitor's bid. In the case of subsea cables, the United States has threatened sanctions on China's subsea cable supplier, HMN Tech, thereby raising the cost of doing business with them despite their systematically lower bids. Thus, sanctions provide one asymmetric tool for increasing a competitor's costs, especially if a state's commercial suppliers cannot lower their own.

In sum, then, cost has been an extremely important factor in shaping digital network competition and looks likely to continue to be, especially in the AI space.

---

[42] Hart and Link, *There Is a Solution to the Huawei Challenge*.

[43] Shao, "Southeast Asia Capital and Companies Eye China AI Development, Similar to the Internet Era."

[44] Bhandari, Fernandes, and Agarwal, *Chinese Investments in India*, p. 6.

Ecosystem Advantages

The second factor determining outcomes in digital network competition is closely related to the first. It is the ways in which either side—but in practice, almost always China—can assemble various elements of statecraft to shape the choices of third parties. Through coordinated state and private-sector actions and offers, China creates systemic advantages that individual U.S. or European firms have difficulty competing against.

China's competition ecosystem has several layers. Beijing first sets the foundation through its domestic industrial policy, cultivating competitive firms and promoting hard-edged competition that winnows the field to one or a few leaders. (This can have negative side effects, such as the phenomenon of *involution*, in which firms battle each other into minimal profits and sometimes bankruptcy. But state support still creates powerful, technologically advanced firms with a massive domestic market as their base of strength.) China then links these firms into a broad set of integrated capabilities and activities. Several of these elements, financing in particular, also appear among the primary factors we identified; here, they function as components of an integrated ecosystem rather than as stand-alone drivers. Those elements include

- direct financing support
- involvement of other firms to assemble end-to-end technology packages in such areas as smart cities, telecommunications, space assets,[45] and AI[46]
- investments from the BRI or other sources to promote related infrastructure or industries, connect digital and physical infrastructure, and offer sweeteners to specific individuals or ministries in the target countries
- general patterns of economic engagement, including trade and investment[47]
- other economic promises or threats, including trade concessions or threats of sanctions and trade and investment punishments
- diplomatic activities aimed at key decisionmakers in the target countries
- information campaigns and cultural diplomacy campaigns to enhance China's reputation
- security commitments and relationships[48]
- human engagement activities, such as scholarships and training programs
- elite capture through direct and indirect bribery and corruption.

The result is a synergistic effect well beyond the sum of its parts. Governments, officials, private-sector leaders, and publics in target countries confront both the potential for gain and the risk of loss across a variety of domains.

---

[45] Chan, *China's Digital Silk Road*, pp. 109–110.

[46] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 26.

[47] One study found that trade ties offer significant predictive power in anticipating a country's cloud computing choices; see Lehdonvirta, Wu, and Hawkins, "Weaponized Interdependence in a Bipolar World."

[48] The same study found a statistical correlation between security ties and data center outcomes; see Lehdonvirta, Wu, and Hawkins, "Weaponized Interdependence in a Bipolar World."

Some of these ecosystem advantages are emerging from Chinese state support. Beijing clearly has an ecosystem-dominance mentality in its digital network plans and offers mutually supporting components of networks, along with financing and associated diplomatic engagements (and in some cases, bribery).[49] As "virtual" as digital data can be, critical elements of digital networks comprise physical infrastructure, such as undersea and subterranean cables, mobile towers and base stations, fiber optics, surveillance technology, and more.

The evidence supporting the importance of Chinese state support comes from a wide variety of sources.[50] It was a dominant theme in our interviews with current and former U.S. government officials and private-sector representatives who stressed the fact that U.S. firms are competing not against individual rival firms but a wider ecosystem of Chinese state activities: "We're not competing against a company—we're competing against China's high tech and manufacturing ecosystem." Studies of China's efforts to gain traction in digital standards setting also stress the ways in which Beijing combines various elements of its efforts for synergistic effect.[51]

Case studies provide some of the best evidence of the ways in which the ecosystem of Chinese tools and activities provides competitive advantage. In our own cases, Costa Rica and the Philippines illustrate China's whole-of-ecosystem approach. In Costa Rica, Huawei's 2009 capture of the Instituto Costarricense de Electricidad (ICE)'s 3G bid was accompanied by low-interest financing; high-profile gifts, including a $100 million national stadium and hundreds of police vehicles; the purchase of $300 million in government bonds; and sustained diplomatic courting of ICE officials.[52] In the Philippines, Beijing assembled a vertically integrated package to secure DITO Telecommunity's entry as the country's third mobile operator, combining China Telecom's 40-percent equity stake and Huawei and ZTE equipment supply, despite espionage concerns raised by Philippine officials.[53] In both cases, Chinese success rested not on any single competitive advantage but on the coordination of financing, equipment, and diplomatic engagement into packages that individual Western firms struggled to match.

The same dynamics emerge in other cases. In Kenya, bilateral trade with China has expanded dramatically, state subsidies promote Huawei products, Chinese firms have invested in the country's physical infrastructure, and Chinese diplomats have engaged with numerous Kenyan officials. Furthermore, Beijing has conditioned foreign assistance to Huawei contracts.[54] In Indonesia, Chinese firms benefit again from subsidized offerings, influence generated from investments and foreign assistance, elite capture efforts that take advantage of lax corruption enforcement, general diplomatic engagement, and other tools.[55] In all these countries, Chinese firms are empowered to offer

---

[49] Patil and Gupta, *The Digital Silk Road in the Indo-Pacific*, pp. 8–9.

[50] Patil and Gupta, *The Digital Silk Road and Smart City Networks in the Indo-Pacific*, describes many ways in which China's digital ecosystems enhance its smart cities offerings abroad.

[51] He, "The Digital Silk Road and China's Influence on Standard Setting," p. 7.

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

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

[54] Chilukuri and Scanlon, *Countering the Digital Silk Road: Kenya*, pp. 2, 8.

[55] Chilukuri and Scanlon, *Countering the Digital Silk Road: Indonesia*, pp. 5–6.

comprehensive investment packages including "everything from a project's initial feasibility study to its financing, construction, labor, and even management."[56]

This factor has not produced unqualified success for China. Over time, Beijing's most intense efforts to use ecosystem advantages to dictate outcomes have generated resentment and pushback. This has been true with the BRI in general and some of China's boldest efforts to bribe officials. In Brazil, China's widespread influence and economic role have generated growing suspicions.[57] Additionally, in Nigeria, Chinese construction projects have been the subject of anticorruption campaigns.[58] Chinese cyber operations and intellectual property theft have alienated some governments and partners.

One critical output of this coordinated approach is the speed of deployment. Because China's ecosystem can bundle such factors as financing, equipment, labor, and diplomatic engagement under centralized direction, Chinese companies can move from an initial offer to operational infrastructure more quickly than U.S. competitors. For developing countries facing urgent connectivity gaps, for example, a credible offer available now often outweighs a superior offer available in three years. China exploits this asymmetry and endeavors to establish a foothold quickly through deployment speed, then builds dependency over time through maintenance contracts, upgrades, and cross-system linkages. The Philippines' DITO rollout illustrates this dynamic, in which China Telecom's equity stake, combined with Huawei and ZTE equipment supply, enabled a vertically integrated deployment timeline. It is unclear whether China's speed advantage would persist if U.S. offerings could match deployment timelines.

Political and Strategic Alignment and Compatibility

Such factors as cost and the competitive effect of ecosystem strategies do not play out on blank geopolitical canvases. Countries are open or closed to U.S. or Chinese digital offerings for reasons related to their geopolitical alignment, national political culture, and business environment. In some cases, our sources described this factor as the one that settled the question: With several U.S. allies, it has overridden all other variables to dictate outcomes in parts of the digital network competition. This is one of the leading demand-side factors that shape digital network outcomes: Recipient countries determine their choices based, in part, on self-determined ideas of norms, values, and strategic alliances.

Among the countries in which this factor prevails, the United States gains tremendous strategic advantage that, in some cases, can negate factors working in China's favor.[59] Such countries as Kenya, Indonesia, Saudi Arabia, and Türkiye want to preserve close security relationships with the United States, and this creates some level of constraint on the degree of their alignment with China in the digital space. These preferences are underpinned in many cases by decades of U.S. security and

---

[56] Chilukuri and Scanlon, *Countering the Digital Silk Road: Indonesia*, p. 5.

[57] Scanlon and Drexel, *Countering the Digital Silk Road: Brazil*, p. 6.

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

[59] Wu, "Technology, Power, and Uncontrolled Great Power Strategic Competition Between China and the United States," pp. 111–113.

private-sector relationships in these countries, which have built a natural support system in these societies, especially in their national security communities.[60] U.S. officials can engage in active diplomatic efforts to capitalize on this leverage—for example, in the case of subsea cables, U.S. officials have tried to create a shared understanding among allies and partners of the threat posed by Chinese cable suppliers. But such countries as Serbia reflect competing alignment pressures: On one hand is a desire and need to integrate its standards and regulatory structure with the European Union, and on the other, a long-standing partnership with China that has produced deeply embedded personal relationships and political cooperation.

However much some countries have traditionally been aligned with the United States, an important element of the alignment dynamic pushes the direction of balance between the United States and China: Many states are determined to hedge in this competition, both in general and in the digital network contest in particular. As noted previously, revelations about U.S. spying in the digital domain (such as the Snowden leaks), as well as recent U.S. coercive behavior, have made many countries even more determined to reduce dependence on U.S. technology ecosystems.

Malaysia provides a good example of this hedging behavior in the digital sphere. It has actively sought high-technology collaboration with Chinese, U.S., and other firms,[61] developing billions in investments and projects with Google, Microsoft, ByteDance, Alibaba Cloud, and many others. Senior Malaysian officials have explicitly indicated that the country will not choose U.S. or Chinese sides in the competition.[62] The government has made some efforts to recognize U.S. technology security concerns, including at least temporarily shelving a planned project to develop an AI system built on Huawei chips.[63] There is evidence, though, that China's ecosystem approach is bearing fruit, with many Chinese AI-related projects gaining a foothold in Malaysia.[64]

These hedging impulses play out differently even within the same region, largely as a product of domestic politics and leadership preferences. Serbia, which has served as China's major partner in the region, has chosen a more consciously hedged position with strong involvement of Chinese firms, engaging strongly with Huawei on 5G, smart city initiatives, and national and city data centers, alongside Nuctech, NetDragon, and BGI (formerly Beijing Genomics Institute).[65] But Albania, Kosovo, and North Macedonia, all seeking closer ties to the West, have been more circumspect in their involvement with Chinese firms and more engaged with U.S. digital standards networks.[66]

Such alignment and culture factors have differential effects across different areas of digital networks and offer no guarantee against significant presence by high-technology firms from the

---

[60] On the Saudi Arabia case, see Chilukuri and Scanlon, *Countering the Digital Silk Road: Saudi Arabia*.

[61] Anand, "Malaysia Taps Chinese Investors to Build More Data Centers."

[62] Confino, "Malaysia Will Work with Both the U.S. and China in Developing AI, Says Top Minister."

[63] Shaw and Anand, "Malaysia Downplays Huawei Deal as US Checks China's AI Reach."

[64] For recent reporting on this connection, see Mokhtar, Hawkins, and Koswanage, "Malaysia Eyes Huawei Chips for AI Project Despite US Warning," and a Chinese report: "China, Malaysia Explore New Opportunities for AI-Driven Economic, Trade Cooperation."

[65] Jagtiani, *Deep Down in the Stack*.

[66] Haxhixhemajli, "The Western Balkans and China's Digital Silk Road."

United States or China. Germany is a U.S. treaty ally and has pulled back from Huawei in the 5G space, but, like many European countries, it relies heavily on subsea and terrestrial cables owned in part by Chinese firms.[67]

Washington's approach to its position in leading-edge digital network areas will shape how third countries perceive U.S. reliability as a partner. Many governments and private firms abroad, already attuned to such episodes as the Snowden revelations, are closely watching for signs that U.S. technology ecosystems might be leveraged to constrain their sovereign autonomy. U.S. government pressure on Anthropic to modify its AI safety commitments, for instance, may also be interpreted in some quarters as precisely such a signal. To the extent that U.S. policy is perceived as prioritizing control over openness, it risks reinforcing the narratives China actively deploys and accelerating diversification away from U.S. digital offerings.

Technology Capabilities and Quality

Third-party choices in digital networks are also consistently associated with the technological quality of competing offerings. In the areas in which the United States and its allies have retained the strongest positions, such as subsea cables, AI, and data centers, U.S. and allied technology remains demonstrably superior, or at least equivalent, to Chinese offerings. Submarine cables illustrate this: U.S., French, and Japanese firms remain the global leaders in the sector. Space represents a mixed picture; U.S. firms retain a clear technological and market lead in space launch, but China has become a genuine competitor in PNT. 5G tells yet a different story: Huawei has developed technology equal or superior to Western alternatives and paired it with a lower price, producing a decisive asymmetric advantage.

Part of the issue surrounding technology capability is innovation and which side can bring new products to market more quickly and offer better systems across these various sectors. This is truer in some sectors than others, depending on the speed of innovation. The technology of 5G telecommunications remains fairly static; a potential 6G or other advance could create new opportunities for breaking up existing market shares. Space launch and communication assets have seen some of the biggest innovations over the past two decades—in this sector, by U.S. firms (notably SpaceX), which have revolutionized satellite-based communications. In the future, breakthroughs will provide the basis for competitive advantage, especially if they allow customers to escape lock-in dynamics with existing providers.

One phenomenon at work in this factor is that many users can get by with "good enough" technology deployed at speed. Chinese cloud service providers may not offer services that compete in quality terms with their U.S. rivals, but if they are mostly as good, and far less expensive, that may be enough for many users' workloads. That said, the "good enough" calculus can shift abruptly when security vulnerabilities are exposed. Instances of cyberattacks or network breaches in third countries have prompted governments to rethink their reliance on Chinese telecommunications infrastructure, although, as noted above, many countries have become equally concerned about the risk of U.S. cyber

[67] Jagtiani, *Risky Configuration*, pp. 18–20.

espionage and coercive use of digital dependencies.[68] Another phenomenon is the recipient country's technical capacity to absorb certain technologies, which could constrain its choice among alternatives on the market.

In terms of technological position across the full range of digital network competition, the United States and its friends and allies remain in a very strong position. Huawei's 5G advances are a celebrated contrary case, but, across much of the competition, U.S. and allied firms remain world leaders in technology and innovation.

Uneven Digital Governance and Institutional Contexts

A final leading factor influencing digital network competition is the maturity and quality of governance and institutional effectiveness in the third-party countries. This factor shapes the degree of influence that outside actors can have: On one hand, powerful, effective institutions and digital governance contexts can make and implement choices freer from external control. On the other hand, uneven digital governance and shortcomings in institutional and policymaking quality in recipient nations sometimes open the door to Chinese influence. This is another demand-side factor, in that it influences the perspective of recipient countries in ways that shape outcomes.

Some developing nations have built relatively strong and independent institutions governing their digital ecosystem development.[69] Others have weak governance structures, high levels of corruption, and inconsistent long-term digital strategies. Even in some leading industrial countries, institutional legacies can complicate restrictions on Chinese offerings. In Germany, for instance, the transportation minister also held responsibility for digital affairs (including cross-border data traffic), creating entangled relationships that have hindered efforts to exclude Chinese providers.[70]

The issue is one not only of untoward influence but also a basic lack of sophistication and institutional positions on some issues. Often, developing countries may lack the technical expertise, dedicated regulatory bodies, or evaluative frameworks to assess long-term security, interoperability, and dependency implications of complex digital infrastructure proposals. Without established review processes and related institutions, third-country officials may be unable to meaningfully compare competing bids on anything beyond upfront cost, which, as discussed above, tends to favor Chinese offerings.

In such environments, decisions may often fall to individual officials or ministries operating without coordinated national digital strategies, making outcomes more susceptible to the preferences of whichever external actor arrives first with a comprehensive proposal. This institutional gap is particularly consequential in emerging areas, such as AI governance and cloud data sovereignty, in which even advanced economies are still developing their approaches. Countries that have not yet formulated national stances on these issues are unlikely to impose meaningful conditions on foreign providers, ceding standard-setting influence to external actors by default.

---

[68] Greig, "US Commits $25 Million to Costa Rica for Conti Ransomware Recovery."

[69] Kenya is one example. See Chilukuri and Scanlon, *Countering the Digital Silk Road: Kenya*, pp. 7–8.

[70] Zimmermann and Verhelst, "German Ministers Dash to China in Bid to Escape Retaliation over EV Duties."

Secondary or Context-Specific Factors

Besides those five leading factors, our research identified four additional variables that shape outcomes but operate differently and appear less uniformly. We characterize these as secondary because, in the cases and evidence we reviewed, they typically functioned as reinforcing mechanisms or consequences of prior choices rather than as independent first-order factors or drivers. Their influence is often conditional and could be consequential in some contexts but marginal in others. The secondary factors are lock-in effects, the role of regulation and legal and policy standards in shaping the landscape for competition and standard-setting processes, on-the-ground presence on the part of outside digital powers, and elite capture.

Lock-In Effects

In some cases, committing to certain categories of U.S. or Chinese digital products can generate significant lock-in effects that make it practically impossible for countries to shift to alternative suppliers. This dynamic can be especially powerful when a country commits to a whole ecosystem from one supplier—from financing mechanisms to associated foreign aid and investments to multiple elements of a specific digital technology offering. For a recipient country, such a decision often comes with short-term benefits, such as interoperability and economies of scale, at the cost of long-term (and often unanticipated) dependencies.

Several examples emerged in our research. In Costa Rica, Huawei's 2009 capture of ICE's 3G network contract created dependencies that proved difficult to reverse. ICE now relies on Huawei routers, private operators Telecable and Claro use Huawei modems, Chinese smartphone brands dominate the consumer market, and municipalities have installed Hikvision surveillance systems.[71] Notably, when Huawei breached contract terms between 2011 and 2014, Beijing converted potential reputational damage into deeper lock-in by offering equipment donations in lieu of financial penalties, yielding additional infrastructure projects that further embedded Chinese technology.[72] Even as Costa Rica has moved decisively toward Western suppliers for its 5G core network, these legacy dependencies persist at the consumer and peripheral layers, illustrating that lock-in can endure in parts of the ecosystem long after strategic direction shifts at the core.

Conversely, the Western ecosystem is now generating its own lock-in. The $300 million U.S. EXIM credit line for 5G procurement, AT&T's role as anchor tenant on the TAM-1 subsea cable, and Costa Rica's adoption of 3GPP-compliant Open RAN architectures collectively raise switching costs for any future reversion to Chinese suppliers.[73] Lock-in, then, is not exclusively a Chinese advantage but a structural feature of digital infrastructure investment that works in both directions and that appears in more than one role in this framework: as a secondary factor that can shape a

[71] Ellis, "China's Success and Struggles in Costa Rica."

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

[73] EXIM, "EXIM Board of Directors Approves Preliminary Commitment to Support Development of 5G Network in Costa Rica"; Submarine Cable Networks, "TAM-1"; CSA Group, "Costa Rica (SUTEL)—National Frequency Allocation Plan Update."

procurement decision and as an outcome of successful deployment that then raises the cost of switching.

Regulatory, Legal, and Policy Environments

U.S. and third-country legal and regulatory structures may impede or encourage integration with U.S. or Chinese firms. This is a distinct factor from institutional quality; the issue here is whether rules and laws in such areas as data privacy, spectrum allocations, export controls, cybersecurity frameworks, and infrastructure regulations make it easier or more difficult for outside firms to capture domestic market share. Recipient countries have their own national development goals and govern them with self-determined legal and regulatory standards. This factor is one of the most prominent demand-side variables shaping digital network outcomes.

In 5G, for example, spectrum allocations, which assign usable broadcast "lanes" to specific firms, are a significant issue; U.S. domestic spectrum decisions can set the stage for success or failure in wider digital networks.[74] On the Chinese side, Beijing's spectrum policy has given Chinese operators a head start on dense deployments and traffic. Large, early mid-band allocations for 5G have materially helped Chinese vendors diffuse their products both at home and abroad.[75] Cyber policy can be equally consequential; national incident response requirements, vendor certification standards, and rules governing cross-border data flows can effectively determine which foreign providers are eligible to participate in a country's digital infrastructure and on what terms.[76]

One aspect of evolving ecosystem dynamics that deserves to be called out on its own terms is the role of technology standards, in both the public and private sectors, which functions both as a component of ecosystem competition, discussed above as a primary factor and, once entrenched, as an outcome that shapes later competition. Governments are setting a range of standards that govern digital networks. In developed nations, some of these relate to information security and sharing. Private firms, as they have done in technology for decades, are setting standards to ensure interoperability, reliability, and other goals. Outcomes in this contest will be strongly influenced by technology adoption: Countries with the dominant market share or technological sophistication in a domain tend to set the standards. China is treating its domestic digital standard development process as a dry run for internationalizing its standards.[77]

There are examples of such policy issues across dozens of countries. In Costa Rica, the interplay between regulatory mechanisms and digital competition has been especially instructive. The government's 2023 decree barring non-signatories to the Budapest Convention on Cybercrime from participating in 5G networks—widely interpreted as targeting Huawei—was one of the most explicit interventions in our case studies. When courts suspended the decree, Costa Rica pivoted to a potentially more durable mechanism of mandating Open RAN architecture, which reduced single-

---

[74] Lee, *Navigating the U.S.-China 5G Competition*, pp. 3–4.

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

[76] Dekker, Okano-Heijmans, and Zhang, *Unpacking China's Digital Silk Road*, pp. 12–13.

[77] Dekker, Okano-Heijmans, and Zhang, *Unpacking China's Digital Silk Road*, pp. 10–12; Chilukuri and Scanlon, *Countering the Digital Silk Road*, pp. 28–29.

vendor dependency without the diplomatic costs of outright country-based exclusions.[78] A similar dynamic occurred in the Philippines with the 2022 revision of Republic Act No. 11659.[79] The act both liberalized foreign ownership in telecommunications and introduced national security screening for critical infrastructure investments, an approach designed to attract capital while retaining control over high-risk participation. In Kenya, government cloud policy issues helped set the context for competition.[80] In multiple countries, new AI deployment and diffusion rules have the same effect.

The character of these issues differs significantly by sector and country. Only within their borders can the United States and China *consistently* leverage legal and regulatory power to "lock out" the other's investments, such as in the case of subsea cables, in which Team Telecom and the FCC have successfully excluded Chinese cables and related infrastructure projects that would have connected to the United States. By contrast, beyond their respective borders, this factor does not generally favor U.S. or Chinese offerings; its effect depends on the context. Nor is it the case that these laws and regulations have the primary purpose of influencing digital competition; they may be the product of domestic interests seeking other goals, but the result is to create a particular context for U.S., Chinese, and other offerings that can favor one competitor.

On-the-Ground Presence and Local Training and Workforce Development Programs

Another important factor involves the ways Chinese or U.S. government and private-sector activities can create a local presence that embeds them in the countries and communities. Such a presence can build relationships, create a stronger basis for private-sector partnerships, provide critical knowledge about local conditions and political realities, and offer jobs and other benefits to people in the target countries (in some cases, through corrupt elite capture). Outside influencers with a stronger presence in the country gain various competitive advantages in seeking digital network influence.

This factor came up in interviews and many case studies. Chinese firms, for example, build relationships in target countries, such as Huawei's Seeds for the Future and One Thousand Dreams projects.[81] Chinese firms are training thousands of workers in dozens of developing countries through such programs.[82] One recent assessment of investments in digital technologies in Indonesia concluded that local knowledge can magnify—or undermine—advantages in the other factors: "Success ultimately hinges on nuanced local knowledge and relationship-driven commerce . . . so even the most capable Chinese technologists struggle without strong domestic networks and a deep understanding."[83]

---

[78] Freedom House, "Costa Rica."

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

[80] Chilukuri and Scanlon, *Countering the Digital Silk Road: Kenya*, p. 2.

[81] Haxhixhemajli, "The Western Balkans and China's Digital Silk Road," p. 5.

[82] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 29. For country-specific examples, see Chilukuri and Scanlon, *Countering the Digital Silk Road: Kenya*, pp. 9, 12–13; Chilukuri and Scanlon, *Countering the Digital Silk Road: Indonesia*, p. 10.

[83] Shao, "Southeast Asia Capital and Companies Eye China AI Development, Similar to the Internet Era."

China gains leverage from its complex ecosystems of engagement with many countries, including diplomats, private-sector staff working in countries, visiting military cooperation delegations, local cultural engagements (such as Confucius Institutes), journalists, and other personnel who either live in or visit countries with whom China is trying to develop strong digital connections. China still faces roadblocks to influence despite its local presence, and indeed that presence can sometimes backfire—for example, when Chinese firms mistreat local workers. But when properly conceptualized and handled, this local engagement can provide critical support to China's digital network advantages.

China tends to view such relationships strategically, using its ecosystems of engagement to build this local presence over time. The U.S. government has tools to achieve the same goals, such as local foreign service and commercial service officers and training grants to sweeten subsea cable bids,[84] but investments in these areas of public-sector presence have been declining over time. Meanwhile, private-sector firms make decisions based on business opportunities rather than centralized strategies for achieving long-term influence. In some cases, such as Nigeria, U.S. firms have pulled back from investments that had the potential to enhance U.S. presence. Private-sector incentives simply will not adequately compete with a state-led ecosystem strategy that can make technically and financially unproductive investments to curry favor with governments.

Elite Co-Optation

The final factor governing outcomes in digital network competitions involves efforts to cultivate influence with or control over specific high-profile actors within a society. These efforts can be systematic, through a broad-based effort to compromise key decisionmakers in a society, but, in most cases, they are far more targeted. Outside actors—in this case, given U.S. legal constraints, largely China—can target specific individuals critical to discrete decisions or ongoing policy and curry favor through legal and illegal means. In its widest sense, this factor represents a sort of clientelism pursued from abroad, in which a foreign patron builds a network of local clients (e.g., politicians, military officers, businesspeople) who are financially dependent on or loyal to the foreign power.

This factor overlaps significantly with others. The status of institutionalization and legal constraints on such co-optation will affect the potential for outsiders to use such tactics. Ecosystems of influence provide multiple avenues for co-optation. And an ongoing presence on the ground gives opportunities for cultivating relationships.

China has pursued such tactics through a variety of means. Some are very direct, such as bribery, blackmail, or forms of coercive pressure threatening an actor's political status or a firm's business.[85] Some are more indirect, such as offering business opportunities to firms, making investments in projects of special interest to the target individual, or promoting scholarships that could benefit their

[84] U.S. Southern Command, "Partnership with Costa Rica to Establish Cyber Security"; Brock, "U.S. and China Wage War Beneath the Waves—over Internet Cables."

[85] There is a substantial literature cataloging China's practices of this sort. See, for example, Brands, "China's Foreign Policy Weapons"; Hillman, "Corruption Flows Along China's Belt and Road"; and Gamarra and Popova, "How China Uses 'Geostrategic Corruption' to Exert Its Influence in Latin America." As part of Xi's anticorruption drive, new Chinese laws threaten theoretical penalties for some of this behavior, but it is too soon to know what effect this might have on the practice. See Huld and Liu, "China's Draft Anti-Cross-Border Corruption Law—How Will It Affect Foreign Companies?"

children or the children of political allies. In one case, Huawei paid for and hosted an exclusive party for Costa Rican officials, courting those responsible for managing public contracts.[86] China regularly runs tours, training programs, conferences, and other visits to bring thousands of people from developing countries to China; participation in these activities can be offered as a benefit. China has appointed local officials to important telecommunications posts in its local investments, provided academic scholarships for study abroad to the children of key officials and private-sector leaders, engaged in direct payoffs, provided investments favored by local officials and business partners, and more.[87]

This factor is not universal. Even in some developing countries, as we learned from our interviews, it is not a major element in China's strategy. But in some contexts, it can combine with other elements of China's competitive ecosystem to provide critical advantages in gaining access to digital networks.

Overall Lessons: A Contest Led by the Match of Technology Offerings and Local Needs

These factors combine and mix in different ways in different contexts. Every country's digital network landscape is unique, and, for each, some factors will be more decisive than others. But our research suggests that these nine variables provide a useful starting point for understanding the considerations that will determine future digital network competition outcomes.

Of the more significant factors, cost, geopolitical alignment, and China's ecosystem strategy recurred most insistently across the evidence we reviewed, were named in nearly every case, were raised unprompted in most interviews, and were treated in the literature as the considerations that most often frame a third country's deliberations. Taken together, they account for the lion's share of what our sources offered by way of explanation for third-country decisions on digital networks, although, as noted at the outset of this chapter, the three are difficult to disentangle in practice because concessional financing is itself an instrument of the ecosystem strategy, and alignment shapes which offers a country will entertain at all. Geopolitical alignment appeared to override many if not all other variables in some cases, as in some telecommunications decisions made by advanced democracies. Cost is a leading consideration for most developing nations. China's ecosystem strategy gives Beijing the opportunity to offer end-to-end solutions in some areas and provides a unique source of influence through the synergy of many factors.

These factors have one overriding implication for U.S. national security strategy. Left to the simple influence of market dynamics and the incentives and capacities of U.S. private-sector actors, the United States will remain at a structural disadvantage in competing for positions in digital networks going forward. Currently, historical influence in such areas as standards setting combined with continued technological leadership in such areas as AI and space has checked enough of the other factors here to keep China from gaining decisive advantage in areas besides 5G. But as those

[86] Martínez-Fernández and Engle, "Costa Rica's Cautionary Tale of Chinese Engagement."

[87] Several interviewees referenced such experiences. See also Chilukuri and Scanlon, *Countering the Digital Silk Road: Kenya*, pp. 3, 8; Chilukuri and Scanlon, *Countering the Digital Silk Road: Indonesia*, pp. 1, 5; Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 27.

technology advantages narrow thanks to China's immense structural investments in related technology and industrial sectors, China's strengths in many of these factors will increasingly come into play, and the United States and other democracies may have an increasingly difficult time competing in these networks.

The dynamism and technological prowess of the U.S. private sector, and that of other leading democracies, in many of the components of digital networks—combined with geopolitical factors and the growing unwillingness of many countries to leave themselves entirely dependent on either China or the United States in the digital realm—will keep the United States competitive to some degree for the indefinite future. But one major lesson of this analysis is that China is investing heavily in many tools of statecraft designed to address most or all of the factors on our list and, over time, risks creating a structural asymmetry in which Chinese firms increasingly have an advantage. Our research suggests that, to remain competitive, the United States government will have to take a more active role in building its approaches to maximize these factors and create a context in which the U.S. private sector can compete. We examine several elements of such an agenda in the next chapter.

Chapter 4

Designing a U.S. Strategy for Success

This analysis was designed primarily to identify the most important factors governing success in digital network competitions, and the previous chapter reviewed those findings. That list and those conclusions carry lessons for U.S. strategy in the digital competition. They point to areas in which the United States needs to improve its approach if it wants to compete effectively over the long term. In this chapter, we review some of the overarching insights of this work and list a few leading implications for strategy.

Although we did not undertake a comprehensive net assessment of U.S. and Chinese positions in the contest in digital networks, our research does support a general conclusion about where it stands. China has gained a predominant position in 5G telecommunications networks outside the set of countries that have banned or placed strict limits on Huawei technology. Across the other digital network domains, however, the United States and its allies retain strong positions and world-leading technologies. The competition over leading positions in future AI networks, space systems, and terrestrial and subsea cables remains very much to be determined.

However, our analysis also suggests that, as China invests ever more in its science and technology ambitions and further develops the major sources of its strategic advantages in the digital network competition, there is a real risk that it will gradually, inexorably achieve in additional areas what it has accomplished in 5G. Given current timelines of digital network deployment and the potential lock-in effects they could create—in such areas as 5G and AI ecosystems—the next five to seven years represent a critical time in which third parties will be making important decisions that will tend to align them with U.S. or Chinese networks. The United States needs a comprehensive, integrated, and intensive strategy to promote strong U.S. and allied positions in global digital networks. This is especially true now, as the contest for providing AI capabilities to developing countries is about to heat up and could set the foundations for global digital advantage for decades to come.

The following themes and insights reflect our best judgment of the major policy implications of our analysis—both for navigating the overall U.S.-China competitive landscape and for developing and assessing a U.S. strategy for that competition. As we have noted, that analysis is grounded in extensive data, case studies, a review of existing literature, and interviews with current and former U.S. government officials and private-sector representatives. Nonetheless, our nomination of the variables most critical to the competition constitutes an informed qualitative extrapolation from many specific data points. The themes below derive directly from our analysis, representing our own expert judgment based on the work in the project.

Navigating the U.S.-China Competitive Landscape

By identifying the factors most consistently associated with outcomes in digital network competition, we also uncovered several structural dynamics and relationships that are otherwise obscured by the complexity of these networks.[88] As policymakers navigate the U.S.-China competitive landscape over the next few years, they should take care to weigh these findings and observed patterns—beginning, most importantly, with an appreciation of *the nature of the relative competitive advantages enjoyed by China and the United States in this contest*. In our analysis, we found that China's advantages center on its ability to offer comprehensive, integrated technology packages at very low cost. Specific advantages include the following:

- *Integrated state-backed approach*. The DSR is not merely a collection of projects but a unified, state-supported framework for digital infrastructure export. While the degree of central control and efficient coordination of efforts among China's kaleidoscope of state entities can be exaggerated, this allows for at least a somewhat more comprehensive, top-down strategy that integrates various digital elements under a single brand than the United States can sustain.
- *Cost-effectiveness and speed*. Chinese firms, benefiting from economies of scale and often state subsidies, can offer digital infrastructure solutions at lower costs and with faster deployment timelines compared with many Western competitors. This is particularly attractive to developing nations with urgent infrastructure needs and limited budgets.
- *Comprehensive ecosystem and training*. The DSR provides an integrated digital solution that combines hardware (e.g., 5G, cables, data centers) with software platforms (e.g., AI, e-commerce, smart cities, surveillance technology). Chinese firms also establish training centers and research and development programs, transferring technical knowledge and boosting cooperation between scientists and engineers in recipient countries and their Chinese counterparts. This holistic approach creates a dependency on Chinese technology and expertise.
- *Engagement with overlooked markets*. China has shown a willingness to invest in regions and countries that Western investors have historically neglected or deemed too risky. This includes parts of Africa, the Middle East, Eastern Europe, and Latin America, where the infrastructure financing gap is substantial. This first-mover advantage in underserved markets allows China to build long-term relationships and establish its technological presence.

Relative U.S. advantages in this competition center on the world-leading technology of some of the United States' firms (and allied firms) in key sectors and its continuing, if eroding, status as leader of a multilateral alliance of countries seeking digital autonomy and open standards and norms. Specific U.S. advantages include the following:

[88] For specific examples of these trends, see Appendix A ("A Snapshot of the Competition for Digital Networks in 2026"), Appendix B ("Evaluating the Priority Areas: Factors Influencing Success"), and especially Appendix C ("Country and Functional Issue Case Studies").

- *Private-sector innovation and capital*. The United States benefits from a dynamic and innovative private sector that drives technological advancements and can mobilize substantial capital. U.S. hyperscalers are major owners of undersea cables, and such companies as SpaceX and Amazon are leading the development of advanced low earth orbit satellite constellations for global broadband. This private sector–led approach fosters rapid innovation and significant investment in cutting-edge digital infrastructure.
- *Emphasis on open standards and interoperability*. The United States promotes open, transparent, and secure digital architectures, which foster greater trust and resilience in digital networks. This approach encourages diverse vendor participation and reduces the risk of vendor lock-in, appealing to countries seeking digital sovereignty.
- *Multilateral partnerships and trust*. The United States leverages its extensive network of alliances and partnerships (e.g., Quadrilateral Security Dialogue [the "Quad"], Group of Seven [G7], Blue Dot Network) to promote a collective approach to quality infrastructure.
- *Transparency and governance*. The U.S. approach emphasizes debt transparency, robust environmental and social safeguards, and respect for human rights in infrastructure projects. This provides a stark contrast to criticisms leveled against some BRI and DSR projects regarding debt sustainability and opaque terms.

Taken together, these competing sets of advantages speak to a situation in which China's main tools and approaches risk creating momentum that becomes hard to reverse. At the same time, the United States and its allies benefit from structural and normative advantages that—if U.S. and allied strategy could mitigate some of China's transactional tools—would provide the basis for lasting competitive advantage.

A second broad finding emphasizes the importance of one Chinese advantage: *Financing terms are frequently the consideration that decides adoption in developing countries with significant fiscal constraints*. The lower cost of Chinese technology offerings, partly because of Chinese concessional loans but other sources as well, often makes their solutions the only viable option, especially for 5G and wireless technology products. Coordinated Western multilateral financing could help match these terms and create competitive alternatives, although the problem of Chinese price advantage is larger than loan policies.

However, a third finding modifies the importance of cost and financing vehicles to some degree. Across many countries, *bilateral relationships, security concerns, and domestic legitimacy can override cost considerations when countries have sufficient resources*. Political tensions can render even attractive financial packages unviable, creating market opportunities for aligned providers despite higher costs. Dozens of countries, especially in Europe and Asia, are now concerned about the security and dependency issues of locking themselves into Chinese technology stacks, although the United States is acting in ways that raise parallel concerns about its own digital offerings.

Fourth, *speed of deployment is often an important consideration for countries choosing a main digital partner*. China often prioritizes rapid deployment over deep integration initially, then builds dependency over time. Rather than seeking comprehensive integration from the outset, Chinese firms prioritize speed to deployment, establishing a foothold through quick wins and then systematically building dependency through the unglamorous work of maintenance contracts, system upgrades, and cross-sectoral linkages that build over time. Such temporal sequencing creates the credible offer of

"digital sovereignty" that emphasizes partner control and autonomous decisionmaking, even as the technical architectures being deployed preserve various forms of Chinese backdoor access. The strategy operates in sequence: Velocity opens doors that would otherwise remain closed to more-demanding partnerships; depth follows once presence is established.

Fifth, *procurement decisions depend on sustained engagement*. Where U.S. diplomatic and commercial presence diminishes, Chinese options encounter less competition, allowing Beijing to shape perceptions. One of China's major advantages is supporting greater on-the-ground presence in the form of private-sector representatives, the equivalent of a digital-sector government representative, engagement with regular diplomats on these issues, and training programs that build local ties—especially in such countries as Nigeria that are experiencing diminishing engagement from U.S. and Western companies.[89]

A sixth overall finding suggests that *narratives determine some choices within constrained opportunity sets and shape willingness to overcome constraints*. Governments derive authority from different sources (e.g., developmental performance, democratic representation, anti-colonial identity), and fiscal or geopolitical pressures rarely eliminate all options, only narrow them. When both Chinese and Western financing exist but on different terms, regime legitimacy foundations tend to predict adoption. Performance-legitimacy regimes tend to embrace China's "rapid modernization" framing and accept debt dependencies. In contrast, representation-based governments are most likely to accept U.S. cost premiums when "democratic technology" and "capacity-building" narratives align with domestic political coalitions. An effective narrative strategy requires diagnosing how target governments justify their authority and aligning specific offerings to the most-compelling narratives, which the United States has heretofore achieved in the competition over undersea cables—for example, by combining diplomatic engagement with technical grants.[90]

Seventh, *when the United States and its allies are absent in key decision windows, that can give China a temporary narrative and competitive monopoly on specific choices*. Infrastructure choices concentrate in discrete moments, such as crisis-driven procurement, national plan cycles, and major policy shifts, when governments actively solicit options and weigh alternatives. A sustained presence ensures visibility during these windows; absence means that countries never consider alternatives because they are unaware of their existence or lack the relationships to pursue them. Where U.S. engagement has lapsed, Chinese vendors become the sole source of information about technological possibilities, cost structures, and implementation timelines, creating uncontested narratives not through superior messaging but through informational monopoly.

An eighth overall finding is that *most countries, even some U.S. allies, find both strategic and technological value in adopting a middle road between U.S. and Chinese digital architectures*. In some cases, a third country may strengthen its resilience by diversifying toward trusted allied or domestic providers rather than U.S. firms specifically; such outcomes still advance the shared U.S. and allied goal of preventing coercive Chinese dependence, even in cases in which they do not increase U.S. market share. Overall, countries enjoy considerable flexibility in mixing Chinese and Western components across infrastructure layers. They can adopt Chinese hardware alongside Western

[89] See Appendix C.

[90] See Appendix C.

software or deploy Chinese solutions in less sensitive sectors while adopting Western technologies for critical systems. The modularity suggests that China's success may not require the wholesale vendor dominance that characterized earlier technological competitions but rather a sufficient presence across enough layers to maintain influence even within hybrid ecosystems. Whether such presence translates into meaningful strategic leverage, however, remains an open question.

Ninth and finally, *the competition has a significant human dimension, which China regularly attempts to use for competitive advantage*. Third-country officials responsible for digital infrastructure decisions often maintain cross-sectoral relationships with Chinese counterparts developed through prior collaborations—relationships that create subtle but potentially consequential path dependencies. When a transport minister with years of productive Chinese engagement assumes responsibility for digital infrastructure, for example, the question becomes whether these prior relationships facilitate smoother cooperation or create blind spots that enable dependencies to accumulate unchecked. Whether such relationships constitute decisive factors or marginal influences in shaping digital infrastructure choices remains, in most cases, an open empirical question.

The competition for digital networks is heating up and entering a critical period. China enjoys some structural advantages that it has created through conscious government policy, which risk generating momentum for Chinese offerings across a wider range of these networks. Accordingly, U.S. policymakers need to counter these trends while maximizing the United States' own sources of strength. However, a deeper understanding of these advantages and weaknesses is insufficient. The final question for the United States is what can it do about these risks.

Developing and Assessing a U.S. Strategy for Digital Network Competition

One thing our research made clear is that the United States lacks a clear, objective set of criteria to determine the degree to which it is succeeding and failing in this competition. We did not set out to develop such criteria, and our research did not generate specific thresholds of success. As noted in Chapter 2, any concept of success or failure must be both absolute and relative and must accept the fact that the United States will not be able to shut China out of these domains. The global digital network balance of influence will likely become and remain a complex, nuanced affair, with each side owning significant advantages in different sectors.

Nonetheless, our work does suggest at least an initial roster of criteria to use when gauging the status of the competition. Table 2.1 (summarized below as Table 4.1) outlined three categories of success and potential constituent elements of each.

Table 4.1. Categories and Elements of Success in the Digital Network Competition

Dimension	U.S. Success	Chinese Success
Instrumental	• Diverse and resilient supply chains • Adoption of open standards and norms • Sustainable and transparent development	• Chinese standards, platforms, and suppliers dominate critical nodes • Diversification pathways foreclosed
Relational	• United States and West as trusted partners • Capacity-building benefits local populations and skills development • Regulatory alignment results in closer bilateral ties	• China viewed as more reliable • Local populations develop skills aligned only with Chinese digital ecosystems • Partners adopt data governance models compatible with Chinese approaches
Strategic	• Digital sovereignty for third countries • Adversaries unable to extract intelligence through infrastructure control • Partners possess capacity to resist coercion	• Diminished U.S. influence results in erosion of digital freedoms • Strategic vulnerabilities enabled (e.g., espionage, data control, breaches) • Beijing gains visibility into partner operations • Partners vulnerable to coercion

Using those initial concepts and the further analysis of the study, we suggest six criteria for measuring success or failure in U.S. strategy on this issue. We outline these criteria below, along with potential metrics for assessing each:

- *The measurable balance of U.S. and allied versus Chinese positions in third-country digital networks.* One obvious metric would rely on basic data on the relative level of U.S. and Chinese presence in the various components of digital networks. How many countries use Huawei for 5G (or Chinese versus U.S. or European firms for 6G)? Who is building the most subterranean and subsea cables or hosting the most satellite services? Basic numbers can mislead, but significant trends can give a sense of the general trajectory of the contest. *Metric: Data on relative positions in major components of third-country digital networks.*
- *Digital sovereignty for third countries.* The United States wants to avoid a situation in which key countries become so dependent on Chinese digital technologies that it creates an analog to the rare earths situation—one in which China can threaten catastrophic outcomes by withholding continued digital cooperation. Some of this risk will inhere in any relationship, but the United States can assess the potential for switching, develop alternatives, and help third countries address these dangers. *Metric: An index that would combine percentage of use of one provider's technologies along with switching versus lock-in factors and the demonstrated use of dependencies for leverage.*
- *Multilateral emphasis on open standards and norms based on U.S. and allied technology platforms.* The United States wants to avoid a situation in which China begins to dominate standard- and norm-setting processes in digital networks. *Metric: A roster of leading norms and standards in digital networks and institutions that develop them, along with an index that assesses which norms and standards derive from Chinese technology or policy and the degree of Chinese presence in these institutions.*

- *Erosion of digital freedom and movement toward restrictive versions of "digital sovereignty."* The United States would seek to avoid the adoption of "cyber sovereignty" models that enable filtering, content moderation, and spying. *Metric: An annual survey of the digital network policies and positions of a representative set of 30 or 40 third countries, along with ratings of digital freedom versus closure.*
- *Data and information security*. The United States would seek to avoid a situation in which Chinese digital network buildouts give it access to basic data for AI training or sensitive information about other societies from third parties. *Metric: A roster of Chinese technology positions in 30 or 40 representative third countries along with an assessment of the potential that those positions provide for intelligence-gathering and data access, matched with an annual review of anecdotal reports of Chinese information and data retrieval.*
- *Human capital alignment.* The United States would seek to avoid a situation in which third countries' technical workforces are predominantly trained on Chinese platforms, educated at Chinese universities, or certified through Chinese corporate programs, such as Huawei's ICT Academy, thereby developing institutional and professional affinities that favor Chinese technology adoption over time. *Metric: A comparative index of U.S. and allied versus Chinese training, scholarship, and certification programs operating in a representative set of third countries, including enrollment figures, the number of graduates placed in government or critical infrastructure roles, and the degree to which training curricula are tied to specific vendor ecosystems.*

The key question then becomes how to measure the acceptable threshold in any of these criteria. Just what degree of overall measurable balance in digital network positions can serve U.S. interests? How much dependency in strategically critical countries is too much? What forms of digital authoritarianism would directly threaten U.S. interests? We did not set out to answer those questions in our study. To develop a coherent strategy for this competition, though, U.S. officials need to develop at least rough ideas on each of those areas.

The resulting ideas of sufficiency must be appropriate to a contest in which many third countries will inevitably be engaging in hedging behavior. U.S. strategy has to assume that many countries will be seeking some degree of balance in their digital architectures and measure success accordingly. Any U.S. approach cannot be premised on demanding exclusive alignment; it must offer sufficiently compelling value propositions that make deeper U.S.-oriented integration the preferred choice rather than the imposed one.

Turning then to the elements of a strategy to compete,[91] a first and obvious priority is to *develop the institutional and policy elements of a more integrated strategy, to match China's holistic approach*. As we have seen, a core aspect of China's approach is to offer turnkey solutions with many coordinated technology, infrastructure, and training solutions. The United States cannot defend its interests in this competition by continuing to invest exclusively in frontier technological excellence while neglecting the deployment, financing, and partnership architecture needed to get good-enough technology adopted at scale across the Global South before Chinese alternatives become entrenched.

[91] Chilukuri and Scanlon, *Countering the Digital Silk Road*, pp. 61–67, contains an excellent and detailed set of proposals for a stronger U.S. strategy for digital network competition. Here, we focus on the key elements that our analysis emphasized most strongly.

Moving toward such a capacity for synergistic digital network offerings demands at least two things: (1) a formal, national-level strategy for global digital network competition and (2) an office in the U.S. government—perhaps in the White House Office of Science and Technology Policy, with interagency input from other bodies, such as the National Security Council—empowered to develop public-private strategic engagements to achieve this goal. As the recent CNAS study made clear, the United States has many pockets in various departments, agencies, and specific programs that can empower digital network competitiveness, but "these tools suffer from a lack of coordination and strategic focus."[92]

The primary goal of an office or function in this institutional sense would be to coordinate among the variety of departments and agencies and the offices within them. It would also raise key roadblocks to policy effectiveness to senior leadership for action. Given the large number of functions across departments and agencies that touch on these issues, it is very unlikely that such a coordinating office would have formal authority to direct outcomes. In this sense, it would sit above those departments and agencies in its involvement of and engagement with the most-senior decisionmakers, but its role is still to coordinate. It would not, for example, take over from such offices as EXIM or the Office of Strategic Capital the task of negotiating specific agreements. Another critical role for such an office would be to develop criteria for strategic investment and long-term strategies for digital network competition that incorporate definitions of success and theories of victory. As of now, one expert has noted, "There is no permanent institution that identifies where strategic capital should flow, determines which agency is best positioned to provide it, and specifies with what instrument."[93]

Second, *the United States and its allies need to invest more heavily in mechanisms and institutions able to address the cost and financing aspects of this competition*. If China's industrial capacity and practices, labor cost advantages, and subsidization and financing efforts make their options vastly cheaper than U.S. and allied technologies, the United States will be running uphill in this contest. One option would be to create digital network programs in both the U.S. International Development Finance Corporation (DFC) and EXIM designed to match any offer from China within 5 to 10 percent. Because of the elaborate and sometimes unfocused agenda of those organizations, however, it might be better to create a single new program with a narrow specialty for this issue. As noted in the previous chapter, China's digital cost advantages come from many sources, not only direct subsidies and concessional loans.

Still, the United States and its allies could do much more to level the playing field. This would primarily involve stronger funding and more-coordinated strategies for DFC and EXIM. The December 2025 DFC reauthorization has already raised the contingent liability ceiling from $60 billion to $205 billion, authorized a $5 billion equity revolving fund at the U.S. Department of the Treasury, and explicitly prioritized telecommunications and digital network deals as a priority. Remaining gaps tend to cluster around such issues as continued risk aversion, slow procedures, limited sector expertise, and insufficient origination capacity. Several added policy changes could build on those steps and help close implementation gaps, including an acceleration of actual projects by taking

[92] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 63.

[93] Jaro, "Closing the Strategic Capital Gap," p. 191.

advantage of the reauthorization's embrace of a greater risk appetite;[94] expanding DFC authority in additional sectors, such as public-sector projects; fully funding the $5 billion Treasury equity capacity and using it for catalytic investments; raising EXIM's lending cap; creating DFC investment liaisons in important embassies; forming a digital network specialist team within DFC with sector expertise; developing a lending authority with broader remit than EXIM's current portfolio; and more strongly coordinating lending and investment support with broader U.S. instruments of power that could improve the capacity of these U.S. tools.[95] Parallel policy changes at EXIM could ease U.S. content and shipping rules to expand its potential to support projects and consciously target a given proportion of its lending to digital network projects.

Third, *the United States should develop more tightly integrated strategies that coordinate the activities of U.S. and allied governments and firms*. Competing with a country with China's scale and capacity is difficult even for the United States. Moreover, in some fields, such as 5G and subsea cables, European and Japanese firms are world leaders. A combined allied effort—to coordinate integrated technology offerings, pool resources to match Chinese prices, and offer on-the-ground training and postdeployment support—would offer force multipliers to U.S. efforts in important ways.[96] Achieving such coordination will likely require formal institutional actions; CNAS has recommended merging DFC, EXIM, and other agencies with related missions into a U.S. Partnership Agency.[97] Whether through such formal bureaucratic reform or through much tighter interagency synergy, or perhaps through a DFC and EXIM shared office on digital network competition, greater coordination among these agencies and with the larger U.S. government is an essential step toward long-term success.

Fourth, *the United States should develop a capacity for stronger on-the-ground presence and postdeployment training and workforce development efforts.* As noted in our analysis, some U.S. technology firms have already undertaken training programs to help develop workforces in several countries. The U.S. government could develop a new category of public service officer to specifically support digital network alliances abroad: digital service officers, much like commercial service officers for digital networks.[98] This career line could be established within the Department of State or, in the commercial service parallel, the Department of Commerce. They would have expertise and training in relevant digital areas, be connected to the coordinating office for digital network competition, and, similarly to commercial service officers, work in strategically important embassies to coordinate U.S. policy and strategy toward the host government in relevant issues.

In both public and private forms, these linked public-private efforts would be designed to achieve several goals: support U.S. and allied firms in winning contracts, train and align local workforces to

---

[94] Thibaut and Ben-Avie, "DFC Reauthorization Is Here."

[95] For a detailed examination of potential DFC reforms related to the energy sector (but with principles that readily apply to digital network investments), see Burns, "A US Strategy for Energy Competition with China in Emerging Markets." On EXIM reforms, see Gebhart, "Revitalizing the Export-Import Bank for Great Power Competition," pp. 173–187; and Jaro, "Closing the Strategic Capital Gap," pp. 188–199.

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

[97] Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 3.

[98] The CNAS study recommends creating such positions, calling them *foreign technology officers* (Chilukuri and Scanlon, *Countering the Digital Silk Road*, p. 4).

U.S. and allied technology, and build relationships with local firms and ministries in the digital space. Such local-sector experts could help close an especially important gap—the fact that U.S. investment offers sometimes come late to the process, after Chinese firms and agencies have been negotiating and seeking influence for some time. Local digitally focused teams could anticipate future procurement decisions and ensure that U.S. and allied offerings are competitive from the beginning.

Fifth, *the United States should build on existing efforts to establish coalitions of like-minded nations pursuing open, autonomous norms for digital networks*. This effort would build on existing U.S. efforts to establish norm-based coalitions promoting openness, transparency, and information security in digital networks. The most significant of these has been the Clean Network initiative, which represented an effort to promote a set of digital-trust principles, including transparency, accountability, and rule of law, and by late 2020 had recruited commitments from more than 60 nations and some 200 telecommunications companies. Similar efforts underway include the Prague Proposals, a multinational effort begun in 2019 to promote open and transparent norms for telecommunications networks.[99] A U.S. digital network strategy could expand on those efforts and make a new push to establish clear norms and to create a set of countries aligned in the core standards of future digital networks. Because so many states are playing both (or all) sides in this contest, such an effort cannot seek to establish a totally exclusive block. But it can serve as an important tool in shifting the global playing field somewhat in the U.S. direction.

Such an effort could be catalyzed by a specific multinational initiative, such as a Trusted Digital Network Standard, which would develop a series of shared norms for such networks and offer various advantages for countries voluntarily participating. It could offer formal, trusted network certification for participating countries and firms, criteria for assessing risk from suspect providers, and preferential access to financing and technology for member states. The United States could link the initiative to expanded development finance tools as suggested above, using its expanding financial leverage to reward countries and firms that voluntarily join the network. It could begin to work more technical aspects of future standards, such as setting up a caucus of aligned countries and companies coordinating positions in future 6G telecommunications (with organizations including 3GPP, the O-RAN Alliance, ITU, and the Institute of Electrical and Electronics Engineers) to develop shared norms that provide the basis for future 6G standards.

In the process, the United States will need to address concerns that it uses its own cyber capabilities and digital access to steal information and gain leverage over third parties. The strategy we have outlined is predicated on the broad notion that the United States and its friends and allies can position themselves as a safer, more reliable alternative to China in this competition. Doing that while closing the gap on such factors as affordability and local presence can put the United States in a better competitive position. But achieving that outcome will require the United States to agree to some clear constraints on its own use of digital network access for clandestine or coercive purposes.

If the United States takes these five steps—better organizing itself for offering integrated technology options, making U.S. and allied options more cost competitive, aligning its efforts more closely with allies, creating a better local presence, and revitalizing global norm-building efforts—and combines them with the natural U.S. competitive advantages noted above, it can better achieve its

[99] Reddy and Soni, *Is There Space for a Digital Non-Aligned Movement?*

overall objectives in the digital network competition. This approach would mitigate China's advantages while building on those of the United States', taking advantage of the fact that the United States has much more leeway to match China's competitive advantages than China does to match those of the United States'.

The next decade may offer a fresh opportunity for the United States to improve its position in the contest for global digital networks. In some technology areas, such as subsea cables, an existing U.S. and allied strong position could be further improved. In other areas, such as telecommunications, the emergence of next-generation technologies (such as 6G) in which standards and vendor relationships remain unset offers an opportunity to take market share from Chinese firms. The United States and its allies retain tremendous competitive advantages in this contest. Relatively modest improvements to the structure of U.S. competitive strategy could make a significant difference in outcomes, but time is of the essence.

Abbreviations

3GPP	3rd Generation Partnership Project
AI	artificial intelligence
BRI	Belt and Road Initiative
CNAS	Center for a New American Security
DFC	U.S. International Development Finance Corporation
DSR	Digital Silk Road
EXIM	Export-Import Bank of the United States
FCC	Federal Communications Commission
GPS	Global Positioning System
GPU	graphics processing unit
ICE	Instituto Costarricense de Electricidad
IoT	Internet of Things
ITU	International Telecommunication Union
PNT	positioning, navigation, and timing
RAN	radio access network
VC	venture capital

References

Alejandro, Omid, "Why English-Based Programming Languages?" Medium, November 14, 2018. As of August 27, 2026: https://medium.com/@omidalejandro/why-english-based-programming-languages-be53a3ad03aa

Anand, Ram, "Malaysia Taps Chinese Investors to Build More Data Centers," Bloomberg, June 26, 2024.

Artha, Katherine, Jason Callahan, John Chen, Jessica Drun, Ed Francis, Kieran Green, Brian Lafferty, Joe McReynolds, James Mulvenon, Benjamin Rosen, and Emily Walz, *China's Smart Cities Development*, SOS International LLC, January 2020.

Bhandari, Amit, Blaise Fernandes, and Aashna Agarwal, *Chinese Investments in India*, Gateway House: Indian Council on Global Relations, February 2020.

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

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

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

Brands, Hal, "China's Foreign Policy Weapons: Technology, Coercion, Corruption," American Enterprise Institute, January 24, 2021.

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

Burns, Steven, "A US Strategy for Energy Competition with China in Emerging Markets," Atlantic Council, April 2026.

Chan, Gerald, *China's Digital Silk Road: Setting Standards, Powering Growth*, Edward Elgar Publishing, 2022.

Cheney, Clayton, "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism," working paper, Pacific Forum, July 2019.

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

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

Chilukuri, Vivek, and Ruby Scanlon, *Countering the Digital Silk Road: Saudi Arabia*, Center for a New American Security, September 2025.

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

"China, Malaysia Explore New Opportunities for AI-Driven Economic, Trade Cooperation," Xinhua, July 31, 2026.

Confino, Paolo, "Malaysia Will Work with Both the U.S. and China in Developing AI, Says Top Minister," *Fortune*, May 28, 2025.

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/

Daniels, Owen J., and Hanna Dohmen, "China's Overlooked AI Strategy," *Foreign Affairs*, July 25, 2025.

Dekker, Brigitte, Maaike Okano-Heijmans, and Eric Siyi Zhang, *Unpacking China's Digital Silk Road*, Clingendael, July 2020.

Dong, Wang, and Gao Dan, "Digital Globalization and China-US Strategic Competition," *China International Studies*, No. 97, November/December 2022.

Dorman, David, "Clear Course for Digital China: 15th FYP Centers on Data," Digital China Wins the Future, March 17, 2026. As of August 27, 2026:
https://digitalchinawinsthefuture.com/digital-china-15fyp-compute-algorithms-data/

Ekman, Alice, *China's Smart Cities: The New Digital Battleground*, French Institute of International Relations, December 2019.

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

Epoch AI, GPU Clusters, database, updated March 13, 2026. As of September 11, 2026:
https://epoch.ai/data/gpu-clusters

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.

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

Gamarra, Eduardo, and Valeriia Popova, "How China Uses 'Geostrategic Corruption' to Exert Its Influence in Latin America," *The Conversation*, May 17, 2023.

Gebhart, Tanner J., "Revitalizing the Export-Import Bank for Great Power Competition," *American Affairs*, Vol. 10, No. 2, Summer 2026.

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.

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

Grewal, David Singh, *Network Power: The Social Dynamics of Globalization*, Yale University Press, 2008.

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

Haxhixhemajli, Arta, "The Western Balkans and China's Digital Silk Road," German Marshall Fund of the United States, January 2025.

He, Alex, "The Digital Silk Road and China's Influence on Standard Setting," Centre for International Governance Innovation, April 2022.

Hillman, Jonathan E., "Corruption Flows Along China's Belt and Road," Center for Strategic and International Studies, January 18, 2019.

Huld, Arendse, and Chenchen Liu, "China's Draft Anti-Cross-Border Corruption Law—How Will It Affect Foreign Companies?" China Briefing, September 10, 2026.

Irwin-Hunt, Alex, "US–China AI Model Costs Diverge," fDi Intelligence, December 10, 2025.

Jagtiani, Sharinee L., *Deep Down in the Stack: China's Entrenchment in Serbia's Technology Landscape*, German Marshall Fund of the United States, June 2025.

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

Jaro, Jan, "Closing the Strategic Capital Gap: The Case for Modernizing the Export-Import Bank," *American Affairs*, Vol. 10, No. 2, Summer 2026.

Jervis, Robert, *System Effects: Complexity in Political and Social Life*, Princeton University Press, 1997.

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.

Klaus, Ian, and Simon Curtis, "The New Corridor Competition Between Washington and Beijing," Carnegie Endowment, April 12, 2024.

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

Kynge, James, "Low-Cost Chinese AI Models Forge Ahead, Even in the US, Raising the Risks of a US AI Bubble," Chatham House, November 20, 2025.

Lambert, Nathan, and Florian Brand, "The ATOM Report: Measuring the Open Language Model Ecosystem," arXiv, arXiv:2604.07190, April 8, 2026.

Lee, Nicol Turner, *Navigating the U.S.-China 5G Competition*, Brookings Institution, April 2020.

Lee, Nicol Turner, "TikTok May Not Be Chinese-Owned Anymore, but There Still Is a Privacy Problem," Brookings Institution, October 2, 2025.

Lehdonvirta, Vili, Boxi Wu, and Zoe Hawkins, "Weaponized Interdependence in a Bipolar World," *Review of International Political Economy*, Vol. 32, No. 5, 2025.

Liu, Xinghua, "Coalition Building and Sino–US Competition in the Digital Era," *Chinese Journal of International Politics*, Vol. 17, No. 4, 2024.

Martínez-Fernández, Andrés, and Allison Engle, "Costa Rica's Cautionary Tale of Chinese Engagement," Heritage Foundation, August 19, 2024.

McMorrow, Ryan, Sam Fleming, Peter Foster, and Joe Leahy, "China Shock 2.0: The Flood of High-Tech Goods That Will Change the World," *Financial Times*, April 14, 2026.

Meadows, Donella, *Leverage Points: Places to Intervene in a System*, Sustainability Institute, 1999.

Meinhardt, Caroline, Sabina Nong, Graham Webster, Tatsunori Hashimoto, and Christopher D. Manning, "Beyond DeepSeek: China's Diverse Open-Weight AI Ecosystem and Its Policy Implications," Stanford University Institute for Human-Centered Artificial Intelligence, December 16, 2025.

Mokhtar, Faris, Mackenzie Hawkins, and Niki Koswanage, "Malaysia Eyes Huawei Chips for AI Project Despite US Warning," Bloomberg, September 7, 2026.

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

Morieson, Nicholas, "How China Is Betting Cheap AI Will Get the World Hooked on Its Tech," *The Conversation*, February 26, 2026.

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

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.

O'Callaghan, Jonathan, "China Has Applied to Launch 200,000 Satellites, but What Are They For?" *New Scientist*, January 14, 2026.

Oreglia, Elisa, Hongyi Ren, and Chia-Chi Liao, "The Puzzle of the Digital Silk Road," in Nargis Kassenova and Brendan Duprey, eds., *Digital Silk Road in Central Asia: Present and Future*, David Center for Russian and Eurasian Studies, Harvard University, June 2021.

Ortiz Freuler, Juan, "'Kill Switch Shield' and the Recurring Erosion of Trust in US Tech," Tech Policy Press, July 28, 2025.

Pannier, Alice, *Software Power: The Economic and Geopolitical Implications of Open Source Software Studies*, French Institute of International Relations, December 12, 2022.

Patil, Sameer, and Prithvi Gupta, *The Digital Silk Road in the Indo-Pacific: Mapping China's Vision for Global Tech Expansion*, Observer Research Foundation, January 2024.

Patil, Sameer, and Prithvi Gupta, *The Digital Silk Road and Smart City Networks in the Indo-Pacific: A Primer*, Observer Research Foundation, September 2025.

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

Reddy, Latha, and Anoushka Soni, *Is There Space for a Digital Non-Aligned Movement?* The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, 2021.

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.

Schwartz, Paul, "Legal Access to the Global Cloud," *Columbia Law Review*, Vol. 118, No. 6, October 2018.

Shahani, Aarti, "A Year After Snowden, U.S. Tech Losing Trust Overseas," National Public Radio, June 5, 2014.

Shao, Grace, "Southeast Asia Capital and Companies Eye China AI Development, Similar to the Internet Era," *AI Proem*, Substack, June 27, 2025. As of August 28, 2026: https://aiproem.substack.com/p/southeast-asia-capital-and-companies

Shaw, Mackenzie, and Ram Anand, "Malaysia Downplays Huawei Deal as US Checks China's AI Reach," Bloomberg, May 20, 2025.

Shen, Hong, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication*, Vol. 12, 2018.

Shi-Kupfer, Kristin, and Mareike Ohlberg, *China's Digital Rise: Challenges for Europe*, Mercator Institute for China Studies, 2019.

Sinha, Satyajit, "State of IoT 2025: Number of Connected IoT Devices Growing 14% to 21.1 Billion Globally," IoT Analytics, October 28, 2025. As of August 28, 2026: https://iot-analytics.com/number-connected-iot-devices/

Stanford University Institute for Human-Centered Artificial Intelligence, "Which Countries Are Leading in AI?" webpage, undated. As of September 11, 2026: https://hai.stanford.edu/ai-index/global-vibrancy-tool

Submarine Cable Networks, "TAM-1," webpage, undated. As of January 25, 2026: https://www.submarinenetworks.com/en/systems/brazil-us/tam-1

Thibaut, Kenton, and Jochai Ben-Avie, "DFC Reauthorization Is Here: The Good, the Bad, and the Next Steps for Connectivity," Digital Forensics Research Lab, Atlantic Council, January 23, 2026.

Thibaut, Kenton, Iria Puyosa, and Konstantinos Komaitis, "AI Cooperation Under the Shadow of China's Digital Silk Road," Digital Forensic Research Lab, Atlantic Council, February 25, 2026.

TikTok Inc. v. Garland, 604 U.S. 56, 2025.

U.S. Government Accountability Office, *Critical Infrastructure: Actions Needed to Better Secure Internet-Connected Devices*, GAO-23-105327, December 1, 2022.

U.S. Southern Command, "Partnership with Costa Rica to Establish Cyber Security," press release, August 22, 2023.

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.

Wooden, Andrew, "Huawei Makes RAN Gains in Several Global Regions," Telecoms.com, February 20, 2026.

Wu, Xiangning, "Technology, Power, and Uncontrolled Great Power Strategic Competition Between China and the United States," *China International Strategy Review*, Vol. 2, 2020.

Yeoh, Kenson, and Dingding Chen, "China-US Competition: Who Will Win the Digital Infrastructure Contest?" *The Diplomat*, December 21, 2022.

"Your Expert Guide to the Debate over Banning TikTok," *New Atlanticist* blog, January 9, 2025. As of August 28, 2026: https://www.atlanticcouncil.org/blogs/new-atlanticist/your-expert-guide-to-the-debate-over-banning-tiktok/

Zimmermann, Antonia, and Koen Verhelst, "German Ministers Dash to China in Bid to Escape Retaliation over EV Duties," *Politico*, June 27, 2024.

About the Authors

Michael J. Mazarr is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. At the time of writing, he was a senior political scientist at RAND. He specializes in U.S. national security strategy, AI and national security, U.S.-China relations, and broad issues of national competitiveness. He holds a Ph.D. in policy studies.

Habiba Ahmed is a policy analyst at RAND. Her research interests include the U.S.-Philippines alliance, Indo-Pacific strategy, the foreign military sales process, security cooperation, and U.S. strategy for countering weapons of mass destruction. She holds an M.A. in communication science.

Marzia Giambertoni is a policy analyst at RAND. Her research interests include Middle East defense and security issues, security cooperation and AI and emerging technology cooperation, and non-state groups. She holds an M.P.A.

Shea Henderson is a Chinese-language specialist research assistant at RAND. His research interests include U.S.-China competition, the intersection of economics and national security, and Chinese industrial policy. He holds a B.S.B.A. in finance and international business.

Robert Ulrich Nagel was a political scientist at RAND. He has worked on projects related to manpower analysis, U.S. Army force posture in Europe, sexual harassment and assault in the Coast Guard, the Integrated Primary Prevention Workforce, and the implementation of the Women, Peace and Security Act. He hold a Ph.D. in international conflict analysis.

Christian Trotti is a defense analyst and a co-lead of the National Security Research Division's Strategic Forces and Deterrence Initiative at RAND. His research interests include defense strategy, nuclear deterrence, and military technology. He hold an M.A. in security studies.