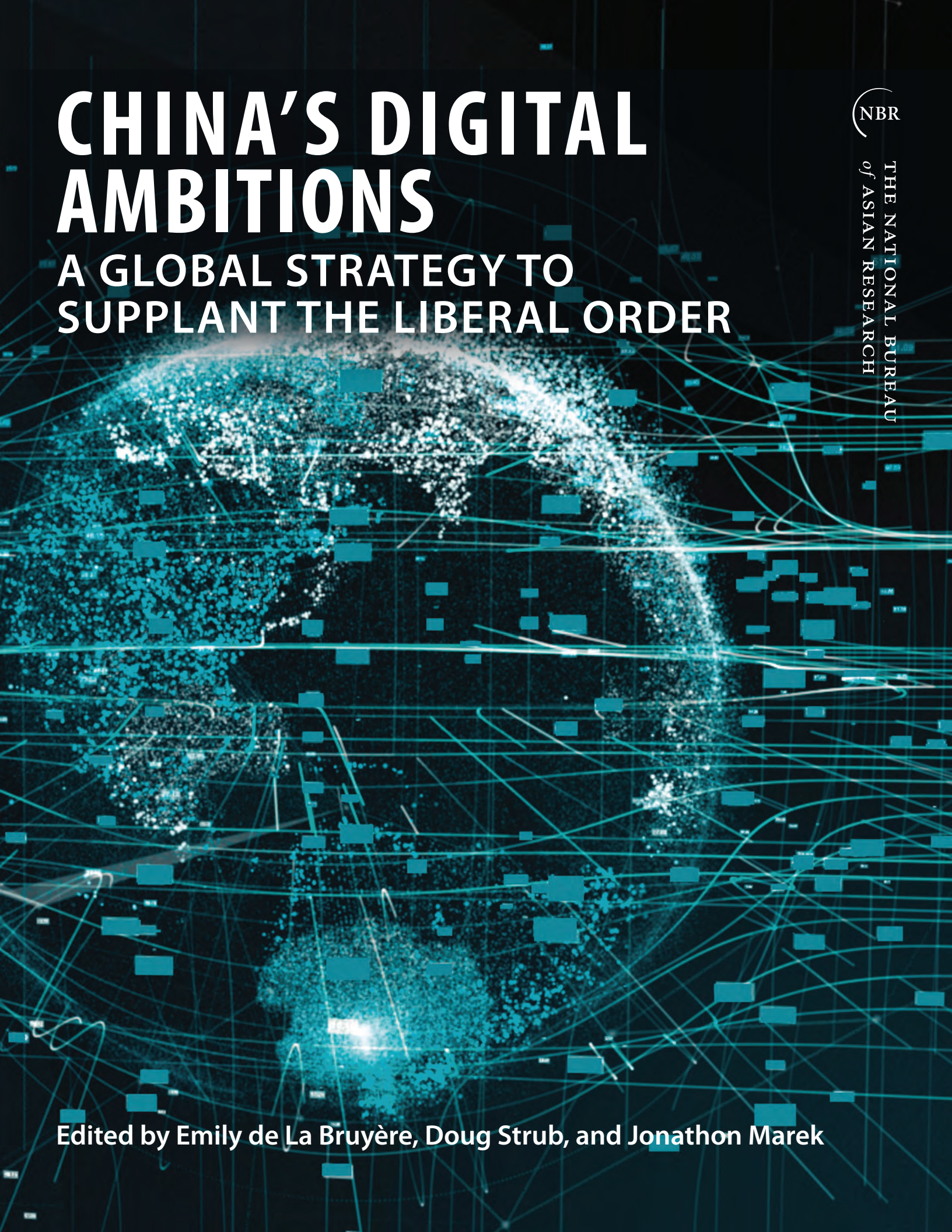
CHINA'S DIGITAL AMBITIONS

A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER



NBR

THE NATIONAL BUREAU *of* ASIAN RESEARCH

Edited by Emily de La Bruyère, Doug Strub, and Jonathon Marek

NBR Board of Directors

John V. Rindlaub
(Chair)
Regional President (ret.)
Wells Fargo Asia Pacific

Thomas W. Albrecht
(Vice Chair)
Partner (ret.)
Sidley Austin LLP

Roger W. Bowlin
Founder and Managing Partner
Real Estate Transition Solutions

Norman D. Dicks
Senior Policy Advisor
Van Ness Feldman LLP

Richard J. Ellings
President Emeritus and Counselor
NBR

Kurt Glaubitz
(Vice Chair)
General Manager, Corporate Affairs
Asia Pacific Exploration and Production
Chevron Corporation

Charles Hooper
Senior Counselor
The Cohen Group

Roy D. Kamphausen
President
NBR

Nobukatsu Kanehara
Professor
Doshisha University

Ryo Kubota
Chairman, President, and CEO
Kubota Vision Incorporated

Quentin W. Kuhrau
(Treasurer)
Chief Executive Officer
Unico Properties LLC

Melody Meyer
President
Melody Meyer Energy LLC

Long Nguyen
Chairman, President, and CEO
Pragmatics, Inc.

Kenneth B. Pyle
Professor, University of Washington
Founding President, NBR

William Rademaker
Entrepreneur
Duthie Hill LLC

Jonathan Roberts
Founder and Partner
Ignition Partners

Tom Robertson
Vice President and
Deputy General Counsel
Microsoft Corporation

Joseph E. Tofalo
Vice President, Engagement and
Customer Affairs
Huntington Ingalls Industries, Inc.

Mitchell B. Waldman
Principal
M Barnet Advisors LLC

Honorary Director

George F. Russell Jr.
Chairman Emeritus
Russell Investments

NBR Chairs and Counselors

Charlene Barshefsky
U.S. Trade Representative (ret.)

Charles W. Boustany Jr.
U.S. House of Representatives (ret.)

Norman D. Dicks
U.S. House of Representatives (ret.)

Richard J. Ellings
NBR (ret.)

Thomas B. Fargo
Admiral, U.S. Navy (ret.)

Aaron L. Friedberg
Princeton University

Jonathan W. Greenert
Admiral, U.S. Navy (ret.)
John M. Shalikashvili Chair

Ashley J. Tellis
Carnegie Endowment for
International Peace

NBR Board of Advisors

William Abnett
NBR

Se Hyun Ahn
University of Seoul

Dennis C. Blair
Admiral, U.S. Navy (ret.)

Ketty Chen
Taiwan Foundation for Democracy

Josh Corless
ConocoPhillips

Linda Distlerath
PhRMA (ret.)

Nicholas Eberstadt
American Enterprise Institute

Karl Eikenberry
Former Ambassador (U.S.);
Lt. General, U.S. Army (ret.)

Bates Gill
Macquarie University

Clara Gillispie
NBR

Stephen Hanson
College of William and Mary

Harry Harding
University of Virginia

Mikkal Herberg
University of California San Diego

Carla A. Hills
Hills & Company

Robert Holleyman
C&M International

Chun In-Bum
Lt. General, ROK Army (ret.)

Mark Jones
Wells Fargo

Amit Kapoor
India Council on Competitiveness

Tariq Karim
Former Ambassador (Bangladesh);
Independent University

Heino Klinck
U.S. Army/Department of Defense (ret.)

David Lampton
Johns Hopkins University

Stephen Lanza
Lt. General, U.S. Army (ret.)

Nicholas Lardy
Peterson Institute for International
Economics

Richard Lawless
New Magellan Ventures

William McCahill
Department of State (ret.)

Meredith Miller
Albright Stonebridge Group

John S. Park
Harvard Kennedy School

Pamela Passman
APCO Worldwide

Rajeswari Rajagopalan
Observer Research Foundation

Clarine Nardi Riddle
Kasowitz, Benson, Torres
& Friedman LLP

Ryo Sahashi
University of Tokyo

Ulrike Schaede
University of California San Diego

Robert Scher
BP

David Shambaugh
George Washington University

Benjamin Shobert
Microsoft

Travis Sullivan
Boeing Company

Travis Tanner
Greenpoint Group

Arzan Tarapore
Stanford University

Jessica Teets
Middlebury College

Dana White
Hyundai

THE NATIONAL BUREAU *of* ASIAN RESEARCH
NBR SPECIAL REPORT #97 | MARCH 2022

CHINA'S DIGITAL AMBITIONS

A Global Strategy to Supplant the Liberal Order

Edited by Emily de La Bruyère, Doug Strub, and Jonathon Marek

The National Bureau of Asian Research thanks the U.S. Department of State and the Institute for War and Peace Reporting for their generous support of this project.

The views in this report are those of the authors and do not represent the views or policies of the U.S. government.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

The NBR Special Report provides access to current research on special topics conducted by the world's leading experts in Asian affairs. The views expressed in these reports are those of the authors and do not necessarily reflect the views of other NBR research associates or institutions that support NBR.

The National Bureau of Asian Research helps decision-makers better understand Asia and craft concrete, actionable policy. NBR is an independent research institution based in Seattle and Washington, D.C. We bring world-class scholarship to bear on the evolving strategic environment in Asia through original, policy-relevant research, and we invest in our future by training the next generation of Asia specialists.

Our research is conducted by a global network of specialists and tackles critical issues identified by stakeholders in anticipation of future challenges. The findings are a result of independent scholarship and do not reflect institutional perspectives. Our rigorous standards facilitate informed decision-making based on knowledge rather than ideology.

Established in 1989, NBR is a legacy organization of Senator Henry M. Jackson, who foresaw the national need for an institution to study and inform public policy on Asia in both the public and private sectors. Building on Senator Jackson's bipartisan approach, NBR engages policymakers looking for reliable Asia expertise through sustained interaction in high-trust, nonpartisan settings. Our experts and research have shaped congressional legislation and administration policies, brought issues to the top of the U.S. foreign policy agenda, and attracted worldwide media attention. We mobilize expertise on Asia for a more effective foreign policy.

NBR receives support from foundations, corporations, government (including foreign governments of allies and liberal democracies), and public agencies, and philanthropic individuals. NBR reserves the right to publish findings. We do not undertake classified or proprietary research work, and we observe policies to avoid conflicts of interest.

To download issues of the NBR Special Report, please visit the NBR website http://www.nbr.org.

This report may be reproduced for personal use. Otherwise, the NBR Special Report may not be reproduced in full without the written permission of NBR. When information from NBR publications is cited or quoted, please cite the author and The National Bureau of Asian Research.

This is the ninety-seventh NBR Special Report.

NBR is a tax-exempt, nonprofit corporation under I.R.C. Sec. 501(c)(3), qualified to receive tax-exempt contributions.

© 2022 by The National Bureau of Asian Research.

For further information about NBR, contact:

The National Bureau of Asian Research
1414 NE 42nd Street, Suite 300
Seattle, Washington 98105

206-632-7370 Phone
nbr@nbr.org E-mail
http://www.nbr.org

CHINA'S DIGITAL AMBITIONS

A Global Strategy to Supplant the Liberal Order

TABLE OF CONTENTS

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

INTRODUCTION

A New Type of Geopolitical Power: China's Competitive Strategy for the Digital Revolution

Emily de La Bruyère

EMILY DE LA BRUYÈRE is Co-founder of Horizon Advisory, a consulting firm focusing on the implications of China's competitive approach to geopolitics, as well as a Senior Fellow at the Foundation for Defense of Democracies and a Nonresident Fellow at the National Bureau of Asian Research. She can be reached at <emily@horizonadvisory.org>.

The Chinese Communist Party (CCP) has diagnosed that the emergence of data as a factor of production is catalyzing a new industrial revolution. Chinese policymakers view this industrial revolution as a competitive opportunity to leapfrog to leadership of the international system. Beijing's global digital strategy rests on seizing this opportunity by competing to control international data, its movement, and, by extension, the production, distribution, and consumption of resources and ideas internationally.

A new global digital architecture is taking shape. It is both disrupting the existing hierarchy and creating the foundation for a new kind of geopolitical power. China intends to define this digital architecture by building its physical infrastructure and corresponding virtual networks and platforms, setting the technical standards that govern them, and shaping the emerging global digital governance regime. In doing so, it is cementing Chinese control over the international flow of data—and, as a result, resources.

The digital revolution promises a new era of opportunity, technological advancement, and freedom of movement and thought. However, it also entails unprecedented dangers: the possibility of digitally empowered authoritarianism that reaps profits as it asserts control, a monopolistic network power that squeezes out competition in favor of a rent-based system of political and commercial hegemony, and the capacity to shape, alter, and amplify information at a network-effect pace and scale. China's digital ambitions threaten the ability of companies to compete fairly in the international marketplace, of information to circulate freely, and of governments to defend themselves. China's success would undermine the existing global system as well as the norms, freedoms, prosperity, and stability that it affords. But China's success in achieving its digital ambitions is not a foregone conclusion—if, that is, liberal democracies and market economies stand up to Beijing's challenge. They must work together to promote and defend a digital architecture that can resist illiberal, non-market control and protect the free flow of information. This will be the defining battleground of international relations for the decades ahead.

This report judges that China is strategically and deliberately capitalizing on the digital revolution as an opportunity to define and assert control over international resources, markets, and governance. The six chapters document Beijing's strategic approach to the digital revolution, its growing global influence, and implications for the international order. The first four chapters map China's efforts to rewrite the international digital architecture from the ground up, including through the proliferation of digital infrastructure and platforms, as well as from the top down, via influence over technical standards and governance systems. They reveal that China is turning traditionally commercial and cooperative global domains into battlefields of nation-state competition. They also find that Beijing benefits from a set of asymmetric, structural advantages—scale, centralization, and industrial capacity—that may be newly and uniquely determinative for the digital contest, at least as China is engaging in it. Chapter 5 draws on these findings to demonstrate that Beijing's approach to the digital revolution could transform the nature and stakes of geopolitical power—with corresponding direct security risks, as well as broader commercial, political, and normative ones. However, Beijing's agenda is not a *fait accompli*. A set of multilateral proactive and defensive actions laid out in the final chapter aim to provide a roadmap for an effective, and feasible, response.

Defining the Digital Revolution

The idea of a new industrial revolution is not unique to China. Germany has its Industrie 4.0 national strategic initiative, venture capital firm Andreessen Horowitz has made "software eating the world" buzzworthy, and the World Economic Forum operates a Center for the Fourth Industrial Revolution. However, China's framing of today's industrial revolution is unique, particularly in terms of the perceived implications for international competition.

Chinese policy and strategic discourse assesses that industrial revolutions come about as a result of new factors of production. Today's industrial revolution, the digital revolution, is a function of data having emerged—alongside land, labor, capital, and technology—as a factor of production. A 2020 article in *Qiushi* explains that "production factors are an ever-evolving historical category. Land and labor were important production factors in the era of the agricultural economy," but "after the industrial revolution, capital became an important factor of production in the era of industrial economy." The article continues: "With the advent of the digital economy, data elements have become the new engine for economic development. Data is a new production factor, a basic resource, and a strategic resource."[1]

Beijing frames the resultant global transformation in geopolitical terms as a competitive opportunity to reshape the international hierarchy.[2] Nation-state interaction is defined by a contest for resources. The incumbent leader is powerful because it has an advantage over the legacy basket of resources. But when a new factor of production emerges, that structural advantage fades, and the playing field evens. Rising powers are presented with the opportunity to challenge the hierarchy—not just grow within it. In fact, they have an advantage: unburdened by the inertia and responsibilities that weigh down the incumbent power, they are both more likely and more able to compete in the ways necessary to take advantage of new trends. A 2020 article in the People's Bank of China's journal *China Finance* argues that "every industrial revolution has reshaped the world pattern. With the digital revolution, the world structure will be reshuffled. The countries that are the first to seize the opportunity will rise quickly and occupy a dominant position in the new world order."[3] Chen Wenhui, vice chair of China's National Social Security Fund, is more direct:

> Technological changes in different periods not only bring about industrial changes, but also affect changes in the world structure….In the early stages of the industrial economy, the United Kingdom became the main country….In the early days of the digital economy, the United States and China became the main countries—and now in the period of digital economy development, which is also a period of structural changes, China is facing strategic opportunities…. The digital economy is prompting a new industrial revolution, and the world landscape is facing a reshuffle. China has a first-mover advantage in the digital economy and is expected to achieve a revival in the fourth industrial revolution.[4]

---

1 Dai Shuangxing, "数据要素市场为经济发展注入新动能" [Data Element Market Injects New Momentum into Economic Development], *Qiushi*, May 12, 2020.

2 Shen Haiyan, "关于功率推动数据因素向实际生产力转化的思考与建议" [Thoughts and Suggestions on the Conversion of Power-Driven Data Factors to Actual Productivity], China Consulting Strategic Research Institute, September 8, 2021.

3 "数字经济与第四次工业革命" [Digital Economy and the Fourth Industrial Revolution], *China Finance*, September 13, 2020.

4 Chen Wenhui, "陈文辉详解数字经济投资逻辑: 得平台者得天下" [Chen Wenhui Explained the Investment Logic of the Digital Economy in Detail: Those Who Win the Platform Win the World], Yicai, July 28, 2020.

Assessing China's ambitions for the digital revolution would be a simple matter if data were like land or labor, factors of production where value comes from ownership. Beijing would simply be competing to accumulate global data as empires once measured their power by conquered land—for example, through telecommunications networks, Industrial Internet of Things standards, and transaction platforms rather than armies. However, data is not like land or labor. Its strategic value does not only come from access or ownership. These are certainly important, given that more data means better targeting for everything from kinetic attacks to advertising campaigns as well as better predictive capabilities, awareness of risks, and ability to identify opportunities. But these advantages are tactical.

Strategic, revolutionary power in the digital revolution lies a step beyond accessing data—it lies in the ability to shape data and its movement. The digital world rests on exchange: people, things, and ideas constantly move across networks that transcend national borders. These networks, and therefore these movements, hinge on and are defined by information. This is evident in everything from GPS-supported troop movements to ride-share apps, from e-commerce platforms to the Bloomberg Terminal, and from text messages to social media. To govern these information networks is to shape global resources and their movement.

Data is revolutionary as a factor of production because control over data promises control over not only production but also distribution and consumption of other resources. In a digital environment, power is therefore a function of both capturing data and controlling the architecture of digital exchange: information infrastructure like 5G and smart logistics hubs, platforms like social media and digital trade hubs, and the technical standards and governance systems that define their operations and evolution.

A New Type of Geopolitical Power

The global digital architecture—composed of international norms, standards, and new infrastructure—will determine how, where, and what resources move. Control of the architecture promises an unprecedented type of international power: the ability to shape data on global exchange, and therefore the exchange itself; set international narratives, including propaganda and disinformation; control the data defining land, air, and sea movement, of people and things, military and commercial; and at any point and with little cost threaten an adversary's ability to see, talk, or move.[5] For example, the player that controls digitized logistics hubs can shape international shipments of cobalt without having to deploy troops to capture mines in the Democratic Republic of the Congo; likewise, the player that controls currency trading channels can overtake the dominant global currency. This is network power.

Amazon offers a ripe example of this type of power and its implications. The company controls U.S. commerce not because it has the best products or production but because it has the dominant information platform. At a first level, this grants Amazon superior access to information. It can identify which product has captured the millennial marketplace and replicate it at a better price. With enough longitudinal data, Amazon can predict how the product and its market will evolve next year.[6] These are huge advantages. However, in theory, competitors (e.g., Walmart) can collect

[5] Emily de La Bruyère, "The Network Great-Power Strategy: A Blueprint for China's Digital Ambitions," *Asia Policy* 16, no. 2 (2021): 5–16.

[6] Charles Duhigg, "Is Amazon Unstoppable?" *New Yorker*, October 10, 2019, https://www.newyorker.com/magazine/2019/10/21/is-amazon-unstoppable.

analogous data and use it for similar results. Amazon's real power lies in its ability to shape the information ecosystem in which users shop. The company can assign its products higher ratings than comparable competitor products, flagging them for targeted buyers and setting their prices according to buyer proclivities. Amazon also can feature its products in its original entertainment content. In determining the information that users receive, Amazon can influence their incentives, desires, and purchases.

The stakes of this type of information control are increasingly recognized in international conversations about the private sector. However, such conversations ignore the risk of a nation-state claiming network power. China's overarching digital ambition is to seize the opportunity of the digital revolution, control data as a factor of production, become the network great power, and leapfrog to leadership of the world order. This is how Beijing frames the competition for and of the fourth industrial revolution.

Based on this framing of the digital revolution and power within it, China competes in relatively novel ways, across the commercial as well as the government and military domains, and with the ultimate goal of shaping the international architecture rather than simply seeking advantage within it. As this report details in chapters 1 and 2, China develops digital infrastructure globally and to scale in order to establish the backbone of the industrial revolution from the bottom up. This infrastructure includes physical systems like data centers, smart cities, and their supply chains, as well as virtual systems like "super apps" and payment platforms. At the same time, as chapters 3 and 4 document, Beijing works to shape the rules of the digital environment from the top down by setting international technical standards and exporting a China-centered system of digital governance. This rule-setting approach could lock in China's advantage in the infrastructure and markets of the digital era.

Beijing's digital strategy demands a redefinition of the stakes of information presence and influence. Conversations about China's digital presence and the threat it presents tend to focus on tactical dangers like surveillance, espionage, and cybersecurity. These conversations ignore the more foundational, strategic contest for the global architecture. As chapter 5 lays out, if China succeeds in becoming the network great power, the country will lock in control over the information environment, shaping it to align with the CCP's broader propaganda and disinformation agenda. Beijing would also establish monopolistic control over the platforms that define economic interaction and prosperity in the digital era and would be able to decide which companies win and lose internationally. Moreover, it would lock in superior information access and the ability to restrict the access of adversaries, both commercially and militarily.

At the broadest level, Beijing would turn authoritarianism into an absolute, and money-making, proposition. The CCP would be able to not just gather information on individuals', companies', and countries' activities but also shape the information environment that defines these activities. And because data is a factor of production, this information collection and dissemination would be profitable.

Asymmetric Advantages: Size, Centralization, and Capacity

The nature of data as a factor of production, and the CCP's strategy to compete for it, also demands a redefinition of forums, tools, and modes for state competition. Neither telecommunications base stations nor delegates to standard-setting bodies have traditionally been

conceived of as agents of geopolitical influence or means to control critical, strategic resources. But they now serve that role. This should change frameworks for assessing competitive balances, as well as what constitutes determinative strengths and weaknesses within them.

The last industrial revolution, which was catalyzed by the emergence of technology as a factor of production, rewarded innovative capacity as a critical source of national strength. Today's digital revolution also is oriented around technology, but innovation may no longer be the determinative asset it once was.[7] Instead, China's digital strategy suggests that scale, centralization, and industrial capacity may define today's competitive balance. Beijing has all of these advantages in spades.

First, China's unmatched size grants it unmatched ability to produce and access data: "As far as China is concerned, a population of 1.4 billion, a super-large domestic market, huge domestic demand potential, and abundant natural resource advantages are the treasures of big data production," explains the China Consulting Strategic Research Institute.[8] This size advantage also makes Chinese digital architecture more competitive globally. Networks and platforms are governed by network effects, and their value increases based on the number of connections they offer. In other words, they are differentiated by size. The best, or most appealing, social media platform is not necessarily the one with the best user interface but rather the one that has the greatest number of active users. This plays to Beijing's strengths: the network and platform preferences of its 1.4 billion people can be shaped by the CCP.

Second, not only is China's scale unmatched, but its centralization allows it to more effectively leverage that scale than any other leading global player. Beijing's ability to shape the actions of its population and private sector means that it can determine which technologies and technological architecture are adopted domestically and advocated for globally. Caught in a government-guided, enterprise-driven system, Chinese commercial and academic actors become tools in the CCP's larger digital strategy. Chapter 2 describes this in the context of Beijing's regulatory crackdown on leading tech firms, while chapter 3 does so for international standard-setting bodies. China's control of its domestic information network also allows the country to control its own data, market, and information systems, even while accessing and competing for inroads into their global counterparts. In addition, digital infrastructure, like all infrastructure, requires deliberate capital expenditure, with a long-term time horizon and coordination among a host of private- and public-sector actors with different agendas, incentives, and modes of doing business. This cumbersome process is most easily carried out by a centralized government. Beijing's centralized system may hurt it in an innovation race, but in a contest for networks, platforms, and standards, centralization may grant an asymmetric competitive edge.

Third, China also benefits from unmatched industrial capacity that allows it to build the physical infrastructure of the digital world. This capacity can also grant Beijing an edge in setting international standards. For example, China increasingly dominates standards in telecommunications, a lead that experts interviewed for this report have attributed to the country's larger industrial dominance in the field. Moreover, China's industrial capacity and market size can be leveraged to incentivize other international players across the public and private sectors to adopt Chinese digital infrastructure, platforms, standards, and norms.

---

[7] Chen Wenhui says as much: "China and the U.S. are leading the digital economy. The U.S. advantage is technology. That of China is the market." See Chen, "陈文辉详解数字经济投资逻辑."

[8] Shen, "关于功率推动数据因素向实际生产力转化的思考与建议."

Importantly, China's industrial capacity is no accident. It is the result of deliberate government policy that frames digital competition in terms of both the real and the virtual economy, prioritizing vertically integrated value chains in strategic areas as much as, if not more than, developing advanced technologies. In part, this prioritization stems from defensive motivation—Beijing cannot establish global control if it is excessively dependent on external inputs or markets. As Xi Jinping stated in 2016:

> No matter how large an internet company is, no matter how high its market value is, if it is heavily dependent on foreign countries for its core components, and if the "major artery" of the supply chain is in the hands of others, it is like building a house on someone else's foundation. No matter how big and beautiful it is, it may not stand up to wind and rain, and it may be so vulnerable that it collapses at the first blow.[9]

But the corollary of defensive logic is an offensive one. Beijing recognizes that other countries are willing to build on foundations that are not their own. Namely, they are willing to accept dependencies on China's resources and production. If China does not depend (or depend equally) on them, it can claim asymmetric leverage over its competitors and prevent them from challenging its digital ambitions.[10] Chapter 5 details a concrete case of Beijing exploiting one-sided industrial reliance for geopolitical ends: in 2010, it restricted rare earth exports to Japan in retaliation for disputes over the sovereignty of the Senkaku Islands. This chapter also details the glaring dependencies on China that remain today—rare earths and other strategic resources as well as areas of strategic production like the semiconductor value chain—and the security risks they create.

Organization of the Report

The six chapters that follow assess China's digital strategy, the risks it presents, and a possible path forward. Chapters 1 and 2 describe Beijing's efforts to shape the international architecture from the bottom up by building the physical infrastructure of the digital world and proliferating the digital platforms that define interactions within it. Chapters 3 and 4 focus on Beijing's top-down efforts, as manifest in the export of digital technical standards as well as systems of digital governance more broadly. Chapter 5 discusses key security implications of China's approach. Chapter 6 then concludes on a positive note by providing a framework for a multilateral response.

China has an asymmetric advantage in the digital revolution competition. Because the digital revolution plays to different strengths than did the last industrial revolution, and therefore to different strengths than China's competitors traditionally assess, Beijing may be farther ahead than is generally recognized. Yet this does not mean that the CCP's agenda is a fait accompli. As chapter 6 explains, the liberal international system is still the incumbent system and has entrenched, structural advantages. Global market economies and liberal governments can present a positive alternative for the digital architecture that protects global norms and values, free and fair markets, and open flows of information. However, doing so will demand multilateral coordination in

[9] "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work], Xinhua, April 25, 2016.

[10] See, for example, Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010; and Emily de La Bruyère and Nathan Picarsic, "Two Markets, Two Resources: Documenting China's Engagement in Africa," U.S.-China Economic and Security Review Commission, November 24, 2020.

creative ways that emphasize both defensive measures and a proactive vision. This will necessitate recognizing that today's competition is not yesterday's; it is being contested on new battlefields, with new tools, and to a different end. Winning requires rewriting the playbook.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 1

Securing the Foundation: Building the Physical Infrastructure of the Digital World

Samantha Hoffman

SAMANTHA HOFFMAN is a Senior Analyst at the Australian Strategic Policy Institute. She can be reached at <contact@samanthahoffman.net>.

EXECUTIVE SUMMARY

This chapter finds that China's expansion of its digital infrastructure internationally, though widely discussed, remains a vastly misunderstood and oversimplified problem.

MAIN ARGUMENT

China's global export of digital infrastructure provides a foundation for the party-state to gain greater access to, and control over, data internationally, while also affording new avenues for Chinese digital companies to gain greater market access that can be leveraged to advance the government's strategic interests. Most debate on the issue underestimates the risks associated with the ways control over digital infrastructure can enable future efforts by the party-state that undermine the interests of countries whose data is being accessed and used. For example, control over digital infrastructure can allow for collection of data that, when aggregated, creates greater visibility of a society, enabling other efforts to subvert democratic debate. It can also embed standards that go against liberal democratic values by enforcing authoritarian definitions of risk rather than democratic definitions. Ultimately, however, the largest issue is that China has a political system that is fundamentally different from liberal democracies and that is embedded in the digital technologies and infrastructure researched and developed in China and exported globally.

POLICY IMPLICATIONS

- Data security policy in liberal democracies is not yet effective enough to account for the risks that China creates through its approach to data security.
- Liberal democracies must develop a better approach for identifying strategic datasets and conducting due diligence on digital supply chain security risks.
- Liberal democratic governments must develop responses to China's use of technology to expand its power globally with the understanding that technology develops on a trajectory and capabilities are likely to improve over time rather than be static.
- Liberal democracies must adopt a more multidisciplinary approach to due diligence on decisions related to digital infrastructure. This approach cannot be country-agnostic and must account for country-specific policy drivers. It must also take into account digital supply chain risks associated with data collection and use.
- Liberal democracies must develop responses that better account for uncertainties around a technology's trajectory or a country's ability to translate concepts into capabilities.

Chinese companies are expanding digital infrastructure internationally. Because of China's unique laws, the large role of state-owned enterprises, and state intervention in private companies that allows the Chinese Communist Party (CCP) to violate or exploit globally accepted data privacy norms, policy discussions on the associated political and security risks have emerged (and are assessed in detail in chapter 5). The most prominent example is the decision to effectively ban Huawei from providing 5G equipment in Australia, the United States, the United Kingdom, India, and numerous other countries, as well as the debate around those decisions.[1]

Despite widespread discussion on problems associated with the proliferation of Chinese companies as providers of these technologies and the role of the CCP in promoting and subsidizing their expansion abroad, the nature of the issue remains ill-defined. Most conversation on the topic is narrow in scope. It has tended to focus heavily on intrusive surveillance technologies[2] and espionage[3] as the primary risks of allowing Chinese companies into digital ecosystems. In reality, however, datasets derived from any digital technology can potentially have a broad range of strategic implications that go beyond both surveillance and espionage and are limited only by the intent of an actor who has access to, or possession of, the data. When aggregated, data that may seem insignificant in isolation can have enormous strategic value in terms of how it informs an adversary about a society or how it might support a wide range of other efforts to subvert democratic processes. MI6 chief Richard Moore recently described the issue as China's "data trap" and said: "If you allow another country to gain access to really critical data about your society, over time that will erode your sovereignty, you no longer have control over that data."[4]

Seeing the value of these technologies and the data they help generate, the Chinese party-state prioritizes investing in and building "new infrastructure," artificial intelligence, 5G, and data centers.[5] "New infrastructure" generally refers to infrastructure that enables the Internet of Things (IoT), Industrial Internet of Things (IIoT), or other data-dependent environments such as smart cities and smart manufacturing. This infrastructure, better described as "digital infrastructure," refers to the physical hardware and software that enables digital connectivity. Digital infrastructure at the physical layer, such as smart cameras, smart cars, smart appliances, and other IoT sensors and devices, helps support real-time decision-making; technology that enables data storage or data flows, such as 5G, helps deliver and exchange that information; and artificial intelligence and big-data processing help derive value out of the data. For example, fiber-optic cables, data centers, and IoT devices enable connectivity in smart cities. All facilitate the collection, processing, usage, transfer, and storage of data, and thus the delivery of a wide range of services on which society is becoming increasingly dependent. Beijing's global digital ambitions require the ability to derive

---

1 Peter Hartcher, "Huawei? No Way! Why Australia Banned the World's Biggest Telecoms Firm," *Sydney Morning Herald*, May 21, 2021, https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html; "Huawei 5G Kit Must Be Removed from UK by 2027," BBC, July 14, 2020, https://www.bbc.com/news/technology-53403793; Gautam Chikermane, "No Huawei in 5G Is a Start, No China in Critical Infrastructure Should Be Next," Observer Research Foundation, Digital Frontiers, May 5, 2021, https://www.orfonline.org/expert-speak/no-huawei-in-5g-is-a-start-no-china-in-critical-infrastructure-should-be-next; and "Huawei Ban Timeline: Detained CFO Makes Deal with U.S. Justice Department," CNET, September 30, 2021, https://www.cnet.com/tech/services-and-software/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department.

2 Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, Working Paper, September 2019, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf.

3 Colin Lecher and Russell Brandom, "Is Huawei a Security Threat? Seven Experts Weigh In," Verge, May 17, 2019, https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g.

4 George Bowden, "MI6 Boss Warns of China 'Debt Traps and Data Traps,'" BBC, November 30, 2021, https://www.bbc.com/news/uk-59474365.

5 "新基建，是什么?" [What Is New Infrastructure?], Xinhua, April 26, 2020, https://archive.vn/c3aKE.

benefits from exporting and scaling this digital infrastructure internationally in order to establish control over the foundation of the fourth industrial revolution from the bottom up.

Understanding how the People's Republic of China (PRC) seeks to derive value from the digital infrastructure it exports globally requires unraveling how the party-state perceives its value in a domestic political context. For the CCP, digital infrastructure is a key to solving problems in governance and improving its political control. Conceptually, this can be understood in the context of the party-state's objective to build a more "service-oriented" government, whereby the CCP is able to improve its capacity to solve problems and deliver social services. The CCP links its capacity to accomplish these tasks to its ability to shape, manage, and respond to society's demands in service of its driving objective to protect and expand its power.[6] In essence, technology is a tool that helps the party accomplish fusing its political control with China's economic prosperity and "social development." Technology streamlines existing methods of economic and social problem-solving while also enhancing the party-state's political control.

In April 2020, Xi Jinping said China must "seize the opportunities given by industrial digitization and digital industrialization, [and] accelerate the construction of new infrastructure such as 5G networks and data centers." He also indicated the strategic relevance of the objective, stating that it was "important to pay close attention to the deployment of digital economy, life and health, new materials and other strategic emerging industries and future industries, vigorously promote technological innovation, strive to expand new growth points, and form new development momentum."[7] More recently, in October 2021, Xi called for the acceleration of intelligent and comprehensive digital information infrastructure construction "that is high-speed, ubiquitous, integrated, cloud-network integrated, intelligent and agile, green and low-carbon, and secure and controllable, which creates information 'arteries' for economic and social development."[8]

Internationally, China's vision is similar. In terms of international politics, the CCP sees new infrastructure as a strategic battleground between nation-states and the integration of new infrastructure into the economy as key to guaranteeing national competitiveness. For example, Beijing Communications Administration chief legal counsel Wang Chunhui described how building new infrastructure would "bring about a 'multiplier effect' of total social demand and GDP that is several times the amount of investment, which has significant and far-reaching strategic significance for building a cyber superpower and a manufacturing power, promoting high-quality economic development in China, and building a 'community of common destiny for mankind.'" He added that the construction of new infrastructure is a requirement for building a modern economic system and "enhancing the international competitiveness of China's economy."[9]

The "community of common destiny for mankind" in large part refers to China's desire to reshape the international political and economic system such that it is conducive to Beijing's

---

6 Samantha Hoffman, "Grasping Power with Both Hands: Social Credit, the Mass Line, and Party Control," Jamestown Foundation, China Brief, October 10, 2018, https://jamestown.org/program/grasping-power-with-both-hands-social-credit-the-mass-line-and-party-control; and Fengcheng Yang, "两手抓的源起、内涵与演变" [Origins, Connotations and Evolution of Grabbing with Both Hands], *Guangming Daily*, February 23, 2011, https://archive.vn/JORej.

7 "新基建，是什么?"

8 Zhou Jingjie, "夯实数字经济底座打通经济社会发展信息'大动脉'" [Consolidate the Foundation of the Digital Economy and Open Up the "Artery" of Economic and Social Development Information], Xinhua, October 26, 2021, http://www.xinhuanet.com/tech/20211026/c10d1908bcd3461aaefb0c6e3f02949a/c.html.

9 "北京市通信管理局聘请王春晖教授担任首席法律顾问" [Beijing Communications Administration Hired Professor Wang Chunhui as Chief Legal Counsel], Beijing Communications Administration, 2021, https://archive.vn/fA7zg; and "王春晖：构建新型基础设施是繁荣数字经济的基石" [Wang Chunhui: Building New Infrastructure Is the Cornerstone of a Prosperous Digital Economy], CWW.net.cn, March 10, 2020, http://www.cww.net.cn/article?id=466631. https://archive.vn/b1z7l.

interests and allows Chinese political and economic development to proceed unencumbered by the existing liberal democratic world order.[10] China has recognized, for example, that securing the digital economy, especially as it relates to data security and information security, requires having sufficient control over one's own digital ecosystem.[11]

There are also political and social concerns driving China's digital ambitions. Information security is a prime example. As the world became increasingly digitally interconnected, there was an assumption, within liberal democracies in particular, that authoritarianism would be severely undermined and democracy would emerge stronger as improved information flows stymied censorship efforts. For liberal democracies, the many color revolutions in the early 2000s and the 2010–11 Tunisian Revolution seemed to prove this point. But for China, these movements heightened threat perceptions and called attention to the fact that in a digitally interconnected world those who controlled information flows had an advantage.[12] The ability to prevent threats before they emerge would become increasingly important. For China, its interests were in the ability not just to censor unwanted information but also to shape discourse around issues of strategic importance globally. Over time, this ambition has evolved to include the ability to control the means of information flows. By controlling the means, one controls the message. These inclinations provided critical impetus for China to launch its massive efforts to control as much digital infrastructure abroad as possible.

How the Party-State Creates Risk

Many countries are still working to develop a clear understanding of what data security risk looks like in terms of strategic competition. Because policy development can be a slow process, many countries are exposing themselves and not regulating how data passing through a data center or other infrastructure is used. China-based companies are particularly high-risk vendors for countries who see the PRC as a potential adversarial state actor. But even if the country where the infrastructure is based does not perceive Beijing as a current or potential adversary, they are still subject to the same risks because of the nature of Chinese law and the ways in which the CCP asserts its power over nominally private companies.

The party-state in recent years has made continual efforts to ensure that it has the technical capacity—and that companies and individuals are aware of its political capacity—to demand and access data if, and when, it wants. It has been explicit that all parts of society, including commercial enterprises, are bound by the party-state's demands. The implications of this political context of party-state power over companies have been illustrated by Alibaba's troubles over the past year. In late 2020, founder Jack Ma briefly "disappeared" as regulators investigated the company following his public criticism of the Chinese government.

In fact, China-based technology companies have acknowledged their exposure to legal risks emanating from the PRC in disclosures such as privacy policies. While it is common for any global company in its privacy policy to communicate that user data may be transferred and governed by

---

[10] Nadège Rolland, "Examining China's 'Community of Common Destiny,'" Power 3.0, January 23, 2018, https://www.power3point0.org/2018/01/23/examining-chinas-community-of-destiny.

[11] See, for example, "资本+技术+政府,破解新基建痛点" [Capital+Technology+Government, Breaking Down Challenges of New Infrastructure], Xinhua, September 9, 2020, http://www.xinhuanet.com/tech/2020-09/09/c_1126469977.htm.

[12] Titus C. Chen, "China's Reaction to the Colored Revolutions: Adaptive Authoritarianism in Full Swing" (paper presented at the APSA annual meeting, Washington, D.C., September 4, 2010), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1644372.

laws outside the user's own jurisdiction, the fact that PRC companies say this in privacy disclosures has unique consequences given the nature of Chinese law. PRC technology companies specifically acknowledge that they may be required to disclose users' personal data in accordance with Chinese law-enforcement or state security demands.[13] Given that political security in China is at the core of the CCP's concept of state security, the system governing when these demands might be made is intentionally designed to ensure that the party can access what it wants, when and if it chooses, and regardless of how companies feel about the situation.

The recently enacted Data Security Law (DSL) and Personal Information Protection Law (PIPL) reinforce these risks. Articles 4 and 5 of the DSL state that the effort to guarantee data security must adhere to the party-state's "comprehensive state security outlook," and that the "central state security leading mechanism" is "responsible for decision-making and overall coordination on data security work, and researching, drafting, and guiding the implementation of national data security strategies and relevant major guidelines and policies."[14]

The term "central state security leading mechanism" in legal documents is synonymous with the Central State Security Commission (CSSC), which is a CCP agency led by Xi Jinping.[15] The law says not only that a party entity is in charge, but that any significant policies will originate within the entity. This means that any department or organ—regulatory bodies like the Cyberspace Administration of China or state security organs like the Ministry of Public Security—that is responsible for implementing elements of the data security strategy will be responsible for overseeing and implementing decision-making and strategy that flow from the CSSC. The CSSC, meanwhile, was established to plan and coordinate the implementation of China's state security strategy.[16] Also notable is that a January 2019 directive established that political and legal affairs commissions—which include judiciary and public security organs—are required to implement state security decision-making of "central and local state security leading mechanisms" (i.e., the CSSC and local-level branches) while prioritizing the party-state's political security.[17] Therefore, political security is at the core of data security and state security. This means that any entity directly exposed to those laws is also directly exposed to the risks emanating from this politicized version of state security.

If there were any doubts about the impact of these laws overseas, the DSL also clearly states that Chinese companies are bound by PRC law no matter the political jurisdiction in which their business operations are located. Article 2 says that it applies to data-handling activities taking place "outside the territory of the PRC" if those activities could "harm the state security, the public interest, or the lawful rights and interests of citizens" and organizations of China. In such cases, violators will be pursued for legal responsibility "in accordance with the law."[18]

---

13 "Thematic Snapshot: Privacy Policies," Australian Strategic Policy Institute (ASPI), June 8, 2021, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-05/Privacy-Policies_Mapping-Chinas-Tech-Giants_Thematic-Snapshot.pdf.

14 "(受权发布)中华人民共和国数据安全法" [(Authorised to Publish) Data Security Law of the People's Republic of China], https://archive.vn/ha1CX.

15 "全民国家安全教育日 这20个法律知识你懂吗" [State Security Education Day: Do You Understand These 20 Legal Trivia?], *PLA Daily*, April 7, 2017.

16 Samantha Hoffman and Peter Mattis, "Managing the Power Within: China's Central State Security Commission," War on the Rocks, July 18, 2016, https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission.

17 "中共中央印发《中国共产党政法工作条例》" [The Central Committee of the Communist Party of China Issued the "Regulations on the Political and Legal Work of the Communist Party of China"], Xinhua, January 18, 2019, https://archive.vn/EKxyq.

18 "(受权发布)中华人民共和国数据安全法."

The PIPL is similarly problematic. It regulates the individuals and entities who handle personal data, and while restricting those entities, it explicitly does not do the same for the state organs that can exert power over them. Even though the law establishes that personal information must be handled "in accordance with the authority and procedures provided by laws," seemingly regulating state power, Article 18 is clear that personal information handlers need not notify individuals that their data is being accessed if other laws and regulations provide that the purpose for that access "be kept confidential or need not be announced."[19] Following this logic, one example is Article 7 of the National Intelligence Law, which states that "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any intelligence work they are aware of."[20]

In sum, these laws are applicable anywhere in the world where Chinese companies have operations. Even if the companies providing digital infrastructure are acting according to their own market interests rather than by direction of the state, the state can leverage that expansion and market success for its own purposes if and when it chooses.

PRC Digital Infrastructure and the Embedded Risks

The political risk associated with a vendor could be that vendor's ability to see specific information or exert control over an end-user's access to information.[21] It will likely become increasingly complex to understand how particular datasets are collected and used by any actor, particularly state competitors or adversaries, and especially an adversary that has shown a willingness and ability to leverage its technology companies to advance national policy goals.

Since digital infrastructure tends to be directly linked to the provision of services (and not, for instance, simply for surveillance), many people falsely assume that as long as one controls physical infrastructure and its day-to-day use, the majority of risks associated with it—except for illicit data access—are controllable. What is overlooked, however, are the fundamental concerns around who has control over systems that enable information flows. When aggregated, data consisting of seemingly innocuous information can become extremely valuable. Sentiment data, location data, and other datasets can all offer important insights, depending on the intent of the actor who is processing and using the data. The technology involved is not always an indicator of the strategic relevance. We know that data from facial recognition systems paired with geolocation data can be used for surveillance purposes, and it is obvious from the invasiveness of the technology (in terms of privacy) that this is a potential use case.

It is less obvious, perhaps, that data collected from service-providing technologies, or technologies that offer convenience, can simultaneously facilitate the CCP's efforts to expand power or control. Technology does not create fundamentally new ways of approaching problem-solving

---

19 National People's Congress of the People's Republic of China (PRC), "中华人民共和国个人信息保护法" [The Personal Information Protection Law of the People's Republic of China], National People's Congress of the People's Republic of China, updated August 20, 2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

20 National People's Congress (PRC), "中华人民共和国国家情报法" [The National Intelligenec Law of the People's Republic of China], June 12, 2018, http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml.

21 Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," ASPI, Policy Brief, no. 19, 2019, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?VersionId=eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT; and Samantha Hoffman and Nathan Attrill, "Mapping China's Technology Giants: Supply Chains and the Global Data Collection Ecosystem," ASPI, June 8, 2021, https://www.aspi.org.au/report/mapping-chinas-tech-giants-supply-chains-and-global-data-collection-ecosystem.

but instead intends to improve the efficiency and effectiveness of those efforts. This means that analysts must recognize that seemingly contradictory features of these applications of technology to governance are actually not mutually exclusive. The failure to think in grayer terms is a problem among analysts and decision-makers who continue to compartmentalize China's technologies as "good" and "bad" or "risky" and "non-risky." This has a negative knock-on effect for efforts to predict the potential strategic value of certain digital and data-driven technologies. If the issue is framed as "a good technology can be misused," rather than "digital and data-driven technologies can be used to achieve multiple objectives at once, and those uses could be (subjectively) both good and bad," then the major game-changing effect of the technology in the lens of geopolitical competition is overlooked.

PRC technology companies do not just provide their products to domestic consumers. They also export them globally. Though the global expansion of PRC digital infrastructure is not overseen completely by the Chinese state, the state attaches its interests to this expansion in direct ways. Plans like the Belt and Road Initiative and Digital Silk Road, which export hard and digital infrastructure, create incentives (i.e., financial support) and overlay strategic objectives on the market activity of companies.[22] As these technologies are exported globally, they can set standards—which reflect the party-state's priorities and ambitions—in the market (as is discussed in chapters 2 and 3). The data derived from these Chinese-provided technologies overseas becomes part of the party-state's data ecosystem. While companies are often expanding in their own commercial interest, the state seeks to leverage that expansion by creating or mandating direct or indirect access, such as through the aforementioned DSL and PIPL. The ability to easily integrate and process data from PRC companies located outside China will also incrementally improve over a longer period of time.

Smart cities, or safe cities, are another example of a project that PRC companies (most notably Huawei) are contracted to deliver overseas. Although smart cities offer solutions for everyday problem-solving in governance, they are also associated with efforts to enhance the party-state's capacity for control. In China, the technologies involved in smart cities are usually linked to either the Skynet project or the Sharp Eyes project. Skynet refers to video monitoring equipment that is mostly used at major intersections, law-and-order checkpoints, and other public assembly locations. It uses GIS mapping, image gathering, transmission, and other technology to improve real-time monitoring and information recording.[23] Sharp Eyes is an extension of Skynet. In addition to surveillance cameras, Sharp Eyes is focused on building video/image/information exchange and sharing platforms and county-village-township comprehensive management centers. Its application extends to state security, anti-terrorism, enhanced logistics, security supervision, and the prevention and control of criminal activity.

Smart cities are an example of China's application of technology to its governance strategy, which is often referred to as "tech authoritarianism," though the phrase "tech-enhanced authoritarianism" is more accurate. This means that technology enhances existing methods of maintaining authoritarian control, instead of creating something completely new. As such, the impact might not always be directly visible. For instance, control is not merely about invasive surveillance; control may also be as simple as improving information sharing and information integration among state agencies to more effectively enforce the law or wield state power. Some

---

[22] Nadège Rolland, "A Concise Guide to the Belt and Road Initiative," National Bureau of Asian Research, April 11, 2019, https://www.nbr.org/publication/a-guide-to-the-belt-and-road-initiative.

[23] Zhen Li, "天网加雪亮城乡共平安" [Skynet Plus Sharp Eyes: Both Cities and Rural Areas Are Safe], *People's Daily*, October 11, 2017, http://archive.fo/uEMVC.

analysts point to the fact that technology has not yet caught up to ideas in this regard because, for example, data integration is still a difficult task. Besides the clear technical argument for why this problem is exaggerated—China is not unique, since data integration is a common, global problem—efforts to apply technology to public administration have contributed to what is actually a decades-long effort to streamline public administration.[24] So technology, on this trajectory, is actually incrementally solving a long-term problem, not creating a fundamentally new one.

Despite—or in some cases because of—the strong link between smart city technologies and coercive state activity in China, these solutions have been exported globally. In 2020, Huawei signed an agreement to supply smart city solutions to Saudi Arabia, including smart streetlights, smart parking, and video analytics solutions.[25] Similarly, in Serbia, the company has made over a dozen agreements to provide technology to government entities. In 2016, Huawei agreed to cooperate with Serbian company Telekom to provide digital infrastructure modernization. In 2017, it agreed with the Serbian Ministry of Interior to implement a safe-city solution, including providing surveillance cameras, a command-and-control center, facial recognition, license-plate recognition, analysis systems, and a data center.[26] Within Serbia there have been concerns about the system being used to target the incumbent government's political opponents, but the projects persist.[27] In other cases, projects have been deployed but are not functional. In Pakistan, safe-city projects in Islamabad, Lahore, and Punjab have seen setbacks due to political, technical, and financial problems.[28]

Data centers are another common type of infrastructure Chinese companies have won contracts for or have built overseas. They are also often included in smart-city packages offered by companies like Huawei. For example, in 2019 Huawei agreed to deliver a "data center, smart city, and surveillance" project to Kenya's Konza Technology City.[29] Likewise, in July 2020, it provided equipment for the Zamengoe Data Center in Cameroon.[30] As part of the project, it provided an access management system, surveillance cameras, a fire-fighting system, an energy management system, and four standby electric generators with the financial assistance of the Export-Import Bank of China.

The risk of a country allowing a China-based company to supply or build a data center is equivalent to allowing a high-risk vendor to build a country's 5G network.[31] As previously mentioned, 5G can serve as a prominent example of the risk associated with digital infrastructure. Australia defines a "high-risk vendor" as "any vendor that, by nature of the product or service they offer, has a significant influence over the security of your system." The vendor then "can be subject to adverse extrajudicial direction, or the vendor's poor cyber security posture means they are subject to adverse external interference."[32] This was the justification for effectively banning Huawei from Australia's 5G infrastructure.

---

24 Hoffman, "Grasping Power with Both Hands."

25 "Huawei-Smart City Solutions Company Agreement," ASPI, Mapping China's Tech Giants, https://chinatechmap.aspi.org.au/#/map/marker-3114.

26 "Huawei in Serbia," ASPI, https://chinatechmap.aspi.org.au/#/map/marker-436.

27 Alessandra Briganti, "Serbia's Smart City Has Become a Political Flashpoint," *Wired*, August 10, 2021, https://www.wired.co.uk/article/belgrade-huawei-cameras; "Huawei in Serbia."

28 "Huawei Safe City Project: Islamabad," ASPI, https://chinatechmap.aspi.org.au/#/map/marker-388; "Lahore Safe City Project," ASPI, https://chinatechmap.aspi.org.au/#/map/marker-354; and "Huawei Safe City Project: Punjab," ASPI, https://chinatechmap.aspi.org.au/#/map/marker-490.

29 Sebastian Moss, "Huawei to Build Konza Data Center and Smart City in Kenya, with Chinese Concessional Loan," Data City Dynamics, April 30, 2019, https://www.datacenterdynamics.com/en/news/huawei-build-konza-data-center-and-smart-city-kenya-chinese-concessional-loan.

30 "Cameroon Tier III (Design) Data Center," ASPI, https://chinatechmap.aspi.org.au/#/map/marker-2548; and Alex Alley, "Huawei Equips Cameroon Gov't Data Center, Helps Rain's South Africa 5G Project," Data Center Dynamics, July 20, 2020.

31 Gareth Hutchens, "Huawei Poses Security Threat to Australia's Infrastructure, Spy Chief Cays," *Guardian*, October 30, 2018, https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says.

32 Australian Cyber Security Centre, "Cyber Supply Chain Risk Management Practitioner Guide," June 2020.

The other issue with 5G is that it is the foundation for the IoT and IIoT, which are the technologies that enable smart-city services.[33] The PRC Ministry of Industry and Information Technology's 2021 Industrial Internet Work Plan calls attention to the economic and strategic value of the IIoT as well as its direct connection to expansion of 5G infrastructure.[34] The IIoT refers to "the billions of industrial devices—anything from the machines in a factory to the engines inside an aeroplane—that are filled with sensors, connected to wireless networks, and gathering and sharing data."[35] These devices ultimately allow for greater visibility and transparency about the state of global supply chains.[36] In regular application, these technologies help businesses reduce costs. But there are also national security reasons for improving efficiency and visibility over key industries in the logistics sector, including aviation, marine, and rail. For China, there is strategic value in having access to data from which it can extract valuable information to maintain an internationally competitive edge.

An example of an IoT device that is harder to connect to strategic interests, yet produces data that could potentially be used in ways that undermine democratic debate, is a smart television. The smart television has transformed the media industry in terms of how content is distributed. The aggregated datasets from smart televisions can be useful for understanding how to target particular audiences not only from an advertising perspective but from a propaganda perspective. In the United States, this data has been sold to political campaigns.[37] Such data-handling practices should be a concern in their own right, no matter where the company generating the datasets is based. Chinese companies are among the global leaders in smart television manufacturing. One such company, Hisense, is a leading global company that sells smart products at more affordable prices than its competitors (using the Roku TV interface).[38] Hisense is a partly Chinese state-owned enterprise (i.e., mixed-ownership company),[39] which allows it access to preferential financing and other state support that enables this price advantage. Hisense's overseas privacy policies also make clear that the personal data the company collects can be held on the company's servers in China.[40] This does not mean that Hisense will use the data for purposes beyond business, but it does mean that the company has the ability to do so.

Similar data can be acquired through digital infrastructure in smart cities. Global Tone Communications Technology (GTCOM) is a company controlled by the Central Propaganda Department that engages in global big-data collection. The company offers machine translation services but also uses data to generate insights that contribute directly to state security, according to its own claims. Embedding the company's translation products in digital infrastructure is a key

---

33 Alexander Hellemans, "Why IoT Needs 5G: Will 5G Become the Backbone of the Internet of Things?" IEEE Spectrum, 2015, https://spectrum.ieee.org/5g-taking-stock.

34 "关于印发《工业互联网专项工作组2021年工作计划》的通知" [Notice on Printing and Distributing the 2021 Work Plan of the Industrial Internet Special Working Group], Ministry of Industry and Information Technology (PRC), May 22, 2021, https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2021/art_a02effb156344a408e8ca5d60d0442de.html.

35 Steve Ranger, "What Is the IIoT? Everything You Need to Know about the Industrial Internet of Things," ZDNet, March 2, 2019, https://www.zdnet.com/article/what-is-the-iiot-everything-you-need-to-know-about-the-industrial-internet-of-things.

36 James Henderson, "IIoT Expected to Boost Revenues across Global Supply Chain," *Supply Chain*, May 17, 2020, https://supplychaindigital.com/technology-4/iiot-expected-boost-revenues-across-global-supply-chain.

37 Sidney Fussel, "Why Politicians Want Your Smart-TV Data," *Atlantic*, November 8, 2019, https://www.theatlantic.com/technology/archive/2019/11/smart-tvs-collect-data-political-advertising-use/601381.

38 "Largest TV Manufacturers in the World by Market Share 2020," Technavio, May 21, 2020, https://blog.technavio.com/blog/largest-tv-manufacturers-by-market-share.

39 "Going Private: Hisense Unveils More Mixed-Ownership Reform," *Week in China*, June 12, 2020, https://www.weekinchina.com/2020/06/going-private-3.

40 "HISENSE USA Corporation Privacy Policy," https://archive.fo/tYp7V.

part of how it is able to improve data collection. For example, one GTCOM product, Language Box, was reportedly integrated into a Huawei smart conferencing solution sold as part of smart-city packages.[41] The company also claims to annually collect two to three petabytes of data globally, which contributes to state security applications ranging from relationship mapping and sentiment analysis to facial and voice recognition.

Chinese technology companies are comparable to U.S. companies in that they tend to occupy all layers of the "technology stack": the physical layer, the network layer, and the application layer.[42] They also have a global presence across each of these layers. The difference between the two is largely the way the party-state seeks to derive value from the companies' activities, as the DSL illustrates. But this is also seen in the way the party-state injects itself into China's innovation ecosystem. Technology companies and researchers who develop digital infrastructure in the PRC are focused on implementing specific applications of technology that meet CCP policy needs. In the PRC, the government is heavily involved in efforts to standardize digital technologies at the design level.[43] As is discussed in chapter 3, government and research institutes collaborate with companies on national standards technical committees to standardize equipment development. These requirements that companies must meet to successfully bid for a project will, over time, lead to increased interoperability and the ability to integrate information. This means that the expansion of Chinese technology companies' global activity presents new and complex policy challenges and risks for liberal democracies.

The standardization also embeds a values system that ultimately runs against liberal democratic values. Financial infrastructure has received ample attention in the past year. Although many countries are just now considering the development of a central bank digital currency, China is already a leader of digital currency electronic payment (DCEP). While the DCEP debate has focused heavily on the implications of internationalizing the renminbi, the real focus should be on the implications of DCEP as a financial technology.[44] The standards of the technology can be exported—DCEP is already integrated with digital payment technology such as Alipay, which is accepted globally.[45] An Australian Strategic Policy Institute report, for instance, called attention to the idea that terms such as "anti-terrorist financing" take on a different and highly politicized meaning in China, where those accused of such crimes are often the CCP's political targets or opponents, such as the Uighurs. Based on these definitions, People's Bank of China officials conduct monitoring using big-data analytics that flag unusual activity that might indicate illegal activity (as defined in the PRC). The People's Bank of China might also seek to more closely monitor a specific subset of individuals and entities who are targets of the regime.[46]

---

41 Hoffman, "Engineering Global Consent."

42 Hoffman and Attrill, "Mapping China's Technology Giants."

43 Samantha Hoffman, "Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies," National Endowment for Democracy, April 2021, https://www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf.

44 Matthew D. Johnson, "China's Digital Renminbi Initiative Is a Network, Not a Currency," ASPI, Strategist, June 16, 2021, https://www.aspistrategist.org.au/chinas-digital-renminbi-initiative-is-a-network-not-a-currency.

45 Ibid.

46 Samantha Hoffman, "China's Digital Currency Electronic Payment and Surveillance," testimony before the U.S.-China Economic and Security Review Commission, April 15, 2021; and Samantha Hoffman et al., "The Flipside of China's Central Bank Digital Currency," ASPI, October 2020, https://www.aspi.org.au/report/flipside-chinas-central-bank-digital-currency.

Conclusion

China's export of digital infrastructure abroad is a critical element of its broader digital strategy. It provides the foundation for the party-state to gain greater access to, and control over, data internationally, while also providing new avenues for Chinese digital companies to gain greater market access. It thus—due to China's legal system that ensures party-state access to private companies' sensitive information—further advances the government's digital agenda.

In order to predict and mitigate risk, decision-makers must bear in mind that digital technology is constantly evolving. They must imagine technology's future trajectory and use cases to adequately develop policies governing the application. For now, the critical domains of influence are in possessing infrastructure, storage, processing capacity, and the actual data. The actor that administers these means can later control much more in terms of how technologies—or the data derived from and passing through them—are used.

The risk of offering prescriptive solutions for ambiguous problem sets like those outlined in this chapter is that it limits conceptualization of how China projects extraterritorial political power. That being said, there are ways to better prepare policymakers for dealing with these problems. These include the following:

- *Recalibrating data security policy and privacy frameworks to account for the fact that PRC regulations on each are not motivated by the same drivers as in liberal democracies*. Even if there are some commonalities in the problem sets, the political nature of the state's security strategy will always be a distinguishing feature. More effective data security policy and privacy frameworks will account for a wider range of risk.
- *Taking a more multidisciplinary approach to due diligence on decisions related to digital infrastructure*. This approach cannot be country-agnostic and must account for country-specific policy drivers. It must consider digital supply chain risks associated with data collection and use.
- *Developing responses that better account for uncertainties around a technology's trajectory or a country's ability to translate concepts into capabilities.*

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 2

Capturing the Virtual Domain: The Expansion of Chinese Digital Platforms

Karen M. Sutter

KAREN M. SUTTER is a Specialist in Asian Trade and Finance at the Congressional Research Service. She previously worked at the U.S. Department of Treasury, the CIA, the U.S.-China Business Council, and the Atlantic Council, and has over 30 years of experience working on U.S.-Asia policy issues and crosscutting economic, political, technological, and national security issues in government, business, and the think tank community. She can be reached at <ksutter@crs.loc.gov>.

NOTE: The views expressed in this chapter are those of its author and are not presented as those of the Congressional Research Service or the Library of Congress.

EXECUTIVE SUMMARY

This chapter examines how the Chinese government is seeking to create a China-centered global digital order in which China's technology firms have a leadership position and China controls or influences key economic, financial, information, trade, manufacturing, innovation, and technology networks; their supporting digital infrastructure; and information that flows through these digital platforms.

MAIN ARGUMENT

China's digital platforms are the likely place where the full range of China's technology, economic, and geopolitical efforts, if successful, could converge and solidify China's position in global markets. These platforms advance the Chinese government's global ambitions as conveyed through its Belt and Road Initiative and related Digital Silk Road plans and seek to leverage and integrate the hard and soft infrastructure that China's firms have established or acquired overseas. Through digital platforms, China seeks to operationalize its technology development efforts across the entire value chain in hardware, software, and related design, manufacturing, infrastructure, and services.

POLICY IMPLICATIONS

- The Chinese state plays a powerful and growing role in China's digital infrastructure and operations. As China's digital platforms expand overseas, these points of control allow the state to access, analyze, and leverage wide swaths of global data across a range of platforms and applications with far-ranging potential ramifications for China's global economic and geopolitical capabilities.
- The Chinese government restricts foreign participation in its digital market, the largest in the world, allowing Chinese firms to secure a global leadership position in China and expand globally through sustained unfair trade and investment practices. These persistent asymmetries due to digital protectionism and state controls allow China to secure a global market position that could become increasingly difficult and costly to counter over time.
- China's use of ostensibly nonprofit and corporate actors to advance state goals challenges key tenets of the global trading system and other countries' abilities to address risks. Many markets are open to commerce, and most policy tools consider Chinese corporate actions on a case-by-case basis in narrow instances of national security risks, allowing governments to miss or dismiss the strategic ramifications of China's early discrete actions.

The People's Republic of China (PRC) is seeking to create a China-centered global digital order in which economic, financial, information, trade, manufacturing, innovation, and technology networks—as well as the digital infrastructure they rely on—are controlled or influenced by China; China's technology firms have a leadership position; and China governs a significant share of international information flows. Digital platforms play a key role in this effort. China is developing digital platforms to promote Chinese technology and economic competitiveness, enhance political and social controls, and challenge current global trade, technology, energy, information, and financial networks by creating alternatives that it controls. China is working to consolidate, centralize, and control global digital networks in part through the use of Chinese companies, technologies, and standards in building and operating global digital platforms. In many respects, China's digital platforms seek to operationalize its development efforts across the entire technology value chain in hardware, software, and related design, manufacturing, infrastructure, and services.

Digital platforms are the likely place where the full range of China's technology efforts, if successful, could converge and solidify the country's position in global markets. China-controlled digital platforms, should they expand internationally, could reinforce and leverage China's construction of digital infrastructure, as discussed in the previous chapter, and solidify its influence over international technical standards, as discussed in the next chapter. These platforms are poised to implement China's broader Digital Silk Road goals in building out global networks—including in information, commerce, currency, and innovation—that are vertically integrated and controlled by China. If successfully established internationally, China's digital platforms could cement Beijing's influence over the global information environment with, as discussed in chapter 5, broad ramifications for China's global economic, geopolitical, and security positions.

China's digital sovereignty approach (discussed in-depth in chapter 4) informs its global digital platform strategy as the Chinese government seeks international technology leadership and state touchpoints and controls over platforms, networks, and the data they generate. This statist approach keeps China's domestic digital market walled off from foreign competition and global connections not controlled by China while Chinese firms create and expand China's digital platforms offshore. This not only ensures that China's champion platforms are protected but also grants these firms exclusive access to China's enormous digital user base. The advantage of this asymmetric positioning is enhanced by Beijing's concomitant emphasis on digitizing all elements of its society, including information, goods, services, labor, trade, currency, finance, manufacturing, health, and personal identity. This compounds the size of China's user base, data base, and the corresponding value of Chinese market control. In absolute terms, China's domestic market represents around 40% of global e-commerce.[1] It has an estimated 1.3 billion mobile internet users and is a top global market for mobile payments. Between 2015 and 2020, China's digital economy grew faster than any other market, at an annual rate of almost 17%.[2]

China's digital platforms are characterized by government controls and convergence ambitions—in which Beijing seeks to integrate digital technologies, content, and networks across its platforms, at least for state purposes—making them potential powerful challengers to the current

[1] Joshua Meltzer, "China's Digital Services Trade and Data Governance: How Should the United States Respond?" Brookings Institution, October 2020.

[2] Fang Su, Xiao-Peng An, and Ji-Ye Mao, "Innovations and Trends in China's Digital Economy," *Communications of the ACM* 64, no. 11 (2021): 44–47.

global system.[3] China's statist approach to digital competition and technology is diametrically opposed to deliberations and efforts by other governments that have sought to use antitrust authorities and other regulatory approaches to encourage innovation and competition. Similarly, China's approach to developing new technologies, such as blockchain, appears antithetical to many corporate efforts outside China that are creating digital networks that promote anonymity and seek to avert government oversight. In contrast, China's approach to antitrust and technology development seeks to enhance state control in the name of privacy. Recent measures enhance the state's access to digital platforms and their underlying technologies so that it can surveil, control, and leverage the data from these networks. China is encouraging horizontal integration across platforms, as in the case of "super apps," as well as integration of their data into a broadly relevant and usable architecture, as in the case of its national social credit system. This enhances the scope of data that China's platforms are able to collect and leverage, making them more valuable and competitive. This can also provide a more interconnected experience for users, making the platforms more attractive. At the same time, it may secure state monopolistic control over the digital platform environment.

U.S. digital platforms currently have a global leadership position with commensurate network and lock-in effects that enhance their market position. However, as this chapter details, China's approach to developing and exporting digital platforms may allow its platforms to gain ground and potentially unseat U.S. leadership. China's digital strategy leverages one-sided market protections and access. Its leading digital platforms—such as Alibaba, Tencent, JD.com, DiDi, and TikTok—have a significant global market share as a result of their dominant position in China's massive domestic market. These Chinese digital platforms are now gaining footholds offshore through a range of strategies that include the use of mobile apps and foreign investments. They leverage China's overseas digital infrastructure but also use foreign digital infrastructure, at least initially, to break into new markets. Additionally, through innovation and industrial digital platforms, China is obtaining the foreign technology capabilities it needs to develop its own technology ecosystem that the Chinese government seeks to leverage to support its digital platforms over time. While initially a latecomer to the platform revolution, China is now seeking a first-mover advantage in the adoption and deployment of new emerging technologies, such as blockchain, and may benefit from state support of its digital platforms as well as broader digitization trends in China and global markets—seeking to digitize information, goods, services, labor, trade, currency, finance, manufacturing, health, and personal identity—that are disrupting traditional markets and facilitating new entrants such as China.

This chapter provides an overview of China's digital objectives and explores how digital platforms advance these broader goals, with particular attention to issues of state control and the potential for platform integration. The chapter surveys China's digital platforms, detailing the different types of platforms and approaches to development and global expansion. It also examines how China's development and deployment of a national blockchain technology is contrary to foreign corporate efforts outside China, and how China's digital platforms are distorting concepts of what it means to be open. Finally, the chapter discusses specific case studies of trade, financial, power, and industrial platforms as examples of digital platforms that are advancing China's Digital

[3] For a discussion of concepts of digital convergence, see Suzy E. Park, "Technological Convergence: Regulatory, Digital Privacy, and Data Security Issues," Congressional Research Service, CRS Report for Congress, R45746, May 30, 2019.

Silk Road goals. This chapter aims to raise issues for consideration and is not designed to be a comprehensive overview of the sector.

An Overview of Digital Platforms

Definitions of digital platforms vary, but they are generally understood to be internet-connected and software-based digital spaces that facilitate the exchange of information and the creation of value through the online interactions of businesses and individuals.[4] Digital platforms aim to provide value by offering a digital place to exchange goods, services, and information. They offer points of connection, exchange, and control.[5] China is developing and deploying several types of these digital platforms.

*Transaction platform*s. These are the most common in China's emerging ecosystem and include trade, e-commerce, and payment systems. Alibaba, Tencent, and JD.com are prominent examples of China's national champions operating in these areas.

Information platforms. While all platforms provide information, these platforms focus on the dissemination of information through private messaging, social media, and news services. China has an estimated one billion social media users. Top firms in this space are Tencent's WeChat (closed voice and text messaging service with additional features including gaming, shopping, and fintech), Sina Weibo (microblogging), and ByteDance's Douyin (the domestic version of TikTok's short video service).[6] Some Chinese firms engage in digital news content and aggregation. ByteDance's Toutiao and Newsbreak are examples of Chinese digital news aggregators that operate in the United States.[7]

Super apps. These multipurpose platforms integrate numerous transaction and information functions described above. A great deal of China's digital economy flows through a few of these mobile apps operated by China's national technology champions.[8] Tencent's WeChat, for example, offers integrated services in communications, social media, digital content (e.g., games, books, news, and music), payment services (e.g., WeChat Pay and QQ Wallet), and tools (e.g., email and browsing software).[9]

Industrial platforms. These platforms share manufacturing-related technology and expertise and aim to upgrade industry through Internet of Things (IoT) applications. They advance China's industrial policy goals in advanced manufacturing, and many operate through partnerships with leaders in advanced manufacturing such as Germany, facilitating technology transfer and cross-border training for Chinese firms. Examples of these industrial platforms include China Aerospace Science and Industry Corporation's INDICS and Haier's COSMOPlat.

Innovation platforms. These platforms support open-source technology collaboration across national borders in software and hardware. While many Chinese firms use Microsoft's GitHub, the Chinese government is sponsoring the development of domestic competitor Gitee.

---

[4] See "ITIF Technology Explainer: What Are Digital Platforms?" Information Technology and Innovation Foundation, October 12, 2018.

[5] Sangeet Paul Choudary, "China's Country-as-Platform Strategy for Global Influence," Brookings Institution, TechStream, November 19, 2020.

[6] See "9 Chinese Social Media Platforms You Need to Know About," Tenba Group, September 16, 2021, https://tenbagroup.com/9-chinese-social-media-platforms-you-need-to-know-about.

[7] Didi Kirsten Tatlow, "Whose News?" Wire China, May 23, 2021.

[8] Caleb Foote and Robert D. Atkinson, "Chinese Competitiveness in the Global Digital Economy," Information Technology and Innovation Foundation, November 23, 2020.

[9] Lala Hu, *International Digital Marketing in China* (New York: Springer, 2020).

In biotechnology, China's BGI Group has developed a platform to conduct cross-border genetic testing; China's WuXi AppTec operates a platform that conducts cross-border drug development.

Infrastructure platforms. These platforms use a robust toolkit of sensors and other surveillance technologies to collect and aggregate complex datasets that support a range of applications enabling the construction and operation of digital infrastructure that includes e-government and public services. China's digital platforms in this area include its operation of supporting services for smart cities and State Grid's domestic grid platform, as well as global ambitions for an interconnected smart power grid.

Enterprise and industry software systems. These large-scale software applications support corporate and industry operations that include business processes, supply chains, information flows, reporting, and data analytics. While many systems focus on facilitating a company's internal processes, they interact with external consumer information and services and can also be considered as digital platforms. A prominent example of a PRC firm operating in this area is China's state-tied Shiji Group, which operates back-office software systems for the hospitality industry. After President Donald Trump blocked Shiji's bid to acquire StayNTouch in March 2020, the company expanded its U.S. operations to sell its information systems software directly to hotels.[10] According to Shiji, over 56% of all hotels in the United States now use its technology in their stack.[11] In another example, Alibaba operates a back-office payment system for Walgreens in the United States through a joint venture structure.[12]

China's Platform Objectives

China is developing digital platforms to promote Chinese technology and economic competitiveness, enhance political and social controls, and challenge current global trade, technology, energy, information, and financial networks by creating alternatives that it controls. There is a disruptive element to these efforts, along two main axes. First, digital platforms are by nature disruptive to established businesses and sectors. These platforms are changing the rules of the game and allowing new entrants to break in and expand quickly. Second, China's efforts are also disruptive in that they seek to overtake the existing digital, and broader global, architecture, which is led by a liberal system and based on values of free and open access to information. Instead, Beijing seeks to create alternative global digital platforms and related architecture that are centered on and controlled by China.

Digital platforms support Chinese government technology-enhanced forms of control, including censorship, surveillance, and propaganda. Domestically, for example, Chinese technology firms have developed e-government platforms, smart cities, and robust surveillance networks to censor content as well as surveil and control the Uighur people. Internationally, Chinese firms are exporting these digital tools and models in their development of sensitive digital infrastructure and platforms in other countries.[13] These surveillance, censorship, and propaganda

---

[10] See Donald J. Trump, "Order Regarding the Acquisition of Stayntouch, Inc. by Beijing Shiji Information Technology Co., Ltd.," White House, March 6, 2020, https://trumpwhitehouse.archives.gov/presidential-actions/order-regarding-acquisition-stayntouch-inc-beijing-shiji-information-technology-co-ltd.

[11] See "Bringing the Future of Hospitality Technology to the Americas," Shiji Group, https://www.shijigroup.com/regions/americas.

[12] Rita Liao, "China's Alipay Digital Wallet Is Entering 7,000 Walgreens Stores," TechCrunch, February 13, 2019.

[13] "China's Algorithms of Repression," Human Rights Watch, May 1, 2019.

risks—as well as the larger challenge of China's export of digital platforms—are particularly acute because of the degree of Chinese government control over its platforms. Under China's digital sovereignty model, foreign participation in the country's internet- and software-tied systems is restricted, and the system is firewalled to networks outside China, closely monitored, censored, and leveraged for propaganda and surveillance purposes. The Chinese government has also tightened the ability to use workarounds such as VPNs.[14]

Since 2007, the Chinese government has implemented a series of laws, regulations, and measures that enhance its controls over hardware, software, and technology services, including digital platforms. China still depends on certain foreign technology, hardware, and software to operate its platforms—including sensors, semiconductors, and high-end programmable logic controllers—but its industrial policies condition foreign market participation to ensure that China controls the underlying technology and learns how it works so as to "digest, absorb, and re-innovate" this capability.[15] China has also enacted a series of national economic security measures since 2014 that strengthen the state's control over digital platforms and economic activity more broadly. Its 2017 Cybersecurity Law codifies broad governmental powers to control and restrict internet and digital platform activity. Since 2020, the Chinese government has strengthened its control over data, algorithms, and digital platform operations. China's new data security law restricts cross-border data transfers, and the new personal information privacy law enhances the state's authority over the collection and use of data.[16]

The Chinese state maintains an array of points of control over China's digital platforms that operate domestically and overseas, including digital architecture, hardware, and software designed, built, and operated by China. Software-based algorithms are typically developed and controlled in China; trusted Chinese companies and PRC nationals give the state potential touchpoints over Chinese companies' overseas digital operations as well. While they also have their own commercial interests, Chinese technology firms and the digital platforms they develop and operate are closely tied to the Chinese state. They benefit from state direction and policy and financial support, as well as from China's foreign policy that promotes their expansion by aligning with UN programs and negotiating government agreements for overseas projects. They are also subject to state lines of control, which can include the government, the party, and the military.

China's Platform Development and Overseas Expansion

China's platform ambitions are evident in its industrial and technology planning. Its 14th Five-Year Plan (2021–25) emphasizes the importance of China's role in setting international rules and standards, particularly in digital and financial trade.[17] Toward this goal, many of China's digital platform efforts are structured or supported by organizations that brand themselves as nonprofit even though they are state-tied and state-interested. This allows China to advocate its views with

---

[14] "Eight Platforms to Promote Your Business in China (2021)," Marketing to China, November 27, 2020.

[15] Karen M. Sutter, "Foreign Technology Transfer through Commerce," in *China's Quest for Foreign Technology: Beyond Espionage*, ed. William C. Hannas and Didi Kirsten Tatlow (London: Routledge, 2021); and Central Committee of the Chinese Communist Party (CCP) and State Council of the People's Republic of China (PRC), "Outline of the National Innovation-Driven Development Strategy," Xinhua, May 19, 2016, available at https://cset.georgetown.edu/wp-content/uploads/t0076_innovation_driven_development_strategy_EN.pdf.

[16] For a discussion of these measures, see Karen M. Sutter, "China's Recent Trade Measures and Countermeasures: Issues for Congress," Congressional Research Service, CRS Report for Congress, R46915, September 20, 2021.

[17] National People's Congress (PRC), "The 14th Five-Year Plan for the National Economic and Social Development of the People's Republic of China and Outline of Long-Term Development Goals for 2035," Xinhua, March 11, 2021.

foreign academic, corporate, technical, and government stakeholders in softer ways than direct government advocacy. Use of these types of organizations also allows the Chinese government to downplay its role in academic research, industry associations, and standard setting, both in China and in overseas organizations (see the case study in the **Appendix** for more information).

Domestically, the Chinese government has sought to develop indigenous and secure internet- and software-tied digital systems since its 9th Five-Year Plan (1996–2000). China's Internet Plus strategy, released in 2015, established its plans to promote the digital economy as a new driver of economic growth and innovation that would make Chinese firms competitive by tying industries, innovation, and economic activity to the internet and information technology applications such as big data, cloud computing, and the IoT.[18] Government policies have incentivized digital platform projects in healthcare, transportation, education, finance, logistics, environment, physical tracking, e-government, and credit ratings.[19] Chinese policies also emphasize—as is discussed in other chapters of this report—the systems that make up the larger ecosystem in which platforms exist and on which they depend. The Chinese government is prioritizing the development of China's digital economy and related strategic technologies in its 14th Five-Year Plan.[20] This includes digital infrastructure: China has committed $1.4 trillion over the next five years to digital infrastructure, including in 5G and 6G, smart cities, and IoT applications for manufacturing.[21] China's ecosystem approach also prioritizes autonomous value chains: long-standing industrial policies support the country's digital strategy in seeking to develop the full value chain of its technological capabilities.[22] Chinese digital policies outline intentions for China to own and control the intellectual property and standards in global technology value chains as part of broader efforts to gain a leadership position.[23]

Globally, China's plans call for the development of China-controlled digital infrastructure in overseas markets. The Belt and Road Initiative (BRI) and related Digital Silk Road initiatives seek to expand China's digital trade, build Chinese information and communications networks, and deepen global digital connectivity that is China-centered and -controlled.[24] China's digital platforms both advance and build off this global construction of digital infrastructure, including transnational land and submarine cable networks, fiber-optic cables, satellite navigation networks (BeiDou), data centers, and related cloud services. Southeast Asia has been a key initial focus in China's efforts to build digital platforms outside its borders. Internet Plus incentivized BRI digital projects, with a focus on a China-ASEAN digital hub.[25] In 2014 the State Council approved a state digital platform hosted by China-ASEAN Harbor Information Co. to promote Chinese digital infrastructure and platforms in South and Southeast Asia as part of the Digital Silk Road.

---

18 "China Unveils Internet Plus Action Plan to Fuel Growth," Xinhua, July 4, 2015.

19 Ana Cicenia, "China's Digital Economy: The Shape of Things to Come," China Briefing, Dezan Shira and Associates, January 4, 2018.

20 National People's Congress (PRC), "The 14th Five-Year Plan"; and Karen M. Sutter and Michael D. Sutherland, "China's 14th Five-Year Plan: A First Look," Congressional Research Service, January 5, 2021.

21 Cheng Yu and Zheng Yiran, "China Eyes 6G as Next Tech Frontier," *China Daily*, March 20, 2021.

22 Karen M. Sutter, "'Made in China 2025' Industrial Policies: Issues for Congress," Congressional Research Service, August 11, 2020.

23 China's Medium and Long-Term Plan for S&T Development (2006–25) set the strategic direction for China's industrial policies introduced since 2006, including Made in China 2025. These policies aim for China to own and control the intellectual property and standards in global technology value chains as part of broader efforts to gain a leadership position. See Sutter, "Foreign Technology Transfer Through Commerce."

24 "President Xi's Speech at the Opening of the Belt and Road Forum," Xinhua, May 14, 2017; and National Development and Reform Commission (PRC), "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st Century Maritime Silk Road," March 28, 2015.

25 Cicenia, "China's Digital Economy."

The firms' projects include surveying and mapping, smart cities, smart harbors, intermodal systems, medical imaging, and trade settlement.[26]

China's competitive approach to developing and exporting digital platforms is evident in its incubation of domestic champions, as well as the methods these champions are now using to make international inroads. Until 2012, Chinese technology firms generally pursued a copycat strategy in which they created digital platforms for Chinese users that mimicked leading U.S. digital platforms. Alibaba began in 1999 as a competitor to Amazon, and in 2003 it developed Alipay as a competitor to PayPal. Baidu started as a competitor to Google in search engine and mapping services and developed a competitor video and movie service (iQIYI) and Chinese version of Wikipedia (Baike). Sina Weibo began as a challenger to Twitter. In 2011, Tencent launched WeChat to challenge Facebook's WhatsApp. In 2012, ByteDance began as a news aggregator, Toutiao, which used an algorithm the company refined in 2016 to launch a short video business, Douyin (the domestic version of TikTok), to challenge Facebook and YouTube.

Once these competitor domestic platforms are established, the Chinese government has consistently proceeded to restrict—or push out of its markets—the foreign digital platforms that were copied and with which the copycat Chinese versions seek to compete internationally. This has played out for Amazon, Google, Facebook, Yahoo, Uber, and, more recently, LinkedIn. This is evidence of China's domestic market protections granting its platforms asymmetric advantage in competing for global market share: Chinese firms are able to grow in the protected, insulated, and government-bolstered Chinese market with little international competition and the advantages of building a globally significant position by leveraging China's enormous domestic user base. China's market matters to global digital competition, and preferential access for domestic firms coupled with restrictions for foreign competitors creates certain advantages and disadvantages globally. Due to the size of China's market and its focus on mobile networks and digitalization, in absolute terms China's domestic market represents around 40% of global e-commerce.[27] It has an estimated 1.3 billion mobile internet users and is a top global market for mobile payments. China's digital economy has grown faster than any other market, at an annual rate of almost 17% between 2015 and 2020.[28] Foreign markets for the most part remain open to China's digital platforms, including related infrastructure such as data centers and cloud services. This asymmetry has allowed Chinese firms to develop within China in a protected market and then expand globally, while U.S. digital platforms are kept out of the world's largest and fastest-growing market.

China's strategy relies not only on domestic market protections but also on removing other countries' market barriers. Beijing's trade policies press foreign countries to lower barriers of entry not only to China but also to one another. This creates the potential for China's platforms to expand across national boundaries. Moreover, BRI leverages the provision of digital infrastructure and systems, as well as preferential financing, to bypass normal trade liberalization reciprocity rules and allow China to expand in foreign markets without having to open its own market in return. This approach has been attractive for some governments. Most have not pressed China for any quid pro quo in return for this market access. China's major trading partners—including many that have competitive technologies and platforms at stake—for the most part have not imposed

---

26 "The Digital Silk Road Initiative: Wiring Global IT and Telecommunications to Advance Beijing's Global Ambitions," Pointe Bello, January 2019, https://a.storyblok.com/f/58650/x/0c5c298009/pointe-bello-digital-silk-road-2019.pdf.

27 Meltzer, "China's Digital Services Trade and Data Governance."

28 Su, An, and Mao, "Innovations and Trends in China's Digital Economy."

requirements in their domestic markets or negotiated rules to require reciprocity in third markets. Further, platform services operate in a gray regulatory environment in which they are disrupting and allowing Chinese participation not only in digital markets but by extension in some of the otherwise most highly regulated industries such as banking, insurance, health, and media.

Today, China's digital platforms are expanding offshore through a combination of approaches that include the use of foreign operating systems and cloud services, the development and use of digital infrastructure that Chinese firms have created overseas, and acquisitions of and partnerships with foreign companies. Many social media and super apps, such as TikTok and WeChat, use a model that allows their platforms to reside within operating systems on mobile phones, such as Apple's iOS and Google's Android.[29] This model creates a low-cost way for Chinese platforms to provide cross-border digital services without a heavy initial investment in supporting infrastructure. As their platforms' use and reach expand, these firms then seek to operate their own data centers and cloud services overseas. Alibaba, Huawei, and Tencent are examples of platform providers that have rapidly expanded their global cloud services.[30]

Some Chinese firms elect, at least for now, to use foreign cloud services and platforms to operate overseas. Baidu's autonomous driving platform, Apollo, is based on open-source Android software and operates on Microsoft's Azure Cloud. This allows Baidu to offer support to over 95 partners (including foreign auto firms) and test Apollo applications overseas, including test-driving in California. The Apollo platform provides data and code that allow Baidu's partners to develop applications.[31] Many of China's industrial and innovation platforms use foreign platforms, such as Microsoft's GitHub, for cross-border technology transfer and collaboration.

Alibaba, Huawei, Dahua, and ZTE are among the Chinese firms building integrated digital architecture and platforms through smart-city deployments in China and overseas. These collect, integrate, analyze, and apply data from a city's operations and management systems to run digital platforms for government services, utilities, energy, transportation, health, and security. These systems use cameras, sensors, radio frequency identification, satellite positioning, card readers, video capturing devices, and data aggregation that in turn feed surveillance systems, artificial intelligence, and cloud computing. To function, these systems have touchpoints to foreign physical, transportation, utility, and other critical infrastructure.[32] Chinese digital platforms can also leverage digital architecture that other Chinese firms have put in place. Huawei, for example, is building overseas data centers and cloud services for other Chinese firms, such as State Grid.[33]

Chinese digital platforms are also expanding overseas through foreign partnerships and investments. Acquisitions of foreign firms have helped China acquire a range of technological capabilities relevant to platform development, including computer architecture, semiconductors, sensors, data and data analytics, biotechnology, and related areas such as genetics and biometrics. BGI Group, for example, acquired its DNA-sequencing capabilities through a 2012 acquisition of U.S.-headquartered Complete Genomics.[34] Also, in a two-part deal that began in 2015, the Chinese

---

29 Jean-Christophe Plantin and Gabriele de Seta, "WeChat as Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms," *Journal of Chinese Communication* (2018).

30 Foote and Atkinson, "Chinese Competitiveness in the Global Digital Economy."

31 Rebecca Arcesati and Caroline Meinhardt, "China Bets on Open-Source Technologies to Boost Domestic Innovation," Mercator Institute for China Studies (MERICS), May 19, 2021.

32 Katherine Atha et al., "China's Smart Cities Development," U.S.-China Economic and Security Review Commission, January 2020.

33 Jonathan E. Hillman and Maesea McCalpin, "Huawei's Global Cloud Strategy: Economic and Strategic Implications," Center for Strategic and International Studies, May 17, 2021.

34 "BGI-Shenzhen Completes Acquisition of Complete Genomics," PR Newswire, May 18, 2013.

government acquired U.S.-headquartered OmniVision, the world's third-largest image sensor provider.[35]

Foreign acquisitions and partnerships have also allowed Chinese platforms to gain overseas market footholds, in some instances skirting the need for licenses and gaining expertise and insights. Tencent has developed its global gaming network largely through investments in foreign gaming firms, including Supercell and Epic Games.[36] Its investments in mobile payment app Lydia and neobank Qonto allowed it to enter the European financial market without a license.[37] Similarly, it entered Latin America through a joint investment with SoftBank in the Argentina-headquartered fintech company Uala.[38] Pharmaceutical technology company WuXi AppTec has used acquisitions to build a U.S. and European presence.[39] ByteDance's acquisition of Musical.ly in November 2017 allowed TikTok to immediately add an estimated 80 million U.S. users to its platform.[40] In 2019, TikTok was the most downloaded app in Apple's store. It has been downloaded more than 1 billion times, operates in over 150 countries, and has become China's fastest-growing digital platform.[41] In Russia, Alibaba's AliExpress created a joint venture with MegaFun, Mail.ru, and Russia's sovereign wealth fund. Alibaba has acquired Trendyol (Turkey), Daraz (Pakistan), and Lazada (Singapore) and invested in other firms in India and Indonesia.[42] It is the largest shareholder in India's leading mobile payment firm, Paytm, and the Philippines' Mynt. Chinese digital platforms are also expanding through shareholding in foreign platforms. Tencent is one of the largest shareholders of Snap, the parent of Snapchat.[43] Since 2019, Snap has expanded into areas of interest to Tencent, such as gaming, e-commerce, and mini apps.[44]

Convergence

The Chinese government appears to be seeking technological, content, and network convergence across its digital platforms, in terms of both their outward-facing operations and the state's access to their back-end operations and data resources. These forms of convergence are distinct to Chinese platforms because of the state's overarching role and interests. Convergence aligns with and fuels centralized government control over platforms and their information. It may also make China's platforms uniquely competitive and powerful. In particular, it increases the scope of data that they can collect, leverage, and disseminate—and may gain additional traction and capabilities because of how it offers users a more seamless and integrated experience across a range of functions and applications.

---

35 Peter Clarke, "OmniVision Agrees to Become Chinese," eeNews Europe, May 6, 2015; and Peter Clarke, "OmniVision Bought Quietly by China's Will Semiconductor," eeNews Europe, May 24, 2019.

36 Pieter Haeck, "China's Tencent Goes on a European Shopping Spree," *Politico*, August 18, 2021.

37 Matteo Giovannin, "Tencent Is Betting Heavy on European Fintech Companies," *China Daily*, February 24, 2020.

38 "Tencent, SoftBank-Led Funding Pushes Argentina's Uala to $2.45 Bln Valuation," Reuters, August 13, 2021.

39 In the United States, the company has acquired AppTech Lab Services (2008), Medkey (2011), Xeno Biotech Laboratories (2014), HD Biosciences (2017), Research Point Global (2017), and Pharmspace (2019). In Europe, the firm has acquired Crelux (2016), Bristol Myers Squibb production facilities (2021), and Oxgene (2021). See "Our History," WuXi AppTec, https://www.wuxiapptec.com/about/history.

40 Mansoor Iqbal, "TikTok Revenue and Usage Statistics (2021)," Business of Apps, September 28, 2021.

41 "9 Chinese Social Media Platforms You Need to Know About."

42 Foote and Atkinson, "Chinese Competitiveness in the Global Digital Economy."

43 As of June 30, 2021, Tencent had invested approximately $16.8 billion in Snap Inc., representing around 15% of its total outstanding shares. See "2021 Interim Report," Tencent Holdings Limited, https://static.www.tencent.com/uploads/2021/08/31/7276c2279348d70e0b0f74f6c470f92e.pdf.

44 Adam Levy, "Snap's Taking Another Step toward Becoming WeChat," Motley Fool, June 15, 2020.

Smart cities offer an example of a Chinese digital system that already integrates a wide range of Chinese infrastructure, technologies, functionality, and data. China's super apps now combine a wide array of integrated services and data. Similarly, China's Integrated Joint Operations Platform for controlling the Uighur population integrates a variety of digital tools and aggregates, analyzes, and acts on a wide range of datasets to surveil.[45] Some analysts see China's social credit system as being stove-piped across applications, but a common identifier or national digital overlay could align systems and functions. More broadly, common identifiers used across platforms or that are identifiable to operators across platforms could facilitate convergence. In 2018, for example, the Chinese government integrated the national ID card with Tencent's QR code and is now leveraging Tencent facial recognition technology to enforce its rules restricting minors' access to gaming domestically.[46] In 2020 the Chinese government leveraged and nationalized the Alipay Health Code app—a digital platform originally developed by Ant Financial for the Hangzhou government—to evaluate health status and monitor and control the movement of people during the Covid-19 pandemic.[47]

China's requirements that platform users use their real identification, along with the growing centralization of personal information on digital platforms, could further enable the aggregation of data and development of rich and sophisticated profiles of users across platforms, for both the operators and the Chinese state. China's growing use of facial recognition and biometrics and advances in biological applications provide a way to further refine identification and surveillance capabilities across digital platforms. There is evidence that similar practices are being implemented abroad as Chinese digital platforms expand in overseas markets—thus giving the Chinese government greater access to foreign data, influence over external digital environments, and heightened ability to surveil foreign populations. This use of both private and state-owned companies to increase Chinese influence and control over international digital ecosystems is a core pillar of Beijing's digital strategy.

China's plans for its digital currency and a globally connected power grid seek to overlay new digital technologies and platforms on existing networks. Digital infrastructure and common technical standards—both goals of the Digital Silk Road—can facilitate interoperability (as is discussed in chapter 3). China is advocating for civilian-military interoperability in its Military-Civil Fusion program and its China Standards 2035 development plan.[48] As discussed in chapter 1, China's development of smart cities, ports, rail, and telecommunications networks overseas creates intermodal and potentially interoperable digital infrastructure on which it can develop services.[49] Cross-shareholding among Chinese technology firms in domestic and foreign digital platforms, as well as large firms in other industries that themselves handle sizeable amounts of data, could also facilitate convergence.

---

45 "China's Algorithms of Repression."

46 Gabriel Wildau, "China Unveils Digital ID Card Linked to Tencent's WeChat," *Financial Times*, December 17, 2017; and Jiang Yaling, "Tencent Deploys Facial Recognition to Detect Minors Gaming at Night," Sixth Tone, July 6, 2021.

47 Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags," *New York Times*, March 1, 2020.

48 Daniel R. Russell and Blake H. Berger, "Weaponizing the Belt and Road Initiative," Asia Society Policy Institute, September 2020; Central Committee of the CCP and the State Council (PRC), "Outline for the Development of National Standardization," Xinhua, October 10, 2021; and Standardization Administration (PRC), "'China Standards 2035' Project Launched in Beijing," February 7, 2021.

49 Ashley Dutta, "Introduction to China's Digital Silk Road: Economic and Technological Implications," *Asia Policy* 15, no. 1 (2020).

China's recent actions against its technology champions appear aimed at state centralization and convergence.[50] Measures since 2020 related to antitrust, privacy, and data appear designed to ensure that the state has access to its digital platforms and that these platforms open their proprietary services to one another to facilitate innovation and development of the sector. China may continue to leverage these companies' digital platforms for its own purposes by asserting stronger controls and reining in or directing certain activity. The government's overlay of new applications such as digital currency could crowd out the current e-wallet leadership of China's super apps, or it might be a measure to capture these platforms and align services.

China's Use of Blockchain Technologies in Digital Platforms

China's emphasis on centralization and expanding and enhancing state control over digital activity is also evident in its efforts to exert control over the development of emerging technologies like blockchain, as well as the platforms for their use. The 14th Five-Year Plan prioritizes the development and deployment of blockchain technology for initial applications in financial payments, supply chain management, and e-governance. These plans build on Chinese leader Xi Jinping's statement in October 2019 at a Politburo study session that blockchain would provide an "important breakthrough point for indigenous innovation in core technologies."[51] Xi also called for a security guarantee system that would be adapted to the technology that guides developers and platform operators to implement "security responsibilities."[52] In 2020 the Chinese government launched two national projects—the Blockchain-based Service Network (BSN) and the Xinghuo Blockchain Infrastructure and Facility (BIF)—to direct and support the development of globally connected data centers that operate through a Chinese government–controlled network.[53] The Hainan Free Trade Zone is China's first blockchain pilot zone. In a nod to state priorities, its plan is called Secure, Sharing, Compliance+ (SSC+).[54] At a Hainan trade forum in December 2019, participating countries signed a digital agreement with blockchain provisions.[55]

Internationally, many companies are developing and deploying blockchain technologies in applications that promote decentralization and anonymity and attempt to circumvent government oversight. China, in contrast, is developing blockchain capabilities to strengthen the state's control of digital platforms and the information that passes through these networks. In addition to developing the government's own capabilities, it is also detecting and shutting down unauthorized operators.[56] The China Academy of Information and Communications Technology (CAICT)—an

---

50 Jing Yang and Keigh Zhai, "Alibaba and Tencent Consider Opening Up Their 'Walled Gardens,'" *Wall Street Journal*, July 14, 2021.

51 Eliza Gkritsi, "Blockchain, Fintech Get Name Checks in 14th Five-Year Plan," TechNode Briefing Newsletter, March 5, 2021; and "During the 18th Collective Study Session of the Political Bureau of the Central Committee, Xi Jinping Emphasized the Use of Blockchain," Xinhua, October 25, 2019.

52 In January 2019 the Cyberspace Administration of China issued regulations to govern blockchain service and platform operators. See Kai von Carnap, "Translation: Blockchain Information Service Management Regulations (2019)," DigiChina, March 17, 2021.

53 Yaya J. Fanusie, "An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success," testimony before the U.S.-China Economic and Security Review Commission, Washington, D.C., April 15, 2021; and Eliza Gkritsi, "China to Release National Blockchain Standard Next Year, Says Official: Report," CoinDesk, October 28, 2021. The BSN is a government organization. It is governed by the BSN Development Association, which is led by the State Information Center, a government think tank under China's National Development and Reform Commission. Other key members are China Mobile, China UnionPay, and Red Date Technology, a Hong Kong–incorporated firm identified as the technical architect.

54 Aarav Ghosh, "China Reinforces Blockchain Connection with BRI Countries," Blockchain News, December 5, 2019.

55 See "Huobi Releases Details from the Hainan Free Trade Port International Cooperation Forum on Digital Economy and Blockchain," PR Newswire, December 9, 2019.

56 Eliza Gkritsi, "China's Qihoo 360 Built Crypto Mining Monitoring Software to Support Crackdown," CoinDesk, December 1, 2021.

institute under China's Ministry of Industry and Information Technology (MIIT)—is developing the blockchain technology that Chinese companies are using in their platforms.[57] China is aiming to issue a national blockchain standard in 2022. In support of this goal, in July 2020 the International Telecommunications Union Study Group Sixteen, chaired by a representative from Huawei, accepted China's proposal for a framework blockchain standard project.[58]

China's real-identity requirements further strengthen the government's capabilities in blockchain. Red Date Technology, the Hong Kong–based technical engineer for BSN, can reportedly censor or delete blockchain users or networks due to a permission service that obligates users to identify themselves to the BSN operator.[59] BSN uses "public city nodes" that operate through data and cloud services that have installed its software and are linked to the BSN network.[60] BSN says it has 100 domestic and 7 global nodes—including in Paris, Sydney, and Tokyo—and aims to create an additional 150 domestically and 50 overseas.[61]

The Chinese government is leveraging access to foreign expertise to develop and deploy national blockchain technologies in digital platforms that will operate outside China. The University College Oxford Blockchain Research Centre directs the Oxford-Hainan Blockchain Institute in Hainan and the Chieftin Lab (China-Europe FinTech Innovation) in Shenzhen. In October 2021, MYEG Services Berhad—Malaysia's e-government service provider—announced an agreement with CAICT and its Industrial Internet and IoT Research Institute to expand China's Xinghuo BIF by introducing backbone nodes (machines running with relevant software) under the Zetrix brand.[62]

Open Platforms with Chinese Characteristics

China's digital platforms emphasize that they are open platforms, but they have key characteristics that challenge concepts of what it means to be open, including the role of the state and asymmetries in openness. These platforms are open only to the extent that Chinese firms are engaging in national technology development, trying to obtain certain foreign firm capabilities, or seeking to work around restrictions on some of China's leading technology firms, such as Huawei. China is not only leveraging foreign open platforms but also developing competitive alternatives.

Domestically, the Chinese government has promoted open platforms among its domestic technology firms to encourage information sharing in the development of national technologies. Recent Chinese government regulation of its major technology firms, including Alibaba, aims to ensure that national champions do not develop technology competencies that are walled off from each other and the state. Relatedly, China is advancing interoperability and common infrastructure and standards that, while often used in global markets to promote commercial development, could enhance state controls by integrating platform operations and aggregating data analytics.

---

57 "Xinghuo BIF 1024 Declaration Is Released to Promote the Development of Blockchain Talents and Industry Integration," *People's Daily*, October 27, 2021.

58 The People's Bank of China's Digital Currency Research Initiative introduced the proposal, but it also involved MIIT's CAICT and Huawei. "China's First Financial Blockchain International Standard Accepted as Project," *21st Century Business Herald*, September 4, 2020.

59 Anna Baydakova, "Inside China's Effort to Create a Blockchain It Can Control," CoinDesk, March 16, 2021.

60 Vipin Varathan, "BSN: The Internet of Blockchains," Medium, April 19, 2020.

61 Mikk Raud, "Knowledge Base: Blockchain-based Service Network (BSN, 区块链服务网络)," DigiChina, July 2, 2021.

62 See the Zitrix marketing presentation at https://www.youtube.com/watch?v=SVBbaSH-8Vo. It claims that users can build decentralized operations and that the platform offers trust-verification tools. "MoU Signed between MY E.G. Services Berhad (MYEG) and Institute of Industrial Internet & IoT, CAICT," PR Newswire, October 13, 2021.

The Chinese government's industrial plans for information technology and software development promote the use of open-source technology and its global community of expertise to advance innovation within an "open, collaborative, and international ecosystem."[63] In July 2020, however, MIIT indicated that it would promote Gitee as an independent open-source digital platform for China.[64] While Gitee's current level of activity is small in comparison to GitHub (the largest global code repository, with more than 40 million users and 206 million code repositories), China may value Gitee as an innovation digital platform it controls and as a possible future, China-centered competitor to GitHub. In the meantime, Gitee also allows China to hedge and potentially counter U.S. technology restrictions. For example, Huawei is hosting its operating system, HarmonyOS, on Gitee in an effort to expand globally despite U.S. export controls. In September 2021, China's OpenAtom Foundation—a Chinese alternative to the Linux Foundation—signed a strategic agreement with the Eclipse Foundation to host Huawei's HarmonyOS in Europe.[65] Greater regional or global acceptance of a Chinese operating system could allow Chinese firms like Huawei a way to expand digital platforms through apps on their own operating systems.

The attempt to brand China's digital platforms as open obfuscates the ways in which China's digital systems are closed to foreign digital competition and subject to state control. Chinese digital platforms' business strategies depend on other markets remaining open to them and reducing barriers in these markets to China and to one another. At the government level, China is focused on reducing other countries' barriers to China while keeping its own market closed. Moreover, the Chinese government is distorting concepts and practices in U.S. technology frameworks and business models for open collaboration and commercial competition. In innovation platforms, China is leveraging the openness of foreign research, technology, and commercial markets to obtain and develop the capabilities it needs to develop domestic competitors that aim to displace these leading experts and companies. Open-source technology models are based on principles of reciprocal openness and transparency that seek collaboration among academic and commercial actors.[66] China's business model, by contrast, is more top-down, being protected and controlled by the state. It emphasizes vertical integration and control of entire value chains and does not reciprocate foreign technology and market openness, including in areas where digital platforms are generating commercialized technologies. China's participants and operators of these digital platforms are state-tied. Its platforms may appear to be open, but that openness tends to be limited to areas where China seeks to obtain certain foreign expertise.

These digital platforms leverage Western concepts of open research to provide China a countermeasure to technology controls imposed by the United States, as well as by Europe and Japan, to gain the computer architecture, software, and hardware technologies and capabilities it needs from the outside to develop its own "indigenous capabilities."[67] These platforms exchange technologies and know-how that many governments consider sensitive with PRC institutes and companies of potential concern. While this type of exchange would otherwise be regulated

---

63 MIIT (PRC), "Five-Year Plan for IT and Software Development (2016–2020)." MIIT issued the new five-year plan for 2021–25 in November 2021.

64 Meaghan Tobin, "China Wants to Build an Open Source Ecosystem to Rival GitHub," Rest of World, January 19, 2021.

65 See "Eclipse Foundation and OpenAtom Foundation Forge a Strategic Initiative Focused on OpenHarmony OS," Globe Newswire, September 28, 2021; and "Eclipse Foundation Board of Directors," Eclipse Foundation, https://www.eclipse.org/org/foundation/directors.php.

66 Steven Weber, *The Success of Open Source* (Cambridge: Harvard University Press, 2004).

67 Sutter, "China's Recent Trade Measures and Countermeasures: Issues for Congress." See Table A-2 for examples of PRC participation in U.S. open-source technology digital platforms that include RISC-V, the O-RAN Alliance, the Open Compute Project, IBM Open Power Project, CHIPS Alliance, and the Open Hardware Group.

through government tools such as export controls, advanced technology collaboration on open-source technology platforms has not been restricted to date. Similarly, there has been little discussion among policymakers about whether current controls should be applied or whether new approaches are needed.[68]

Conclusion

Data is increasingly the underlying source of value in economic and geopolitical activity. The ability to access, analyze, leverage, and control data in a variety of interrelated and complex applications is increasingly powerful in the global economy, particularly for those commercial or state actors able to achieve dominant positions across sectors and domains. China's interest in data and understanding of its importance and sensitivity are well documented. CAICT assesses that data has become a "key factor in production," and that a "new digital technology-economic paradigm" is taking shape.[69] Defensively, China's policies restrict foreign access to its digital market and increasingly curtail the ability of foreign firms to collect or leverage data from China. Offensively, China's cybertheft and foreign acquisitions target industrial, government, and personal datasets and capabilities.

In the absence of national-level restrictions or global rules, China is moving quickly to establish its digital platforms. It is capitalizing on an ability to restrict digital infrastructure and platforms in China without consequences while its firms expand overseas in these areas. Chinese digital platforms have not faced antitrust actions and benefit from policy stasis in other countries on whether or how to consider the potential risks that China's digital platforms may pose. These potential risks include how China might use its unfair market practices to gain a global leadership role in digital platforms over time, as well as the role of the Chinese state in its platforms. These digital platforms are also breaking into sensitive and otherwise highly regulated foreign markets that are considered critical infrastructure, including finance, health, media, public utilities, telecommunications, and government services.

The growing global role of China's digital platforms offers the country increasingly powerful and complex capabilities to leverage global networks and data. To date, attention has focused on how China's digital platforms give it potential access to sensitive personal data internationally. But this is just the tip of the iceberg. China could also use these platforms to leverage and shape industrial, commercial, financial, and trading data. Control of digital platforms also allows an operator to deny, manipulate, and propagate information.

The international system has yet to respond to the growth and expansion of China's digital platforms and the challenges that they may pose to both national governments and the broader global system. Some Chinese firms are developing bifurcated digital platforms to separate aspects of their China and global businesses. In some cases, this is a response to China's digital sovereignty policies; in others, it is a response to foreign governments' defensive requirements that Chinese digital platforms establish a separate legal entity and data centers. However, such defensive measures leave outstanding questions about the extent to which the Chinese state may

[68] Sutter, "China's Recent Trade Measures and Countermeasures: Issues for Congress."

[69] "Digital Economy Development in China (2020)," China Academy of Information and Communications Technology, July 2020.

still have touchpoints and access, even over "firewalled" platforms.[70] Most international policy tools leveraged thus far to protect against China's digital platforms and the information superiority they might provide the Chinese government are tactical in nature and consider risks on a case-by-case basis. This approach may not appreciate the potential strategic economic, geopolitical, and national security challenges that the expansion of China's digital platforms might pose to other countries and the integrity of broader global digital architecture. In addition, these defensive tools are subject to the asymmetric pressures and constituencies that China's market protections have created. For example, TikTok and WeChat are major Chinese platforms uniquely able to operate in both China and the United States. The Trump administration's efforts to ban TikTok and WeChat from the U.S. market due to national security concerns faced pushback in part because of how such a restriction might curtail cross-border communication options. These arguments ignore the underlying reasons why Chinese firms have a unique ability to serve both markets, potentially rewarding Chinese government protectionist policies as a *fait accompli*.

[70] For a discussion of potential risks with regard to digital platforms that have strong ties to China, such as TikTok and Zoom, see Sutter, "China's Recent Trade Measures and Countermeasures: Issues for Congress."

APPENDIX: CASE STUDY OF HOW DIGITAL PLATFORMS EXPAND BEIJING'S INFLUENCE ABROAD

The PRC is using a wide array of tactics—many of which are being implemented as components of its Belt and Road Initiative and corresponding Digital Silk Road—to facilitate the proliferation of Chinese digital platforms abroad. In doing so, the Chinese government is working to secure greater access to global data, increase its control over information flows in third countries, shape the emerging digital ecosystems in developing countries, and ultimately exert greater influence over the global digital domain. There is a close relationship between China's agreements with other governments and the ways in which Chinese digital platforms are developing under these agreements in foreign countries. In many cases, Chinese platforms are formally structured as nonprofits or consortia. But these digital platforms are state-directed and -supported efforts. China's ability to access, assess, and act on data collected across global trade, currency, energy, and manufacturing platforms could give the state unparalleled influence because of how it could access data across platforms, either in a direct and open way or through back-office convergence. Chinese corporate investments overseas support the development of these digital platforms through the infrastructure and influence in corporate constituencies they are building in key functional areas. This platform expansion is also supported by Chinese government trade policies and government-to-government agreements that seek to reduce global trade barriers to China while its barriers remain intact.

China's platform ambitions are evident in a host of different industries and domains of interaction. In trade, Alibaba's eWTP (electronic World Trade Platform) is leading the Chinese government's efforts to create digital trade zones with partner countries and working to build out China's global logistics capabilities to support this platform. These efforts are shaping the architecture for digital trade. The Chinese government is also launching a digital currency and related platform to diversify away from its dependence on the U.S. dollar and promote alternative payment systems with other countries. It has reined in nonstate bitcoin operators and super app payment systems in order to bolster its state-controlled payment currency and emerging platforms. While Alibaba and Tencent are partners in the digital currency, the Chinese government is overlaying its own system and controls in its use of their digital platforms. In energy, the Chinese government is using a State Grid–affiliated research institute to advocate and develop institutional ties to promote global cross-border energy connectivity through a Chinese digital platform. This effort benefits from China's investments in renewable energy and power businesses in other countries. And in manufacturing, in order to enable the advanced manufacturing goals outlined in industrial policies such as Made in China 2025, China's digital industrial platforms are partnered with advanced manufacturing leaders in Germany to gain competencies.

China's digital platform strategy puts the country in a unique global position in which it benefits from access to both international and China-controlled digital platforms and related infrastructure while also maintaining barriers to overseas competition. This position could allow China a tutelary period in which its platforms can develop and mature in a protected environment while also learning from foreign systems. Unique access to both global and Chinese digital platforms allows China distinctive advantages to have greater visibility, control, and operational flexibility across these platforms. This unique dual access could position China not only to work around global

restrictions but also to be able to gain commercial, geopolitical, or military advantages by taking down a global platform while its own platform remains operable.

China's digital platforms aim to shape new emerging pathways for commerce, manufacturing, and innovation. These platforms realize the Chinese government's goals of shaping, controlling, and leveraging this emerging information architecture and the data generated from these networks. The examples that follow provide some details about the digital platforms China is developing and how they are evolving domestically and overseas. In each instance, while Chinese firms have the lead in developing these digital platforms, the platforms are advancing key government policy goals and enjoy government support.

Trade: Alibaba's eWTP

Alibaba's eWTP supports the Chinese government's larger efforts to establish a global leadership position for China in digital trade. The platform is branded as an NGO but has strong ties to the Chinese government and aligns with Alibaba's global logistics ambitions. The Chinese government initially proposed the concept for eWTP at the 2016 G-20 Leaders' Summit held in Hangzhou. Since then, the platform has expanded through a combination of government and company agreements and Chinese government domestic policies that have established digital free trade zones (FTZs). In April 2020 the Chinese government created the Yiwu Comprehensive Bonded Zone and Digital Customs Clearance Port, where eWTP operates. In September 2020 and September 2021 the State Council issued plans to create and expand pilot digital export zones, including in Beijing, Anhui, Hunan, and Zhejiang.[71] The Zhejiang FTZ plans promote the global role of eWTP and Zhejiang's role as one of two national agriculture and energy stockpiling bases. Plans include a soybean import pilot, the development of the Zhoushan port, and cross-border renminbi settlement.[72]

China and Malaysia's 2017 BRI memorandum of understanding paved the way for a digital FTZ between the two countries, and that same year Alibaba and the Malaysia Digital Economy Corporation (MDEC) launched the Malaysia Digital FTZ.[73] The zone includes a fulfillment hub and an e-commerce platform that leverages Alibaba's OneTouch e-services platform and Alibaba-controlled Lazada's e-commerce operations.[74] The deal builds on an existing e-trade program between Alibaba and MDEC that was created in 2014 to defray the costs of firms that used Alibaba's e-Trade Global Supplier Package.[75] Ahead of the October 2021 G-20 Leaders' Summit, Xi Jinping announced China's intent to join the Digital Economy Partnership Agreement (DEPA), an agreement launched by Singapore, New Zealand, and Chile. If China is allowed to join, the DEPA could allow it to promote eWTP and digital trade without having to make commitments—the agreement focuses on best practices and cooperation frameworks.[76]

---

71 Zhong Nan, Cheng Yu, and Zhou Lanxu, "Nation Promoting Digital Trade and Cooperation," *China Daily*, September 4, 2021.

72 "China Outlines Policy for New Storage Bases for Energy, Agri Imports," Reuters, September 21, 2020; and Eugene Lim, "China Launches Four Free Trade Zones," WTS Global, April 13, 2021.

73 Vasundhara Rastogi, "Malaysia's Digital Free Trade Zone," ASEAN Briefing, Dezan Shira and Associates, January 18, 2018.

74 Alibaba controls Lazada through investments it made between 2016 and 2018. See Jon Russell, "Alibaba Doubles Down on Lazada with Fresh $2B Investment and New CEO," TechCrunch, March 19, 2018.

75 Tham Siew Yean, "The Digital Free Trade Zone (DFTZ): Putting Malaysia's SMEs onto the Digital Silk Road," ISEAS–Yusof Ishak Institute, March 26, 2018.

76 Cissy Zhou, "China Applies to Join Digital Trade Pact with Singapore and New Zealand," *Nikkei Asia*, November 1, 2021.

Alibaba's eWTP seeks to expand China's digital networks in global trade, tourism, training, and technology. The platform aims to create a single ecosystem for logistics firms and provides certified logistics (e.g., labeling and parcel tracking), e-trading (e.g., customs clearance), and financing and payments (e.g., foreign exchange conversion and tax). It currently focuses on digital trade between China and Europe, Southeast Asia, and Africa through agreements with foreign airport authorities that have established six Alibaba warehousing facilities, or e-hubs, including in Belgium, Malaysia, Ethiopia, and Rwanda. The platform has an import hub in Hangzhou (where Alibaba is headquartered) and an export hub in Yiwu in Zhejiang Province. In addition, the platform currently has over 3,000 logistics partners, including the top 15 distribution firms in China and 100 firms operating globally. The platform promotes Alibaba's services, including its logistics firm Cainiao (China Smart Logistics Network, Ltd.), and participating e-hubs connect through Alibaba's OneTouch supply-chain management digital platform. Alibaba almost certainly gains data and insights from the manufacturing and logistics firms that use its platform. The platform also is poised to leverage China's expansion of transportation links, including rail and air cargo, between China and Europe and China and Southeast Asia.

Alibaba is investing in other platforms that could help it build out eWTP's capabilities and geographic reach, such as China's digital freight platform, the Full Truck Alliance.[77] The firm offers industry-wide logistics support, including freight matching and pricing. The founder previously worked as an Alibaba business-to-business executive, as did several other Full Truck Alliance leaders. While the Full Truck Alliance is focusing on China, it plans to provide cross-border services to BRI countries. By the end of 2020, the company had nineteen registered trademarks and one pending trademark in other countries, including India, Russia, and Vietnam.[78] The company's 2021 initial public offering in New York has provided U.S. capital in support of this expansion.[79]

Fintech: The Central Bank Digital Currency

China's central bank, the People's Bank of China (PBOC), has been developing a digital currency since at least 2014. This is part of an effort to establish a first-mover advantage in setting digital currency rules and standards. At the Bank of International Settlements (BIS) Innovation Summit in March 2021, China submitted a proposal on global digital governance that discusses its views for standards and norms on cross-border digital transactions, risk supervision, and the use and ownership of data. At the BIS event, the director of the Digital Currency Institute said that China seeks to be among the first to issue a sovereign digital currency as part of efforts to internationalize the renminbi, reduce dependence on the global U.S. dollar system, and safeguard China's monetary sovereignty.[80]

A central bank digital currency and global digital payments network could help China diversify away from the dollar and provide workarounds to U.S. dollar–based sanctions. It also could give China greater visibility and control of certain global financial flows.[81] A digital currency platform and related networks could allow China over time to expand the use of its digital currency across

---

77 The company was created in 2017 by merging competitor platforms Yunmanman and Houchebang and the software firm Jiangsu Manyun.

78 See Full Truck Alliance Co. Ltd., Form F-1 Registration Statement, as filed with the Securities and Exchange Commission on June 15, 2021.

79 Michael Hytha and Julia Fioretti, "China's Full Truck Climbs in Debut after $1.6 Billion IPO," Bloomberg, June 22, 2021.

80 "China Proposes Global Rules for Managing Sovereign Digital Currencies," Dezan Shira and Associates, April 4, 2021; and "China Suggests Principles for Cross Border CBDC to 'Avoid Dollarization,'" Ledger Insights, March 25, 2021.

81 See Rebecca M. Nelson and Karen M. Sutter, "De-Dollarization Efforts in China and Russia," Congressional Research Service, July 23, 2021.

its other platforms, allowing it a greater role in global payments and visibility into and control of these financial flows. As the first to market certain approaches, China also might seek to gain advantages in standardizing the technologies and systems it is using that could in turn be adopted by other countries. This potential for interoperability could allow China to expand the reach of its digital currency payment platforms.

PBOC engaged in domestic and overseas trials—including in Hong Kong, Thailand, and the United Arab Emirates—in the lead-up to the 2022 Winter Olympics as it prepares to officially launch its digital currency.[82] In 2016, PBOC established the Digital Currency Institute to lead national efforts. PBOC has filed 80 patents related to technologies and processes for issuing digital currencies, including interbank settlement and the integration of digital wallets and bank accounts.[83] In January 2021, it announced a joint venture (JV) with Belgium-based financial messaging service the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[84] The JV will build a storage center in China that will allow the PRC government to monitor and analyze cross-border payment messaging and build a localized network in China. The JV includes government shareholders that operate China's cross-border renminbi payments and settlements system for banking and nonbanking institutions.[85]

China may seek to align its new digital currency payment system with its other digital platforms, such as those in trade and retail e-payments. Alibaba and Tencent are among a small group that PBOC has entrusted to distribute its digital currency. In January 2022, Chinese Android and Apple app stores offered a pilot digital currency "e-CNY" app that was developed by PBOC's Digital Currency Institute for use in trial cities and locations in China hosting the Olympics.[86] While the Chinese government is seeking to leverage these firms' platforms to launch PBOC's digital currency, it may impose new state overlays, controls, and players and combine certain networks and systems.[87] PBOC, for example, is including China UnionPay (CUP) in its effort in a sign that CUP might lead business use of the currency and payment settlements.[88] Similarly, China's national blockchain technology could be used within these digital payments, which could allow greater interoperability and also points of visibility and control for the state.

Smart Grids: Global Energy Interconnection

The Chinese government through its national monopoly and champion, State Grid, is promoting a global energy digital platform for cross-border data sharing and the trading and transmission of renewable energy to supply countries' national electric grids. In September 2015, Xi Jinping introduced the Global Energy Interconnection proposal for China to connect (and

---

82 Frank Tang, "China Digital Currency: China, Hong Kong Begin Testing Digital Yuan as Beijing Ramps up Research into Cross-Border Use," *South China Morning Post*, April 2, 2021; and "Joint Statement on Multiple Central Bank Digital Currency (m-CBDC) Bridge Project," Hong Kong Monetary Authority, February 23, 2021, https://www.info.gov.hk/gia/general/202102/23/P2021022300482.htm.

83 Hannah Murphy and Yuan Yang, "Patents Reveal Extent of China's Digital Currency Plans," *Financial Times*, February 12, 2020.

84 SWIFT is the current global system that facilitates electronic financial transactions.

85 Shareholders include China's Cross-border Interbank Payment System and the Payment and Clearing Association of China. See "China Central Bank Says New SWIFT JV Will Set Up Localized Data Warehouse," Reuters, March 23, 2021.

86 Coco Feng, "China Digital Currency: e-CNY Wallet Lands in App Stores Ahead of Winter Olympics 2022," *South China Morning Post*, January 4, 2022.

87 Alibaba and Tencent have invested heavily in fintech services as a key profit center for their super apps. Alipay loans to businesses and individuals in close to real-time transactions based on its Sesame Credit scoring system. Tencent's WeChat wallet is ubiquitous in China.

88 PBOC created CUP in 2002 as a state monopoly to provide credit card settlement in China and overseas. CUP aggressively blocked U.S. competitors Visa, MasterCard, and American Express from the Chinese market while expanding globally. See U.S. Trade Representative, "China—Certain Measures Affecting Electronic Payment Services (DS413)," written submission of the United States of America to the World Trade Organization, September 20, 2011.

control) power grids around the world.[89] China's plan includes both improvements to physical grid infrastructure and, relevant for this case study, developing Chinese smart platforms to manage these newly connected grids. The plan promotes Chinese renewable technologies and products (wind, solar, and hydropower) and State Grid's ultra-high voltage AC/DC hybrid-power grid that it can overlay on traditional grids to transmit renewable energy.[90] By 2050, China seeks to operate and control one intercontinental grid, seven cross-border grids, and eighteen regional interconnections through its digital platform.

The Chinese government argues that cross-border energy trading and grid integration are inherently positive developments but proposes to advance these practices through its digital energy platform with no commensurate cross-border liberalization of China's own power sector. China's power sector would remain under state monopoly control with one-way cross-border digital connectivity that would vertically integrate China's control over cross-border power data, trade, transmission, and connectivity. The Chinese government is advocating its digital platform concept through a State Grid research organization, the Global Energy Interconnection and Development Cooperation Organization (GEIDCO), that is headed by the former chairman of State Grid. GEIDCO has offices around the world, including in New York City. The organization presents itself as a nonprofit research institute but is controlled by State Grid and tied to the government's China Electric Power Research Institute (CEPRI). CEPRI oversees China's national key labs in energy that lead in developing relevant national technologies and standards that support State Grid's energy platform.[91] CEPRI also oversees the development and operation of China's domestic digital platform for electric power allocation and trading. It is poised to play a key role in any regional or global digital platform that GEIDCO would develop.[92]

GEIDCO's first step in the development of its digital energy platform has focused on data and research. Its global research platform, Nenglian, includes data, trading, and government and company information. The Global Energy Connection platform includes supply/demand energy data, global flows of technology, capital, energy, and talent and allows for data and information sharing with the eventual goal of real-time data sharing, energy trading, and power transmission.[93] To develop the platform from the technology infrastructure side, State Grid and China's other state monopoly in the power sector, China Southern Power Grid, are working with Huawei's global energy business unit to use its data and cloud services. Huawei provides these firms cloud-based data services for their smart-grid operations in China. Huawei says it is supporting the power grids in Qinghai Province and Shenzhen as well as 190 electric power companies worldwide, including

---

89 Xi tied this plan to the United Nations' 2030 Agenda for Sustainable Development and outlined how it could address global power demand with clean energy. "Remarks of Xi Jinping at the UN Development Summit," Xinhua, September 27, 2015, http://www.xinhuanet.com/world/2015-09/27/c_1116687809.htm.

90 Huang Lei and Wang Qiankun, "Global Energy Interconnection: A Bold Initiative for a Sustainable Energy Future," *Horizons: Journal of International Relations and Sustainable Development* 17 (2020): 268–81.

91 Yin Bo, "Adhere to Openness and Win-Win Cooperation and Move into an Era of Global Energy Interconnection," GEIDCO presentation, February 7, 2019. CEPRI oversees three State Council–level state key labs in China that are developing power grid and storage technologies and standards relevant to GEIDCO's plan. The three labs are the State Key Lab on Power Grid Security and Energy Conservation, State Key Lab on New Energy and Energy Storage Operations Control, and State Key Lab on Power Grid Environmental Protection. See CEPRI's website at http://www.epri.sgcc.com.cn/html/epri/col2019102101/column_2019102101_1.html.

92 Following Chinese government power reform of electricity allocation and sales in 2015, CEPRI worked on behalf of State Grid with Huawei Cloud to develop a platform. See "Several Opinions of the CPC Central Committee and the State Council on Further Deepening the Reform of the Electric Power System," 2015; and Huawei Cloud website, https://www.huaweicloud.com/en-us/cases/1517799381278.html.

93 GEIDCO, "Research Report on the Belt and Road Energy Interconnection," April 2019.

state electricity operators in Saudi Arabia, Thailand, and Turkey.[94] The Chinese government could leverage ties to these power systems to advance GEIDCO's digital power platform.

While its digital energy platform concept may seem overly ambitious and difficult to achieve, GEIDCO could gain traction by leveraging its research on regional energy infrastructure and systems (including in North America) to advocate as a research institute with foreign universities, industry associations, and government partners about why cross-border liberalization is needed. In the developed world, GEIDCO is appealing to environmental interests in clean energies and efficiencies. In the developing world, it is working with countries that lack energy access and may assess that current energy distribution systems are unfair. GEIDCO is also leveraging ties to countries where China has built power infrastructure as well as China's ties to the United Nations and regional development banks.[95] GEIDCO could influence other countries' views of its digital energy platform through China's control of renewable power generation and power operator companies in these countries, an area of significant Chinese investment.[96]

Manufacturing: Industrial Digital Platforms

China is prioritizing the digitalization of manufacturing and the use of the IoT to promote advanced manufacturing in China, particularly among its state industrial firms. In most instances, these digital platforms involve technology transfer and the sharing of foreign manufacturing capabilities that China is seeking in its industrial policies, such as Made in China 2025. These platforms give China access and visibility to advanced knowledge and research overseas, as well as, if networks are not properly secured, to potential sensitive digital touchpoints into foreign competitors' trade secrets and proprietary manufacturing processes.

Chinese industrial policies and state subsidies promote industrial platforms, and the government considers cross-sectoral platforms as national champions.[97] The Ministry of Industry and Information Technology (MIIT) published a three-year industrial internet action plan, first in 2019 and again in 2021, to provide direction and incentives for the development and use of the IoT to promote advanced manufacturing.[98] The Chinese Academy of Sciences' Shenyang Institute of Automation hosts China's national Key Laboratory for Networked Control Systems and leads the development of technologies underpinning China's intelligent manufacturing systems.[99] MIIT has created several alliances since 2016 to align government and corporate efforts in developing

---

94 Huawei FusionPlant operates domestically, and OceanConnect operates in foreign markets. Huawei offers smart photovoltaic solutions and IoT architecture for State Grid. See the Huawei Cloud website, http://huaweicloud.com/solutions/fusionplant; and "Power Industry Needs Urgent Transformation," TradeArabia, July 9, 2020.

95 In 2018, GEIDCO leveraged its ties with Guinea—where China developed the largest hydropower project in West Africa—to form the African Energy Interconnection and Sustainable Development Alliance among twenty cities. GEIDCO, for example, conducted a joint study with the ASEAN Center for Energy and the UN Economic and Social Commission for Asia and Pacific and worked with the Asian Development Bank on its Mekong Subregion project. Under BRI, GEIDCO has negotiated with the South Korean government and KEPCO. GEIDCO has also worked with the Latin American Energy Organization on clean energy research and financing. See Edward Downie, "Powering the Globe: Lessons from Southeast Asia for China's Global Energy Interconnection Institute," Center on Global Energy Policy, Columbia University, April 23, 2020.

96 Through land and corporate acquisitions, China operates extensive solar and wind farms overseas, including in the United States, and is the controlling shareholding in power operators, such as Portugal's EDP, which operates more broadly in Europe, the United States, and South America.

97 In November 2017, the Chinese government issued the "Guiding Opinions on Developing the Industrial Internet by Deepening Internet Plus Advanced Manufacturing." In 2018, MIIT issued its first set of 93 industrial internet projects to encourage the development of industrial digital platforms.

98 Caroline Meinhardt, Anna Holzmann, and Gregor Sebastian, "MIIT Accelerates Industrial Internet Applications and Standard Setting in Traditional Manufacturing," MERICS, March 2, 2021.

99 See "Digital Factory Department," Shenyang Institute of Automation, Chinese Academy of Sciences, http://english.sia.cas.cn/rh/rd/201402/t20140227_116971.html.

industrial internet platforms and related technologies, systems, and standards. These groups include the Edge Computing Association (ECA)[100] and the Alliance for the Industrial Internet (AII).[101] In 2018, the ECA signed a memorandum of understanding with the IEEE Standards Association to codevelop edge-computing standards.[102]

Many of China's industrial digital platforms rely on strategic partnerships with foreign firms for software and cloud service support while China develops its domestic providers. Foreign digital platforms that compete and partner with China include Microsoft's Azure, PTC's ThingWorx, Siemens' MindSphere, and SAP's HANA Cloud Platform. Some of these foreign platforms use Chinese cloud providers in order to operate in China.[103] In an effort to foster the development of indigenous software capabilities, China's construction equipment firm Sany incubated the industrial internet platform provider ROOTCLOUD.[104] Several executives with another platform provider, Beijing Sysware, have a background in state aircraft production—a key sector of interest for advanced manufacturing. Other emerging providers that China is developing include Guoxin Lucent Technologies, You Ye, CyberInsight, NeuCloud, Zhejiang SUPCON, and MJ Intelligent Systems.

China's industrial platforms seek to develop the country's advanced manufacturing capabilities by digitizing manufacturing, sharing know-how across companies and industries within China, and transferring foreign advanced manufacturing capabilities to China. These platforms facilitate the transfer of advanced manufacturing capabilities and talent training from leaders in the field such as Germany. This industrial digital platform cooperation with Germany stems from government agreements on advanced manufacturing and Industrie 4.0 that Germany and China signed in 2015 and 2016. In a sign that this cooperation is valuable to China, its 2021 industrial internet action plan seeks to deepen ties and emphasizes developing industrial internet platforms that connect with Europe.[105] Among prominent examples, the German government and German companies support the industrial cloud platforms INDICS and CASICloud of China's space defense firm China Aerospace Science and Industry Corporation (CASIC). INDICS has an office in Germany and operates a testbed with TU Darmstadt. Haier's COSMOPlat industrial digital platform has research ties to Germany's Aachen University's Industrie 4.0 Institute. The platform also supports a partnership between the Tianjin Research Institute for Advanced Equipment and the German Fraunhofer Logistics Research Institute.[106] China's Xuzhou Construction Machinery Group (XCMG) operates an industrial digital platform in Germany that focuses on technology transfer and talent training for its operations in Germany and in China.[107]

---

100 The head of the Chinese Academy of Sciences' Shenyang Institute of Automation chairs the ECA. Other participants include the China Academy of Information and Communications Technology, Huawei, U.S. semiconductor firms Intel Corporation and ARM, and the U.S.-based platform service developer iSoftStone. See Ken Briodagh, "Chinese IoT Edge Computing Consortium Established," IoT Evolution, December 1, 2016.

101 AII includes China's national technology champions, state telecom firms, and several foreign manufacturers, such as Advantech, Foxconn, General Electric, Schneider Electric, and Siemens. See Rebecca Arcesati et al., "China's Digital Platform Economy: Assessment Developments Toward Industry 4.0," MERICS, May 29, 2020.

102 See the ECA website, http://en.ecconsortium.net/Lists/show/id/136.html.

103 Siemen's MindSphere uses Aliyun to operate in China.

104 See the ROOTCLOUD exhibitor webpage from the 2021 HANNOVER MESSE exhibition, available at https://www.hannovermesse.de/exhibitor/rootcloud-technology/N1436810.

105 Meinhardt, Holzmann, and Sebastian, "MIIT Accelerates Industrial Internet Applications."

106 Other partners include Chinese companies Alibaba, BaoSteel, China Telecom, and Huawei and German firms Bosch, Echlebracht, and SAP.

107 XCMG has had an R&D center in Germany since 2012, the same year it acquired the German company Schwing, a producer of cement truck mixers and sludge pump systems. XCMG is partnering with the HWK Erfurt Vocational Training Center as a model to develop XCMG's Technical College.

Conclusion

The platforms highlighted in this case study cover some of the key areas where Chinese platforms are working toward state objectives of greater global influence in and control over emerging digital architecture. Through these examples, this study seeks to demonstrate a pattern of Chinese platforms' efforts to advance state goals. Similar strategies are being carried out across a range of sectors. These actions highlight the process and specific pathways through which the Chinese government could expand its global digital influence: while several platforms are in early stages of development, they reflect the PRC's broader digital ambitions.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 3

Setting the Standards: Locking in China's Technological Influence

Emily de La Bruyère

EMILY DE LA BRUYÈRE is Co-founder of Horizon Advisory, a consulting firm focusing on the implications of China's competitive approach to geopolitics, as well as a Senior Fellow at the Foundation for Defense of Democracies and a Nonresident Fellow at the National Bureau of Asian Research. She can be reached at <emily@horizonadvisory.org>.

EXECUTIVE SUMMARY

This chapter examines how China, fueled by its unmatched size, centralization, industrial capacity, and resolve, is competing to lead international standard setting in order to control emerging digital markets, as well as to shape technological and commercial evolution.

MAIN ARGUMENT

Beijing's digital strategy hinges on setting emerging technical standards globally. Standard setting promises Chinese commercial players an advantage in defining digital infrastructure. In addition, it locks in Chinese influence over emerging digital governance. More broadly, standard setting allows China to shape the future of technological development and commercial hierarchies in an enduring fashion. Beijing pursues its standards strategy through international standard-setting bodies, international investments and commercial footholds, and regional and national standard-setting partnerships. In the process, it benefits from size, as well as centralization that allows it to leverage that size by ensuring coordination among Chinese actors both in developing standards and in promoting them internationally. Unmatched industrial capacity also offers China influence over the commercial ecosystems that develop *de jure* standards and define *de facto* ones. And the lure of China's market incentivizes international players to comply with Beijing's national standards. China also benefits from the fact that it is actively competing to set international standards, while other countries tend not to. Beijing treats technical standard setting as an opportunity, and strategic imperative, of the digital revolution.

POLICY IMPLICATIONS

- China's influence over standards is both growing and greater than most analysts recognize. The stakes are enormous for international prosperity and security: standards constitute the rules of new-type geopolitical power in a digital environment.
- No other country is likely to rival the structural advantages that China brings to bear in standard setting. A tit-for-tat competition is unlikely to succeed. Instead, an effective response to China's standards strategy will demand international coordination among private- and public-sector actors across not only formal standards bodies but also informal commercial and industrial partnerships that shape the standards environment on the ground.
- A competitive response should include pushing for greater transparency in international standard setting, defending against China's efforts to co-opt cooperation, and promoting a proactive standards development agenda.

In October 2021, the Central Committee of the Chinese Communist Party (CCP) and the State Council issued the National Standardization Development Program. The program details a fourteen-year, national-level project to develop technical standards—especially in emerging and digital domains—and export them globally. The underlying goal is simple: "comprehensive competitiveness."[1] "In the past five years," declared Zhang Xiaogang, former chair of both the International Organization for Standardization (ISO) and the China Iron and Steel Association, "China has been recognized by all countries in the world as the country that has made the greatest contribution in the field of international standardization."[2]

Technical standards are established norms or requirements for engineering or technical criteria. These are the rules that permit interoperability across countries, technologies, and industries. 4G (fourth generation) telecommunications is a standard and constitutes the internationally accepted suite of technologies that allow mobile handsets and other network-connected devices to communicate. Likewise, HTML (Hypertext Markup Language) is a standard language used by every webpage. ISO/IEC 27001, an international certification standard for information security, constitutes a set of best practices for organizations handling sensitive data. Standards represent the technical rule sets for globalization, as well as the information technology (IT) that fuels it.

By extension, standards are a key factor in enabling market dominance.[3] An entity that sets a technical standard can lock in an essential role for its product or technology. If, for example, patented Huawei technology becomes incorporated into international 5G standards, every system built using these standards will have to pay Huawei to license its technology.[4] Huawei will also claim a competitive advantage in markets supporting and based on 5G standards. This advantage endures. Like all rule sets on which complex systems are built, once established, standards are difficult to uproot. Further, in many digital environments, standard setters are also able to shape how their technological or industrial ecosystems evolve—and therefore to stay ahead of innovation within them. Zhang Xiaogang argued in a 2020 speech that in an IT environment, "standards lead products and industries. This is a new trend that has emerged with global technological developments."[5] Using 5G as an example, and suggesting that 5G standards will determine the development direction of new technologies such as domestic-use robots, Zhang concluded: "The leader of the standard must be the leader of technology and the controller of the market."[6]

Beijing's digital strategy hinges on setting emerging technical standards globally. Standard setting promises Chinese commercial players an advantage in defining digital infrastructure and exporting digital platforms. This is a mutually reinforcing process: defining and exporting these also grants China an advantage in setting their technical rules. In addition, standard setting locks in Chinese influence over emerging digital governance. More broadly, it allows China to shape the future of technological development and commercial hierarchies in an enduring fashion,

---

1 Central Committee of the Chinese Communist Party (CCP) and the State Council Information Office of the People's Republic of China (PRC), 国家标准化发展纲要 [National Standardization Development Program] (Beijing, October 2021).

2 "专家:中国成为近五年在国际标准化领域全球贡献最大国家" [Expert: China Has Become the World's Largest Country in the Field of International Standardization in the Past Five Years], CCTV, August 12, 2020.

3 "It is precisely because Intel established the central processing unit (CPU) standard, Microsoft controlled the operating system standard, and Apple led the mobile phone application standard that these giants have the 'discourse power' in international market competition and value distribution," explained the *China Daily* in October 2021. 强化贸易便利化标准支撑 提升我国标准化对外开放水平 [Strengthen the Support of Trade Facilitation Standards, Improve the Level of China's Standardization and Opening to the Outside World], *China Daily*, October 14, 2021.

4 This is an example of a "standard-essential patent" (SEP). SEPs are patents that are necessary, or essential, for a given standard.

5 "专家:中国成为近五年在国际标准化领域全球贡献最大国家."

6 Ibid.

with direct implications for market competition as well as political, normative, economic, and technological influence.

Beijing pursues its standards strategy through international standard-setting bodies, such as the ISO; international investments and commercial footholds, such as infrastructure construction; and regional and national standard-setting organizations, such as the Association of Southeast Asian Nations (ASEAN) and the Association Française de Normalisation. In doing so, Beijing leans not only on government entities but also on companies, universities, and research institutions—all of them guided by Chinese digital industrial policy.[7]

This chapter examines China's standardization ambitions, the influence that the country has secured thus far, and the mechanisms that it uses to expand that influence. It finds that in international standard setting, Beijing benefits from asymmetric structural advantages. Size grants China a significant voice in international standards organizations; centralization allows it to take advantage of that voice, ensuring coordination among its commercial, academic, and government entities—both in developing standards (e.g., for complex systems like smart cities) and in promoting them internationally. Furthermore, unmatched industrial capacity (e.g., in telecommunications) offers China outsized leverage over the commercial ecosystems that develop *de jure* standards and define *de facto* ones. The lure of China's market incentivizes international players to comply with its national standards. Finally, China also benefits from the simple fact that Beijing is actively competing to set international standards. Other national governments tend not to.

This chapter finds that China's standards influence is both growing and far greater than most analysts recognize. Whether national governments recognize as much or not, the stakes are enormous for international prosperity and security: standards constitute the rules of new-type geopolitical power.

This chapter begins by detailing the strategic framework for Beijing's standards ambitions in emerging digital domains. It then describes the international standards ecosystem, before assessing China's influence in that ecosystem based on membership and especially leadership in international organizations, Beijing's ability to leverage that representation, and the network of regional and bilateral standards cooperation efforts that allow Beijing to shape the incentives and agendas of other countries and regional organizations.

China's Strategic Framework for Standards

Companies have long recognized the strategic value of international standards and actively compete in their development.[8] By contrast, countries have traditionally treated standard setting as a collaborative endeavor, emphasizing rules and cooperation. They have approached standards as tools through which to create a non-zero-sum, globally connected commercial and

[7] The National Standardization Development Program defines this as "an international standardization work mechanism with government guidance, enterprise entities, and industry-university-research linkages." Central Committee of the CCP and the State Council Information Office (PRC), 国家标准化发展纲要.

[8] For example, in 2007 the member countries of ISO, one of the world's preeminent standard-setting organizations, voted on Microsoft's Office Open XML (OOXML) standard, the native file format for Microsoft Office's 2007 suite. As they prepared to do so, Microsoft launched a drawn-out lobbying campaign. The company reportedly stacked delegations with supporters, stuffed ballots, and outright bought votes. This campaign caused an uproar: movements erupted calling on members to vote against OOXML, and IBM threatened to leave ISO and other software-relevant standards bodies. But the campaign also worked, and ISO ratified OOXML. This marked a tremendous victory for Microsoft. Some governments and institutions mandate use of ISO-approved document standards, and OOXML's ratification locked in Microsoft's control over these markets as well as anyone seeking interoperability with them. See Michael Calore, "Microsoft Allegedly Bullies and Bribes to Make Office an International Standard," *Wired*, July 21, 2007; and Jeremy Kirk, "IBM Threatens to Leave Standards Bodies," *New York Times*, September 23, 2008.

technological environment.[9] China, however, is an exception. As one standards consultant put it in an interview for this project, "historically, countries haven't asked what happens if I don't follow the rules. But now China is asking that question." According to Shu Yinbiao, chair of the International Electrotechnical Commission (IEC) and academician of the Chinese Academy of Engineering, "a country's international standardization level reflects that country's comprehensive strength and core competitiveness."[10]

Beijing's competitive approach to standards is not new. For two decades, government planning and authoritative discourse have emphasized the imperative of exporting Chinese technical standards globally. The Main Points of National Standardization Work released by the Standardization Administration of China (SAC) in 2008 explained that Beijing sought international standards influence "so that China's leading enterprises will truly lead the entire global industry and lead the future."[11] As a *Zhejiang Daily* article put it in 2015, "standards are the commanding heights, discourse power, and the power to control. Therefore, 'the one who obtains the standards gains the world.'"[12]

Beijing's standard-setting strategy has received new emphasis—and taken on new significance—since 2015. In part, this is a function of China's growing international influence in industrial competition and corresponding assertiveness.[13] China's heightened emphasis on standard setting also stems from a diagnosis of new strategic opportunity: Beijing sees today's industrial revolution as a chance to challenge developed economies' long-standing control of international standards. Chinese analysts also explain that the networked nature of information technology makes standards a particularly critical battleground in the digital revolution.

In 2015 the State Council issued the National Standardization System Construction and Development Plan (2016–2020).[14] The plan outlined a set of key, high-level goals for the five-year period: China would participate in at least half of all standards drafting and revision in recognized international standard-setting bodies, strengthen its role in these bodies' governance, increase the number of Chinese-held leadership positions in their technical committees and working groups, and use overseas construction contracts and equipment exports to promote Chinese standards.[15] "By 2020," the document projected, "China's influence and contributions toward setting international standards [will] have greatly increased, and China [will have] entered the ranks of the world's standards powers."[16] In 2018 the SAC launched the two-year China Standards 2035

---

[9] Author interviews. For additional context on this approach, see Giulia Neaher et al., "Standardizing the Future: How Can the United States Navigate the Geopolitics of International Technology Standards?" Atlantic Council, October 14, 2021.

[10] "唱响国际标准的中国强音! 2020国际标准峰会在京举办" [Sing China's Strong Voice in International Standards! 2020 International Standards Summit Is Held in Beijing], China Electric Power News, December 7, 2020.

[11] Standardization Administration of China, 2008年全国标准化工作要点 [Main Points of National Standardization Work in 2008] (Beijing, March 2008).

[12] Guo Zhanheng, "习近平标准化思想与浙江实践" [Xi Jinping's Standardization Thought and Zhejiang Practice], *Zhejiang Daily*, September 25, 2015.

[13] See, for example, Emily de La Bruyère, "China's Quest to Shape the World through Standards Setting," Hinrich Foundation, July 13, 2021, https://www.hinrichfoundation.com/research/article/tech/china-quest-to-shape-the-world-through-standards-setting.

[14] State Council Information Office (PRC), 国家标准化体系建设发展规划(2016-2020年) [National Standardization System Construction and Development Plan (2016–2020)] (Beijing, December 2015).

[15] See discussion in US-China Business Council, "China in International Standards Setting: USCBC Recommendations for Constructive Participation," February 2020, https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.

[16] State Council Information Office (PRC), 国家标准化体系建设发展规划(2016–2020年).

research program, intended to establish the foundation for a national standardization strategy.[17] In 2021, Beijing issued the Standards Development Program.

This new wave of Chinese ambitions has targeted emerging, digital technologies. "Emerging industry standards are particularly valued," declared Zhang Xiaogang in a 2020 speech.[18] The same year, a *Global Times* article explained that "China intends to lead the formulation of technology rules," and therefore "promote the cultivation of 5G and AI industries."[19] The SAC's Main Points of National Standardization Work in 2021 highlights the importance of standards in "new generation information technology systems," including the Internet of Things (IoT), artificial intelligence, big data, blockchain, IPV6 (Internet Protocol version 6), new infrastructure, information and information infrastructure security, the industrial internet and intelligent manufacturing, and unmanned aerial vehicles, smart cars, smart ships, smart roads, and smart car data collection.[20] The Ministry of Industry and Information Technology's Main Points of Industrial and Informatization Standards Work in 2021 provides a similar list of priority digital domains for standard setting.[21]

The logic behind this prioritization is straightforward. China's larger industrial strategy hinges on claiming an advantage in emerging, digital technologies. Standards provide an avenue to secure this superiority. The last industrial revolution proved as much—the United States, Europe, South Korea, and Japan were able to dominate in large part because they controlled international standards. As long as the technological paradigm remained unchanged, Beijing could only challenge their standards control at the margins due to the lasting structural advantage in technological and commercial competition that standards provide. However, new industrial revolutions bring new rule sets and the chance to leapfrog the incumbent hierarchy. Moreover, the nature of digital technologies is likely to make standards more strategically significant. Information technology is networked, which makes standards critical for its development. Chinese discourse suggests that in a world based on integration, standards are what govern and permit that integration.

Du Chuanzhong of Nankai University explains these points clearly in a 2019 *Social Science Frontiers* article. He writes that the fourth industrial revolution has catalyzed a new international technology competition that "mainly depends on the ability to control intellectual property rights, architectures, and interface standards" because the digital revolution hinges on "integration of different modules in the value chain through a global value network." Such integration "can only be realized when a globally consistent international standard is formulated." Therefore, "the country that takes the lead in dominance over international standards will enjoy the first-mover advantage in the fourth industrial revolution…the control

---

17 Standardization Administration of China, "'中国标准2035'项目结题会暨'国家标准化发展战略研究'项目启动会在京召开" ["China Standard 2035'"Project Closing Meeting and "National Standardization Development Strategy Research" Project Kick-Off Meeting Was Held in Beijing], January 15, 2020.

18 "专家:中国成为近五年在国际标准化领域全球贡献最大国家."

19 "国际标准制定，中国加强存在感 以占据竞争优势" [Setting International Standards, China Strengthens Its Presence in Order to Gain a Competitive Advantage], *Global Times*, July 31, 2020.

20 Standardization Administration of China, 2021年全国标准化工作要点 [Main Points of National Standardization Work in 2021] (Beijing, April 2021).

21 Ministry of Industry and Information Technology (PRC), 2021年工业和信息化标准工作要点 [Main Points of Industrial and Informatization Standards Work in 2021] (Beijing, March 2021).

of the new generation of information technology standards will become the commanding heights of the future international industry competition."[22]

Du argues that the industrial revolution grants China the opportunity to establish such a lead. He explains that the United States defined the standards of the IT revolution of the 1970s, claiming a "first-mover advantage in technology" and, with it, an "enduring competitive advantage in information technology standards." But now that advantage is up for grabs: "With the birth of the fourth industrial revolution, the international standards competition pattern…has undergone significant changes. The competitive advantage in standards is shifting from developed countries such as the United States to emerging economies represented by China."[23]

The Formal Standard-Setting Ecosystem

Understanding China's approach to and influence over standards requires understanding the international standards ecosystem itself. Most global technical standards are formed and ratified through international standard-developing organizations (SDOs), standard-setting organizations (SSOs), and market-based consortia. There is little consensus on the precise distinctions between these. However, generally speaking, SDOs are organizations dedicated to crafting standards (usually within dedicated working groups), while SSOs ratify them. Consortia are like SDOs but focus on specific industry verticals. There are thousands of these entities internationally, forming a convoluted, interconnected, and sometimes even competitive web. This is not a neat, mappable, or clearly hierarchical network. A standards consultant interviewed for this report describes it as a "rat's nest."[24]

That said, three standard-setting organizations are widely accepted to have the most leverage internationally: ISO, IEC, and the International Telecommunications Union (ITU). Together, these three organizations constitute the World Standards Cooperation (WSC).[25] They are global and have nation-state members, and accordingly have more formal influence than any other standards bodies.

ISO develops and publishes international technical, industrial, and commercial standards, while IEC handles international standards for all electrical, electronic, and related technologies. Membership for both ISO and IEC is composed of one representative per country, subordinate to that country's national standards body (NSB).[26] NSBs can be government (e.g., the SAC) or nongovernment (e.g., the American National Standards Institute) entities, or a combination of the two. As with most standards organizations, standards development and deliberations at ISO and IEC take place in technical committees or subcommittees, all of them with a specific focus area (e.g., screw threads or surge arresters). The two organizations collaborate on work related to information and communications technology (ICT) through a joint technical committee: ISO/IEC Joint Technical Committee 1 (JTC 1).

---

22 Ministry of Industry and Information Technology (PRC), 2021年工业和信息化标准工作要点."

23 Ibid. Du is not alone in making these points. A 2020 speech by Zhang Xiaogang makes a similar point in its argument about standards leading innovation in an IT environment. See "专家: 中国成为近五年在国际标准化领域全球贡献最大国家."

24 See, for example, Open Web Standards Network Map, https://joryburson.com/standardization-project.

25 International Telecommunication Union, "World Standards Cooperation (WSC)," https://www.itu.int/en/ITU-T/extcoop/Pages/wsc.aspx.

26 This is made up of manufacturers, providers, consumers, distributors and vendors, governmental agencies, and trade associations.

ITU is the United Nations' specialized agency responsible for ICT and consists of three sectors: ITU-T develops technical standards to ensure interconnectivity and interoperability of international ICT systems, ITU-R allocates global radio spectrum and satellite orbits, and ITU-D works to improve access to ICT across the developing world. ITU has 193 member states, including every UN member except Palau, plus the Vatican City. In addition, it has hundreds of individual members representing government, private, and academic sectors.

ISO, IEC, and ITU are complemented by an extensive network of additional ICT-standards bodies. Some, like the high-profile European Telecommunications Standards Institute (ETSI), are international and wide-ranging in their focus. ETSI's committees cover everything from emergency communications to IPv6. Others are more narrowly scoped. For example, the World Wide Web Consortium (W3C) focuses on standards for, as the name suggests, the World Wide Web. Some standards bodies are formed through partnerships of other standards organizations. For example, ETSI, Japan's Association of Radio Industries and Businesses (ARIB) and Telecommunication Technology Committee (TTC), China Communications Standards Association (CCSA), Telecommunications Standards Development Society, India (TSDSI), South Korea's Telecommunications Technology Association (TTA), and the Alliance for Telecommunications Industry Solutions (ATIS) of the United States together formed the 3rd Generation Partnership Project (3GPP) in 1998. The same seven SDOs, as well as the Telecommunications Industry Association, established an IoT-focused partnership, oneM2M, in 2012. In many cases, the standards developed in these organizations feed into ISO, IEC, and ITU pipelines. As an interviewee explained, "if you're an industry, and your standards group wants to make a global standard, ultimately it will have to bubble up to ISO/IEC JTC 1" or ITU.

Some regional and subregional organizations also have standards bodies. For example, the ASEAN Consultative Committee for Standards and Quality sits under the purview of the ASEAN economic ministers. These tend not to develop their own standards. Instead, they review existing global standards and decide whether to adopt them.

Importantly, not all countries or regions treat standards and their development in the same way. The United States tends to follow a market-driven approach: companies form standards of their own volition and through their own partnerships, with little government attention. By contrast, the European Union and its member governments are more involved in the process.[27] And in China, most standard setting is government-led, and companies and academic entities receive state support for participation in international standardization.[28]

Finally, not all standards are set through standard-setting bodies. In some cases, companies create less formal standardization agreements among themselves, namely through multi-source agreements (MSAs). MSAs allow multiple manufacturers to produce a compatible set of products and constitute de facto standards. They are growing in popularity today, as the long, cumbersome process of standard setting stymies efforts to keep up with shortening product and technology life cycles.[29]

---

27 Take, for example, the Multistakeholder Platform (MSP). The MSP was launched after the EU Commission resolved to advise on matters relevant to implementation of an ICT standardization work program. Its main job is to determine which technical specifications in ICT should be referenceable in public procurement and policies. Its membership includes representatives from EU member states and European Free Trade Association countries, European and international ICT standardization organizations, and industry and consumer stakeholders.

28 US-China Business Council, "China in International Standards Setting."

29 There is no comprehensive database of MSAs, which are private-sector, ad hoc arrangements. However, this report used media and commercial releases to identify 36 MSAs formed since 2000. Of those, more than half (19) have been formed since 2018.

An Asymmetric Contest: Scale, Centralization, and China's Growing Presence in SSOs and SDOs

Chinese discourse and policy documents prioritize SSOs and SDOs—and representation in them—as key channels through which to influence international standards. For example, the SAC's Main Points of National Standardization Work in 2008 calls for "expand[ing] the number of participating members in ISO technical committees or subcommittees."[30] The State Council's 2015 Development Plan notes that "Chinese experts hold a series of important positions such as ISO Chairman, IEC Vice Chairman, and ITU Secretary General, and the number of Chinese-led international standards is increasing year by year."[31]

China allocates resources accordingly and provides a host of preferential policies to encourage Chinese actors to join, engage in, and contribute recommendations to standard-setting bodies. These include monetary rewards for companies that propose international standards; training for delegates, or "standardization talents"; and financial support to join standardization organizations.[32] As the 2019 China Standardization Development Report explains, "China vigorously encourages enterprises and social organizations to participate in international standardization activities, compiles and publishes Chinese versions of ISO/IEC guidelines for enterprises to participate in these activities…and formulates programs for enterprises and social organizations to participate."[33]

Such state support can make a determinative difference. Participation in SSOs and SDOs tends to be an expensive, laborious, and knowledge-intensive process. Meetings are long and take place all over the world, membership costs can be high, and progress tends to be measured over long-term time horizons.

The following section seeks to assess China's influence in SSOs and SDOs and whether government efforts have paid off. It does so in part by tallying up membership positions and leadership roles.[34] It also explores how China leverages representation in SSOs and SDOs and competitive asymmetries that might result. The findings suggest a rapidly growing Chinese presence in the international ICT-standards ecosystem, especially in areas like telecommunications, where China benefits from outsized industrial capacity. The section also finds that Beijing's centralization may allow it to take advantage of representation in SDOs in a way that other national governments cannot.

Counting Seats

Most work in standards organizations takes place in domain-specific subgroups (i.e., technical committees or working groups). Members propose and vote on recommendations. These subgroups also have management teams (e.g., secretariats, chairs, and vice chairs) that grant influence over standardization agendas. "Chairs have power," explained an ECMA delegate interviewed for this project: "a chair with an agenda can steer conversation." Chairs can also decide where and when

---

30 Standardization Administration of China, 2008年全国标准化工作要点.

31 State Council Information Office (PRC), 国家标准化体系建设发展规划 (2016-2020年).

32 Most SDOs charge annual membership fees. In ITU, these range from just over $4,000 for academic entities to almost $35,000 for corporations.

33 State Council Information Office (PRC), 2019中国标准化发展年度报告 [2019 China Standardization Development Report] (Beijing, February 2019).

34 Most standards organizations do not publish which entity originally recommended or led the development of the standards they approve. However, representation statistics offer a valuable proxy. They have also been a priority of Chinese standards planning for over a decade.

meetings are held. More empirically, ISO data suggests a correlation between working group chairs and the publication of standards suggested by Chinese players: approximately 50% of ISO technical committees with SAC secretariats published standards recommended by China in 2019 or 2020. Overall, only around 25% of ISO technical committees did.[35]

China is rapidly increasing its membership and leadership positions in international standards bodies. The 2019 China Standardization Development Report celebrates that "as of the end of 2019, China has undertaken vice chair positions in 73 ISO and IEC technical institutions, and 88 secretariat positions."[36] Between 2011 and 2020, Chinese-occupied secretariat positions in ISO technical committees and subcommittees increased by 73%. In IEC, they grew by 67% between 2012 and 2020. These figures remained largely stable for other major participants, including the United States and Japan.[37] This growth in Chinese representation correlates with an increase in Chinese-led standards in ISO and IEC: between 2013 and 2020, these increased by 4.1 times to reach 788.[38]

Nonetheless, China's presence is not outsized relative to the size of its market, nor is it the most significant player in ISO or IEC. In ISO, China ranks second in secretariat positions after Germany. In IEC, China lags behind Germany, the United States, France, Japan, the United Kingdom, and Italy in leadership posts in technical committees and subcommittees. And in ISO/IEC JTC 1, China's presence is even less significant. It has 22 subcommittees and 17 working groups, but none of the subcommittees and only 3 working groups (smart cities, quantum computing, and unmanned aircraft systems) have Chinese conveners.

Some U.S. analysts have treated this as evidence that standards bodies are structurally sound and that Beijing—whatever its ambitions—neither does nor will claim disproportionate influence over them. These analysts also cite the fact that Chinese-led international standards still account for only around 2% of the total.[39] Such points are valid. They suggest that at present, Beijing's influence over the international standards ecosystem remains limited. However, this conclusion ignores the rate of growth of China's presence in international standards bodies and what that means for tomorrow's ecosystem. As will be discussed in the next section, this conclusion also ignores both Beijing's asymmetric ability to use its representation and the outsized presence China has secured in other SDOs, especially those related to telecommunications.

China holds significantly more management team positions in ITU-T, the branch of ITU responsible for ICT standards, than any other country, with 34 posts out of a total of 225.[40] South Korea ranks second with under 20. The *Global Times* reported in 2019 that China had proposed more standards at ITU than any other country, accounting for 33% of the total.[41] A similar story

---

35 Most SDOs, including ISO, do not publicly publish the recommending unit for the standards they issue. However, the Chinese government has, for the past few years, published a list of all ISO standards that were recommended by Chinese units. This assessment draws on that list. See, for example, State Administration for Market Regulation (PRC), 关于公开国际标准化组织(ISO)2019年发布的我国牵头制修订的国际标准情况的通知 [Notice on Disclosing the Situation of the International Standards That China Has Taken the Lead in Formulating and Revising Issued by the International Organization for Standardization (ISO) in 2019] (Beijing, March 2020); and State Administration for Market Regulation (PRC), 关于公开国际标准化组织(ISO)2020年发布的我国牵头制修订的国际标准情况的通知 [Notice on Disclosing the Situation of the International Standards That China Has Taken the Lead in Formulating and Revising Issued by the International Organization for Standardization (ISO) in 2020] (Beijing, August 2021).

36 State Council Information Office (PRC), 2019中国标准化发展年度报告.

37 US-China Business Council, "China in International Standards Setting."

38 "唱响国际标准的中国强音!2020国际标准峰会在京举办."

39 See Neaher et al., "Standardizing the Future."

40 Every ITU-T study or focus group, as well as work program, has a chair and at least one vice chair. These chairs and vice chairs are collectively known as "management teams."

41 "国际标准制定,中国加强存在感 以占据竞争优势."

holds in 3GPP. Of the 44 chair or vice chair positions in open specification groups, China holds 15. The United States holds the next most, with 9. China's lead is particularly noticeable in radio access network–focused specification groups. There are 5 such groups, with 15 leadership posts. China holds 7 of those, followed by the United States with 3.

Moreover, China's dominant role in ITU is borne out in specific cases. Take, for example, an October 2021 meeting of ITU-T Study Group 20, dedicated to IoT and smart cities. This meeting addressed 94 total standards contributions, 53 of which were proposed by Chinese actors. South Korea had the next most contributions with 21.[42]

China's lead in telecommunications-relevant standard-setting organizations may in part stem from lower barriers to entry. The membership structure of ITU, which includes private-sector as well as national body members, might make it easier for a coordinated, government-led, enterprise-driven approach to gain traction. China's lead also likely stems from the country's stronghold in the telecommunications value chain. Regardless, the advantage aligns with a Chinese strategic emphasis on telecommunications as the backbone of the digital revolution.[43] In a 2019 article, Sun Lu of the Communication University of China argued that not only are information technology standards the crux of today's industrial revolution but telecommunications standards are the crux of those:

> Technical standards are the "compass" and "beacon" of industry…One of the most important points is interconnection in telecommunications, which both improves the level of interconnection and interoperability of international communications and promotes a new generation of ICT….In the current complex background of the world, the issue of standards in the field of international telecommunications has become one of the focal issues of global governance.[44]

A Coordinated Approach

China's centralization may also allow it to leverage representation in SDOs in a way that other national governments cannot. Standards are defined through coordination among private-sector, academic, nonprofit, and government entities. These players tend to be fragmented, focused on technical merit—or their own self-interest—rather than on nationalism or a country-level strategic agenda.

ITU-T has almost 500 sector, associate, and academic members. Of these, 73 are headquartered in the United States, but that does not mean they coordinate or respond to U.S. national directives. The Bill and Melinda Gates Foundation and Intel Corporation follow their own agendas. Similarly, Bouygues Telecom and Orange are both French companies, but that does not mean that they collude in 3GPP. On the contrary, they might be more likely to compete, rivals as they are in the French market. This is not the case in China. As one ISO delegate put it, "other countries' delegates act like individuals. China's act like a group."

---

[42] Author's interview.

[43] The National Medium and Long-Term Program for Science and Technology Development (2006–2020), which proposed the construction of a standards strategy, launched sixteen key national science and technology projects, including one dedicated to "new generation broadband wireless mobile communication networks." See State Council Information Office (PRC), 国家中长期科学和技术发展规划纲要(2006–2020年) [National Medium and Long-Term Program for Science and Technology Development (2006–2020)] (Beijing, February 2006). SAC's annual planning documents began to emphasize telecommunications standards in 2009. See de La Bruyère, "China's Quest to Shape the World through Standards Setting."

[44] Sun Lu, "'一带一路'与中国国际电信标准化之路" ["One Belt One Road" and China's International Telecommunication Standardization Road], Guangming Net, October 14, 2019.

The CCP is asymmetrically able to shape the incentives of its private-sector and academic players and, by extension, their engagement in international standard setting. This process is direct for state-owned entities: of the fifteen 3GPP chairs and vice chairs in open working groups affiliated with Chinese entities, 60% work for state-owned enterprises.[45] Beijing also has outsized control over the actions of its companies that are not state-owned, as is evident in the state's recent regulatory crackdown on the tech sector.

Moreover, China's domestic standard-setting system is a government-controlled affair. Standards innovation bases offer a useful example of Beijing's process: SAC oversees at least fifteen of these across China. In them, companies engage with a centralized platform to develop and hone their standard recommendations before taking them to international standards bodies.[46] Or, in a more ad hoc example, in 2020 the China Satellite Navigation Office formed a "Chinese expert group"—composed of representatives from the China Academy of Information and Communications Technology, Datang Telecom, Huawei, ZTE, China Mobile, China Unicom, and China Telecom—to "submit four Beidou-3 B1C signal technology proposals" to 3GPP.[47]

This government-guided system grants China an advantage in developing complex technical standards, such as those for smart cities, that require coordination among a diverse range of technologies as well as among public- and private-sector stakeholders. Beijing can ensure that all of these actors work together to formulate and implement a standard, which it can then present as ready-made and tested to international partners whose more fragmented domestic systems preclude such coordination. A standards consultant interviewed for this project suggested that, as a result, Chinese standards in these complex domains will inevitably be adopted as international standards.

China's centralized approach to standards also means that the proposals it brings to SDOs tend to align with the strategic interests of the Chinese government and be backed by the broader ecosystem of Chinese actors. Chuanzhong Du describes bloc voting of Chinese companies in 3GPP. He uses the example of the 2016 meeting in Reno, at which 3GPP delegates chose between polar code, favorable for Huawei, and low-density parity-check code:

> At the Reno Conference…almost all Chinese companies coordinated tacitly to support the polar code led by Huawei as a control channel coding standard…. This shows strong nationalism. While on the surface, the 5G international standard competition is a competition between technical solutions, at a deeper level, it is dominated by nationalism.…This is particularly obvious among Chinese companies.[48]

---

45 Of the fifteen Chinese entities contributing proposals to the October 2021 ITU Study Group 20 meeting, all but one, Tencent, was state-owned.

46 This process is described in "我国在国际标准化组织中影响力不断增强" [China's Influence in the International Organization for Standardization Continues to Increase], Guangming Net, December 13, 2020.

47 "让北斗系统汇款全球移动通信应用" [Let the Beidou System Remit Money to the Global Mobile Communication Application], China Quality News, October 27, 2020. The Chinese Society for Electrical Engineering's International Standards and Technology Research Institute offers another case. The institute is a professional organization dedicated to "international standards policy strategy research… and international standards construction." It is designed "as a bridge between Chinese enterprises and the ISO" to ensure the coordination of China's standards and companies' approaches to them. The institute describes its ultimate purpose as promoting "the 'Go Out' of the whole chain of Chinese standards + Chinese technology + Chinese equipment." See "唱响国际标准的中国强音! 2020国际标准峰会在京举办." Or take, for example, the IMT-2020 5G Promotion Group, jointly launched by China's Ministry of Industry and Information Technology, the National Development and Reform Commission, and the Ministry of Science and Technology in 2013. This group serves as a work platform for Chinese companies, academic entities, and government players to research, coordinate, and promote international standardization in 5G and related technologies. "组织架构" [Organization], IMT-2020 5G Promotion Group.

48 Du Chuanzhong, "全球新一代信息技术标准竞争态势及中国的应对战略" [Global New Generation Information Technology Standards Competitive Situation and China's Response Strategies], *Social Science Frontiers*, July 15, 2019.

More recently, in 2020, Huawei proposed a fixed 5G standard in cooperation with ETSI. In doing so, it benefited from the support of some ETSI members in Switzerland, Altice Portugal, and every Chinese operator. It also benefited from little competition. When Nokia had proposed a different standard at ITU in February 2020, a minority coalition led by Chinese operators and vendors blocked the move.[49]

Nor is it only Chinese players that Beijing can influence. As chapter 4 will illustrate, China's market and investments also grant the CCP leverage over other international players. The SAC's Main Points of National Standardization Work in 2008 notes that China should "strengthen exchanges and cooperation with African countries and strive for support from African countries in international standardization activities."[50]

Bilateral and Multilateral Engagement

Beijing also leverages bilateral and multilateral engagement to influence standard-setting ecosystems. "In 2019," reads the China Standardization Development Report, "China will actively participate in the activities of regional standardization organizations."[51] The report also describes standardization conferences held between China and Germany, the United Kingdom, Japan and South Korea, Canada, and Russia "to connect standardization strategies [and] promote standards cooperation."[52]

This section surveys China's regional and bilateral standards partnerships. It argues that these constitute an avenue for recognition of Chinese standards internationally, which in turn increases their legitimacy, scale, and, by extension, likelihood of formal adoption. More directly, bilateral and multilateral standards partnerships can be used to drum up support in international standards bodies. They can also be used as channels through which to develop joint standards that, by virtue of being multilateral, might be more likely to take hold globally.

Cooperation among standards organizations is not anomalous. This is a normal activity for NSBs rather than a unique tool in China's arsenal. But in China's case, such cooperation is asymmetric. Beijing is actively competing to shape global standards for the sake of national power, channeling its standardization engagement through government entities (e.g., SAC). China's partners, many of which are private or nonprofit entities, are not.

Beijing signed its first bilateral standardization cooperation agreement in 2002. Today, China reports 98 standardization agreements with 55 different countries (see **Figures 1** and **2**).[53] Some of the earliest such agreements involved cooperation with Japan and South Korea, discussed in detail in the case study in the **Appendix** to this chapter. More recently, in 2019 the British Standards Institute (BSI) signed a memorandum of understanding with SAC during a meeting of the UK-China Standardization Cooperation Commission.[54]

---

[49] Chris DePuy and Alan Weckel, "650 Group Interview about 60 Ghz Wireless Market and a Follow-Up about Throughput and Range," 650 Group, January 21, 2021, https://www.650group.com/blog/category/fwa.

[50] Standardization Administration of China, 2008年全国标准化工作要点.

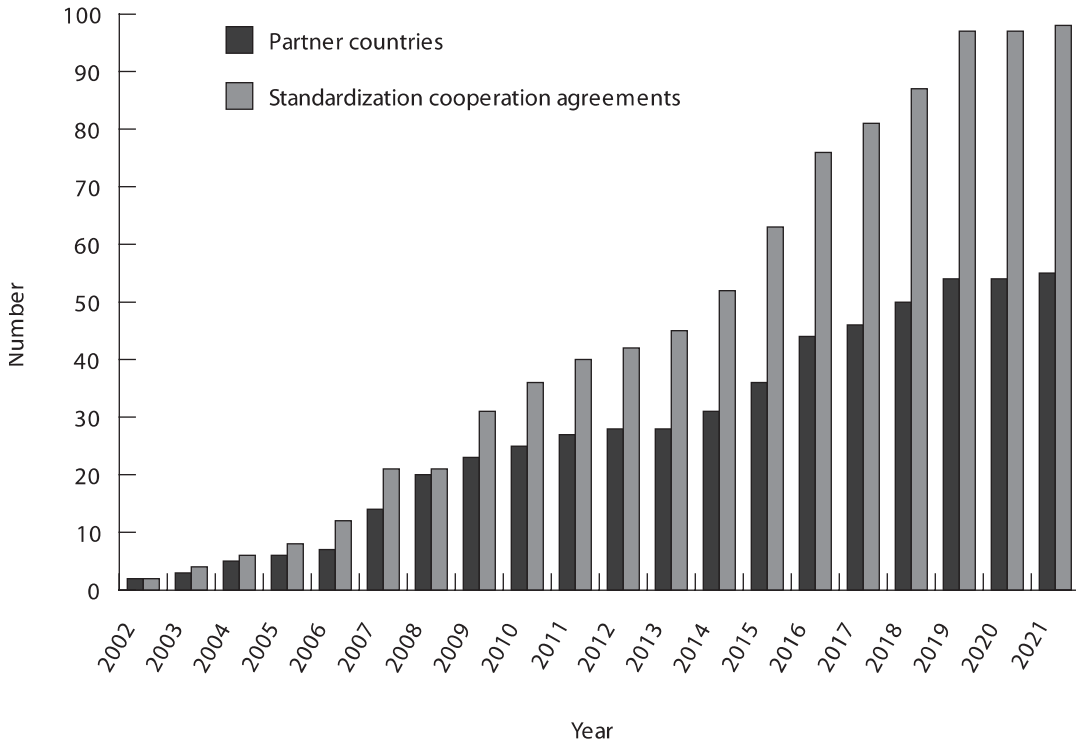
[51] The report points in particular to the Pan American Standards Commission, the European Committee for Standardization/European Committee for Electrotechnical Standardization, the Pacific Area Standards Conference, and the African Organisation for Standardisation. See State Council Information Office (PRC), 2019中国标准化发展年度报告.

[52] Ibid.

[53] Standardization Administration of China, "大道致远，海纳百川—国际标准化合作协议遍地开花" [The Road Stretches Far, and All Rivers Reach to the Sea: International Standardization Cooperation Agreements Are Blooming Everywhere], August 4, 2021.

[54] "BSI Extends Agreement with Standardization Administration of China," BSI Group, June 14, 2019, https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2019/june/bsi-extends-agreement-with-standardization-administration-of-china.

FIGURE 1 China's total standardization cooperation agreements and partners (2002–21)



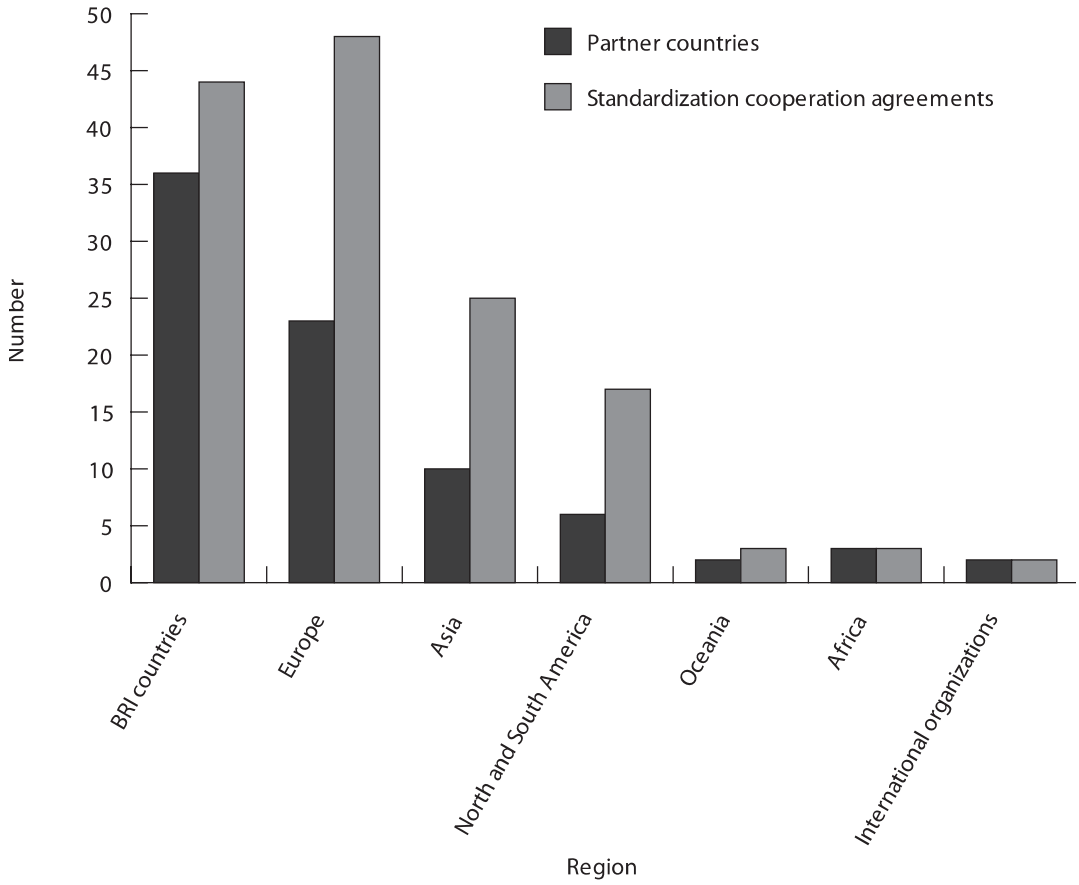
SOURCE: Standardization Administration of China, "大道致远，海纳百川—国际标准化合作协议遍地开花."

China takes different approaches, and focuses on different technologies, with different national and regional partners. Beijing channels much of its standards cooperation with ASEAN countries through the regional organization itself. For example, in 2019, China and ASEAN held an inaugural international standardization forum, the second iteration of which took place in 2021. The two parties also operate a China-ASEAN standards research center and have identified a set of "major projects for China-ASEAN standards cooperation." With ASEAN partners, Beijing tends to focus on standards for smart manufacturing, smart cities, autonomous vehicles, and financial information—as well as on more legacy, non-digital-relevant fields like healthcare, agriculture, and construction.[55]

By contrast, China's engagement with European and North American national standards bodies tends to be more bilateral. This engagement is tailored to the industrial and technological advantages of the partner in question. For example, China's standards engagement with the UK prioritizes smart cities and graphene, while that with Germany emphasizes the auto industry and

[55] Cai Xuping and Lu Yunmiao, "国家东盟标准化研究中心建设现状与展望" [The Current Situation and Prospect of the Construction of the National ASEAN Standardization Research Center], Popular Standardization, 2019; and Ministry of Commerce (PRC), "中国—东盟强化标准 '软联通' 推动RCEP落地落实" [China-ASEAN Strengthens the Standard "Soft Connectivity" to Promote the Implementation of RCEP], September 13, 2021.

FIGURE 2 China's total standardization cooperation agreements and partners (by region)



SOURCE: Standardization Administration of China, "大道致远，海纳百川—国际标准化合作协议遍地开花."

advanced manufacturing.[56] The latter provides an instructive case. Germany is a crucial player in international standards and holds more leadership positions in ISO and IEC than any other country. China has secured a close standards partnership with Germany in precisely the emerging domains where Germany excels and which China prioritizes, including advanced manufacturing.

In 2011, SAC and the German Institute for Standardization (DIN) formed the German-Chinese Standardization Cooperation Commission.[57] The commission meets annually and serves as a platform for dialogue and cooperation on standardization strategies. It focuses on shipbuilding, biotechnology, smart cities, medical technology, automotive steel, and especially electromobility and Industry 4.0, both of which have dedicated sub-working groups.[58] German players have

[56] See, for example, "我国已与21个'一带一路'国家签署标准化合作协议" [China Has Signed Standardization Cooperation Agreements with 21 "Belt and Road" Countries], Legal Daily, May 14, 2017; BSI Extends Agreement with Standardization Administration of China"; and Daniel Fuchs and Sarah Eaton, "Diffusion of Practice: The Curious Case of Sino-German Technical Standardization Partnership," October 2020.

[57] Michael Sutherland, "Setting a New Standard: Implications of China's Emerging Standardization Strategy," *China Studies Review* 5 (2019): 65–78.

[58] "International Cooperation," German Institute for Standardization, https://www.din.de/en/din-and-our-partners/international-cooperations.

attributed the formation of the commission, and especially the Industry 4.0 sub-working group, to Chinese government pressure.[59] The commission's work feeds directly into international standards bodies, including ISO and IEC (e.g., ISO/IEC Joint Working Group 21).[60] In 2019 the partnership added the Strategy Dialogue Group to focus on forming a coordinated front, generating support, and countering resistance in ISO.[61] In August 2020, Tian Shihong, director of SAC, met with DIN's chair of the executive board. They discussed the ISO Strategy 2030, the digitalization of standards, and the governance of ISO/IEC JTC 1.[62]

Germany's influence over international standards is unique, but this type of bilateral cooperation is not. Just days before the meeting with DIN, Tian held bilateral standardization cooperation talks with BSI, in which they discussed the China-UK Standardization Cooperation Commission, progress on the China Standards 2035 plan, cooperation in ISO and IEC, and institutional reform of IEC.[63] Three months later, Tian held a similar meeting with the chair of the American National Standards Institute, and two months after that with the Association Française de Normalisation.[64]

From the Ground Up

As discussed in chapter 1, China's bilateral and multilateral engagement also targets entities other than standards bodies to change facts on the ground. Beijing's size and centralization allow it to leverage trade, investment, and industry partnerships to proliferate de facto standards. When Chinese entities build infrastructure projects internationally, they tend to do so according to Chinese standards. In many cases, requirements mandating Chinese standards are written into contracts.

Chinese policy documents emphasize the value of the Belt and Road Initiative to this end: the Development Program suggests that China "actively promote the docking and cooperation in the field of standards with the co-construction of Belt and Road countries."[65] In 2015, SAC issued the Belt and Road Initiative for Standards Connectivity (2015–17). This was followed by the Action Plan for Standards Connectivity to Build the Belt and Road Initiative (2018–20). The plans explicitly target the "formulation and implementation of Chinese standards" across both traditional industries and infrastructure and emerging ones, including information technology.[66] A prescient 2012 article in the *International Journal of IT Standards and Standardization Research* predicted this approach and its risks:

> Once Chinese infrastructure is laid and Chinese equipment is loaded on it, it is only a matter of time before Chinese standards will be used…Due to its huge

---

59 Fuchs and Eaton, "Diffusion of Practice."

60 "Five Years of Sino-German Cooperation on Standardization in Industry 4.0," GPQI, October 29, 2020, https://www.gpqi.org/news_en-details/five-years-of-sino-german-cooperation-in-industry-4-0.html.

61 Fuchs and Eaton, "Diffusion of Practice."

62 "China Holds High-Level Talks on Standardisation with the United Kingdom and Germany," SESEC, September 17, 2020, https://sesec.eu/Archive/category/others/page/2.

63 Ibid.

64 State Administration for Market Regulation, "田世宏出席中美标准化合作双边视频会议" [Tian Shihong Attended the Bilateral Video Conference on China-U.S. Standardization Cooperation], November 27, 2020; and "中法标准化合作双边视频会议召开 双方将在重点领域国际标准制修订方面相互支持" [Sino-French Standardization Cooperation Bilateral Video Conference Is Held. Both Parties Will Support Each Other in the Formulation and Revision of International Standards in Key Areas], China Business News, December 4, 2020.

65 CCP and the State Council Information Office (PRC), 国家标准化发展纲要.

66 State Council Information Office (PRC), "标准联通共建'一带一路'行动计划(2018-2020年)发布实施" [Action Plan for Standards Connectivity to Build the Belt and Road Initiative (2018–2020)], November 15, 2018.

> domestic market and global influence, we expect that China's standards will become a real threat to the incumbent standards from traditional players like the United States, Japan, and EU.[67]

In addition, as their global reach and clout grows, Chinese companies are increasingly active in more informal, inter-company standard setting, such as MSAs.[68] Partnerships with foreign industry associations offer another avenue for bottom-up influence. These groups are not necessarily themselves standard-setting bodies, but their decisions and initiatives influence best practices across their industries, constituting a de facto rule set that, with enough global buy-in, is likely to ultimately become an international standard. For example, Alibaba, the Chinese Ministry of Transport, and the International Port Community Systems Association—an association of sea and air port authorities, port community system operators for both sea and air, and single-window operators—have jointly launched a task force on logistics visibility.[69] The Ministry of Transport bases its contributions on China's National Transport Logistics Public Information Platform, an information hub controlled by the ministry that collects and integrates multimodal information on trade across China and internationally. The outputs of this task force will become de facto industry standards. They will also likely be adopted by ISO and will become a foundational element of smart supply chains. Chapter 2 described Alibaba's eWTP (electronic World Trade Platform) and, with it, the company's state-backed efforts to define digital trade platforms. Should those efforts be scaled and combined with standard setting in digital logistics, Alibaba could lock in vertically integrated control over information flows for future trade and the physical goods and systems that will depend on them.

Conclusion

The digital revolution has raised the strategic value of standards, and Beijing is competing to set them. It treats technical standards as tools, and sources, of national power, while other countries have historically left the standards contest to commercial players. This strategic approach creates an inherent asymmetry—China competes where other countries are cooperating. Moreover, China's size, centralization, and industrial capacity grant it structural advantages in influencing international standards: Beijing's representation in international organizations is growing at a breakneck pace; its infrastructure construction and platform proliferation, especially in the developing world, may allow it to shape standards from the bottom up. These advantages are such that, especially as technologies and their standards grow more complex, Beijing is likely to claim outsized influence in setting the rules of the digital environment.

No other country, or even group of countries, is likely to rival China on these metrics. A tit-for-tat competition is unlikely to succeed; instead, an effective response to China's standards strategy will demand coordination among private- and public-sector actors across not only

---

[67] The article continues: "Chinese companies supply telecommunications equipment in the early development of every country's market. Then they get subsequent network upgrades as the economy grows. Once the core network is built by made-in China, all upgrade contracts will follow." Heejin Lee and Joon Huh, "Korea's Strategies for ICT Standards Internationalisation: A Comparison with China's," *International Journal of IT Standards and Standardization Research* 19, no. 2 (2012): 1–13.

[68] This report's analysis of MSAs formed since 2000 found that Chinese companies did not figure in them before 2016. But in 2020, Chinese companies accounted for approximately 25% of participants in identified MSAs (30 out of 123).

[69] "Logistics Visibility Task Force," International Port Community Systems Association, https://ipcsa.international/initiatives/logistics-visibility-task-force.

formal standards bodies but also informal commercial and industrial partnerships that shape the standards environment on the ground. Key first steps in developing such a response should include the following.

Greater transparency. SSOs and SDOs should be required to publicly note the formulating and proposing entity for every standard they develop and approve.

Stronger defense. China benefits from the reality that it competes for international standards while other national governments cooperate. The United States and its allies and partners should recognize as much and stop making unforced errors. They should terminate bilateral standards cooperation with the Chinese government and government-controlled entities. They should also bar domestic standards organizations from including as members Chinese entities that have been designated as tied to the Chinese military, engage in human rights abuses, or are under the control of the CCP.

A proactive agenda. The United States and its allies and partners should establish and fund a new organization composed of government and industry representatives that is dedicated to developing and proposing new standards recommendations in strategic areas.

APPENDIX: CASE STUDY OF HOW STANDARDS COOPERATION AMONG CHINA, JAPAN, AND SOUTH KOREA ADVANCES CHINA'S DIGITAL INTERESTS

Beijing's standards strategy does not rely only on Chinese actors. China also pursues bilateral, multilateral, and regional engagement to shape the direction of other countries' standards development, lock in recognition of Chinese standards in foreign markets, and drum up support in international standards bodies. China's long-standing and extensive engagement with Japan and South Korea provides a quintessential example and highlights the influence that such engagement promises over international standards.

Japan and South Korea are established leaders in the international standards environment. Both boast outsized representation in major international standards bodies, including ISO, IEC, and ITU. South Korea has the second most leadership posts in ITU, after China, while Japan has the second most technical committee secretariat positions in IEC, after Germany. This makes the two countries valuable assets in Beijing's bid to influence international standards.

Japan's and South Korea's economic and technological positioning also makes them auspicious targets—despite their historically competitive, and even confrontational, relationships with China. As neighboring countries, they need technical interconnectivity, and interoperability, with China. They depend on China's market, value chains, and emerging digital ecosystems. A 2012 article in the *International Journal of IT Standards and Standardization Research* about China's standards relationship with South Korea explained that "while they compete against each other in the arena of international standardization, they need each other to support the development of each other's standards and to strengthen them in markets, both domestic and international."[70]

Such support is evident in long-standing, extensive standards cooperation among China, Japan, and South Korea. This cooperation takes place at a high level: the three countries hold regular ministerial-level, trilateral meetings dedicated to cooperation in ICT and the international standards therein. At the second such meeting, held in 2003, they signed an "information and communication cooperation arrangement," committing to work together in standardization for third-generation and next-generation mobile communications, next-generation internet technology, and network and information security.[71] At the 2011 meeting, China's Ministry of Industry and Information Technology (MIIT) proposed coordination in IPv6 standardization; at the 2018 event, the three sides agreed to coordinate in developing 5G systems.

Cooperation among the three countries also takes place at a more granular level. Since 2002, they have operated a series of dedicated trilateral standardization cooperation mechanisms designed to implement their national commitments to standardization cooperation and, more broadly, foster a unified front and greater influence in international standards bodies. These mechanisms include the Northeast Asia Standards Cooperation Forum (NEAS Forum) and the China-Japan-Korea IT Standards Meeting (CJK-ITSM), as well as more targeted mechanisms like the Northeast Asia Open Source Software Promotion Forum (OSS Forum).

---

[70] Heejin Lee and Joon Huh, "Korea's Strategies for ICT Standards Internationalisation: A Comparison with China's," *International Journal of IT Standards and Standardization Research* 19, no. 2 (2012): 1–13.

[71] "中日韩签署有关文件将加强信息通信领域合作" [China, Japan, and South Korea Signed Relevant Documents to Strengthen Cooperation in the Field of Information and Communication], Xinhua, September 9, 2003.

NEAS Forum

At the 2010 trilateral summit, the three countries' leaders signed a joint statement reaffirming their dedication to standards cooperation. That statement pointed in particular to the NEAS Forum as a primary mechanism for promoting the "coordination of international standardization,"[72] which had been formally launched in 2002 by their standardization bodies—the Japanese Industrial Standards Committee, the Korean Agency for Technology and Standards, and the Standardization Administration of China. In a 2012 interview, the SAC official in charge of international activity, Shi Baoqun, described the NEAS Forum as "an important bridge linking the standardization work of China, Japan, and South Korea."[73] He also explained that the forum had been launched in large part to "strengthen [CJK] communication and coordination in international and regional standardization activities." The NEAS Forum is, as China's Ministry of Foreign Affairs puts it, "government-led, with public participation."[74]

A set of working groups—32 at present, though the number changes every year—undertakes the NEAS Forum's technical activities, every one of them with a dedicated country lead or set of country leads. Some of these working groups explicitly target a defined ISO or IEC technical committee, such as the ISO/TC 20/SC 16 UAS testing working-group preparation plan, led by China. Others are broader, such as the "international standardization in the Internet of Things (IoT)" cooperative project, also led by China.[75] Further, as of 2019, the NEAS Forum has effectively absorbed CJK-SITE, a mechanism established in 2007 to cooperate on international standards in IT and electronics. CJK-SITE focuses on the standardization activities of ISO/IEC JTC 1, as well as other IEC technical committees covering information technologies and electronics.

The NEAS Forum holds an annual meeting at which delegations from the three countries—composed of public- and private-sector representatives and led by their respective standardization bodies—determine the work agenda for the year ahead. Attendees propose and vote on new working groups and on disbanding existing ones. Since 2008, the annual meeting has served as an arena for bilateral exchange as well: every pairing of countries holds bilateral cooperation mechanisms concurrently with the NEAS Forum. In 2021, these focused on standards for automatic identification and data collection as well as logistics and advanced manufacturing. "China, Japan, and South Korea will strengthen cooperation in international standardization of digital transformation," reported Chinese media coverage of that year's event.[76]

Over the past nineteen years, China's role in the NEAS Forum has increased significantly. In 2010, China led only 2 of the 12 cooperative items with single-country leads, compared to 6 for Japan and 4 for South Korea. In 2021, China led 7 out of 28. While it might still lag behind the other two on that metric, China consistently recommends more new working groups than either country—of the 15 new items proposed at the 2021 conference, China suggested 12. In 2010, those

---

72 "Japan-China-ROK Trilateral Summit Joint Statement on Standards Cooperation among the Republic of Korea, Japan and the People's Republic of China," Ministry of Foreign Affairs (Japan), May 30, 2010, https://www.mofa.go.jp/region/asia-paci/jck/summit1005/joint_standards.html.

73 Liu Zhiyang, "进一步推动中日韩标准化领域合作: 访国家标准化管理委员会副主任石保权" [Further Promote the Cooperation in the Field of Standardization between China, Japan and South Korea: Interview with Shi Baoquan, Deputy Director of the National Standardization Management Committee], China Standardization, 2012.

74 "Full Text: China-Japan-ROK Cooperation (1999–2012)," Ministry of Foreign Affairs (PRC), May 10, 2012, http://www.china.org.cn/world/2012-05/10/content_25347883_4.htm.

75 "The 19th Northeast Asia Standards Cooperation Forum," Japanese Standards Association, July 1, 2021.

76 "中日韩三国将在数字转换国际标准化方面加强合作" [China, Japan and South Korea Will Strengthen Cooperation in International Standardization of Digital Transformation], Go Out Network, June 23, 2021.

figures were 12 and 5, respectively.[77] This high number of proposals may stem from active SAC encouragement and coordination. Before every annual meeting, SAC issues a "notice on soliciting cooperation projects." "All units are requested to actively organize and put forward proposals for cooperation projects," reads the 2021 notice. The notice requests that all projects align with China's national technological and standardization priorities as well as with proposals to ISO/IEC that it "hope[s] will be supported by Japan and South Korea."[78]

As this guidance suggests, the NEAS Forum and its projects are designed to influence international standards and standards organizations, especially ISO and IEC. That much is clear in the projects themselves—in many cases they cite specific ISO or IEC technical committees to target—as well as from the fact that representatives from ISO and IEC regularly attend. Descriptions of the forum indicate that it serves as a mechanism through which China, Japan, and South Korea can bolster each other's broader postures at ISO and IEC. Liu Zhiyang of the China National Institute of Standardization explained in a 2012 article that the NEAS Forum allows the three countries to develop and apply "close cooperation in assuming leadership (e.g., chairman or secretariat) roles in ISO and IEC technical committees and subcommittees, in running for leadership positions at all levels of ISO and IEC, and submitting international standards proposals."[79] Press coverage of the 19th NEAS Forum, held in 2020, noted that the three countries had committed to exploring "solutions to support each other in ISO activities," as well as the stationing of ISO and IEC management personnel. The SAC describes the purpose of the conference as "promot[ing] more standards projects in China to the international stage."[80]

The SAC has described success in doing so. In February 2020 the administration reported that the NEAS mechanism had "promoted the establishment of five ISO technical committees or subcommittees and the issuance of 22 international standards…Among those, China led the establishment of one technical committee and three standards proposals."[81]

CJK-ITSM

In 2002, the China Communication Standards Association, Japan's Telecommunication Technology Committee, Japan's Association of Radio Industries and Businesses, and South Korea's Telecommunications Technology Association signed a memorandum of understanding to establish the CJK-ITSM.[82] The CJK-ITSM has a plenary as well as five working groups: Network and Service Architecture, International Mobile Telecommunications (IMT), Information Security (IS), Wireless Power Transmission, and TACT. Until 2018, the CJK-ITSM met annually, but the plenary appears not to have convened since then. Meetings are attended by representatives of the countries' standards organizations, private-sector entities, and often ITU representatives. The Chinese delegation typically includes CCSA and MIIT leadership, as well as executives from

---

77 "Resolutions of the 9th Northeast Asia Standards Cooperation Forum," Japanese Standards Association, 2010; and "The 19th Northeast Asia Standards Cooperation Forum."

78 "关于征集'第十九届东北亚标准合作会议'合作项目的通知" [Notice on Soliciting Cooperation Projects of the "Nineteenth Northeast Asia Standards Cooperation Conference"], China Standardization, April 13, 2021.

79 Liu, "进一步推动中日韩标准化领域合作: 访国家标准化管理委员会副主任石保权."

80 "中日韩三国将在数字转换国际标准化方面加强合作."

81 "东北亚标准合作会议基本情况" [Basic Situation of the Northeast Asia Standards Cooperation Conference], China Bidder Association, February 22, 2020.

82 China-Japan-Korea IT Standards Meeting (CJK-ITSM), "Memorandum of Understanding (Draft Proposal)," June 26, 2002.

China's key telecommunications companies (e.g., China Telecom, China Mobile, China Unicom, Huawei, ZTE, and Datang Mobile).

Like the NEAS Forum, the CJK-ITSM explicitly targets international standardization activities by "facilitat[ing] cooperation among firms and among governments of the three countries and contribut[ing] to the work of standards organizations of regional and global levels."[83] However, where the NEAS Forum targets ISO and IEC standards, the CJK-ITSM is more focused on ITU. As the TTC's current description of the mechanism puts it, "the CJK IT Standards Meeting brings together standards organizations from Japan, China, and South Korea to exchange information and opinions on standardization activities at the ITU."[84] Concrete examples abound. At the 2018 plenary, the IMT working group reported having led five submissions to ITU-R; the IS working group discussed how ITU-T Study Group 17, which focuses on security and is currently chaired by a South Korean representative, should be organized.[85]

In 2011 the CJK-ITSM signed a memorandum of understanding with ITU. In it, CCSA, TTC, ARIB, and TTA recognized ITU as "the pre-eminent global ICT standards body," while ITU granted them "better access to international standards-making activities."[86] The next year, an ITU Secretariat representative attended the CJK-ITSM plenary. He suggested ways in which the ITU Secretariat might contribute to the effectiveness of CJK in ITU, including supporting the formulation of coordinated CJK positions for ITU meetings and assistance in input documents.[87]

OSS Forum

China, Japan, and South Korea also operate more targeted standards-relevant cooperation mechanisms. Take, for example, the OSS Forum, launched in 2004 by China's MIIT; Japan's Ministry of Economy, Trade and Industry; and South Korea's Ministry of Science and ICT. Partially funded by all three governments and organized by the countries' respective OSS Promotion Alliances, the mechanism is dedicated to "promot[ing] the development of the open source software industry in the three countries and enhancing the status and influence of Northeast Asia in the international open source community and industry."[88] It has four working groups, all composed of company and government representatives from the countries: technology development and assessment, talents education and incentives, study of standardization and certification, and promotion of technological applications. The latter focuses on applications ranging from mobile internet technology to cloud computing and IoT to smart cities.[89]

Like the NEAS Forum and the CJK-ITSM, the OSS Forum engages with international standards bodies, including ISO/IEC JTC 1 and the Free Standards Group. According to the China OSS Alliance chairman, Lu Shouqun, it rests on the consensus that "China, Japan and South Korea

---

83 CJK-ITSM, "Memorandum of Understanding (Draft Proposal)," June 26, 2002.

84 "CJK IT Standards Meeting," Telecommunication Technology Committee, https://www.ttc.or.jp/activities/gcag/cjk.

85 Hideyuki Itawa, "Report on 16th CJK (China, Japan, and Korea) IT Standards Plenary Meeting," *NTT Technical Review* 16, no. 2 (2018), https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201802gls.html.

86 "ITU Teams Up with Leading Asian Standards Organizations," ITU, Press Release, July 6, 2011, https://www.itu.int/net/pressoffice/press_releases/2011/22.aspx.

87 ITU, "The Eleventh CJK (China, Japan, Korea) IT Standards Meeting (CJK-11)," March 14, 2012, https://www.itu.int/en/ITU-T/tsbdir/sap2012/Pages/cjk-11.aspx.

88 "Apache Kylin 亮相东北亚开源软件推进论坛" [Apache Kylin Appeared at the Northeast Asia Open Source Software Promotion Forum], Sohu News, November 16, 2018.

89 Liu Jinfa, "'第十三届东北亚开源软件推进论坛'在武汉召开" ["The 13th Northeast Asia Open Source Software Promotion Forum" Was Held in Wuhan], China Electronic News, November 23, 2014.

should contribute to the formulation of Linux international standards (or the formation of de facto standards)."[90] Since its earliest days, the OSS Forum has focused on cooperation in developing Linux standards. This and the forum's larger open-source mission are framed in opposition to Microsoft—and as part of the Chinese government's effort to unseat that legacy company's market, standards, and dominance. "We are not developing Linux to counter or replace Windows," said Lu in a speech at the opening ceremony of the 3rd OSS Forum meeting, "but we do not approve of Microsoft's monopoly operation."[91] In 2005, two years after that speech, Japanese, Chinese, and South Korean companies jointly unveiled new software based on the Linux operating system, Asianux 2.0, developed by South Korea's Haansoft Inc., Japan's Miracle Linux Corp., and China's state-owned Red Flag Software Co.

In recent years, China's efforts to develop and popularize open-source software have begun to figure in the international policy community's conversations about the country's digital ambitions. But the significance of CJK open-source software—and its potential to transform economic, technological, and geopolitical power dynamics—was clear over a decade ago. "If the cooperation turns out to be successful," wrote Bongsung Chae and Roger McHaney in 2006, "the impact on the world IT industry may be enormous." They suggested that technologically CJK cooperation in OSS could accelerate the momentum for Linux as well as Linux-based embedded applications across consumer electronics, industrial equipment, and emerging ICT systems.[92] Economically, a unified Chinese, Japanese, and South Korean front in favor of Linux would present a steep challenge for Microsoft, as "CJK's global ambition for the world's open source software market may threaten U.S. technological leadership and could damage U.S.-based companies."[93]

Standards have not historically been considered sites for nation-state competition. Beijing is changing this, and its approach to competing for international standards should also change the way that influence over them is measured. Standards are the rule set for a globalized world. In that globalized world, countries and their influence over international standards should not be measured in isolation. The global system must also assess how much leverage one country has over other countries' standards ecosystems—and how independent those ecosystems are, or can be, from that country's digital strategy.

---

90 "陆首群:标准化是中日韩三国Linux发展关键" [Lu Shouqun: Standardization Is the Key to Linux Development in China, Japan, and South Korea], Sina, January 5, 2005.

91 Yang Guoqiang, "中日韩加快Linux方面合作 欲制定统一标准" [China, Japan, and South Korea Speed Up Cooperation on Linux to Develop Unified Standards], Sina, December 22, 2004.

92 Bongsug Chae and Roger McHaney, "Asian Trio's Adoption of Linux-Based Open Source Development," *Communications of the ACM* 49, no. 9 (2006): 95–99.

93 Ibid.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 4

Writing the Rules: Redefining Norms of Global Digital Governance

Nigel Cory

NIGEL CORY is an Associate Director at the Information Technology and Innovation Foundation, where he focuses on cross-border data flows, data governance, intellectual property, and how they each relate to digital trade and the broader digital economy. He previously worked for eight years in Australia's Department of Foreign Affairs and Trade. He can be reached at <ncory@itif.org>.

EXECUTIVE SUMMARY

This chapter examines China's increasingly assertive efforts to influence international data governance, especially cross-border data flows, and promote its concept of "cyber sovereignty," while also analyzing its restrictive approach to domestic data governance as the basis for its international advocacy efforts.

MAIN ARGUMENT

In recent years, China has clearly and forcibly advocated in the international sphere for "cyber sovereignty" and a state-centric approach to international data governance, including through proposals such as its Global Initiative on Data Security. The principles of state and cyber sovereignty emphasize that governments can essentially take whatever actions they deem necessary with respect to data, including leveraging it for economic development and national security. Beijing's strategy for influencing international data governance includes an expansive digital agenda at the United Nations, selective attempts to influence data discussions at the G-20, and government and private-sector engagement in standard-setting organizations and other countries' domestic digital governance policies. China's approach to digital trade provisions and agreements in the Asia-Pacific and at the World Trade Organization is also evolving. Its success will depend in no small part on how well the United States and other liberal democracies respond to these efforts.

POLICY IMPLICATIONS

- Data governance, especially the restriction and control of data flows, is central to China's international advocacy for a state-controlled internet. The U.S. and other liberal democracies need to develop a detailed, whole-of-government global digital strategy to counter China's efforts.
- The contest over the flow of data is critical for shaping the future of the internet. The outcome will impact success in today's data-driven economy, which increasingly depends on how effectively firms can leverage data to generate insights and unlock value.
- There are few international binding rules and agreements governing how organizations collect, use, protect, store, and share data, or regarding what happens when data is transferred across borders. This is also true for related issues like cybersecurity, cybercrime, and digital development. This provides China room to expand its leadership in global digital governance if the U.S. and others do not develop better, alternative approaches to addressing these issues.

China's efforts to play a larger role in global data governance are nascent and evolving, but increasingly well-articulated and prosecuted. Until recently, China was inwardly focused on domestic internet governance and efforts to assert state control over its rapidly growing digital economy. But in recent years, Beijing has clearly and forcibly advocated for "cyber sovereignty" and a state-centric approach to international data governance, such as via its Global Initiative on Data Security (GIDS). The general lack of binding international rules and agreements around data provides China with an opportunity to play a leading role in how these rules and norms evolve, especially with new negotiations and governance initiatives at the United Nations, World Trade Organization (WTO), and elsewhere. China's success will depend in no small part on how well the United States and other liberal democracies respond to its efforts to create an international framework that allows broad state control over data and the internet.

China's international data strategy is based on the principle of state and cyber sovereignty, where governments can essentially take whatever actions they deem necessary with respect to data. China clearly recognizes data's critical role in economic development and national security. For example, it has designated data as the fifth factor of production—after land, labor, capital, and technology.[1] However, China differs from other major countries in its emphasis on political control over data. China's recent crackdown on its own tech industry provides clear evidence that it wants to support data-driven innovation, but that nothing should threaten political stability or the grip on power by the Chinese Communist Party (CCP).[2] In 2015, President Xi Jinping delivered a seminal speech at China's World Internet Conference clearly articulating that Beijing's approach to international data governance would align with its restrictive approach at home. He declared that "China will vigorously implement a strategy to make China a cyber great power," including through construction of a "community of common destiny in cyberspace," global internet infrastructure, and appropriate internet governance norms.[3]

This prioritization of data control manifests in an emphasis on forcing firms to only store data locally within a country's borders (a concept known as data localization). China does this at home and, increasingly, in international digital governance. China is a world leader in using data localization, enacting dozens of laws and regulations making data transfers illegal or prohibitively complicated and costly.[4] China's efforts to set up stringent oversight mechanisms to review requests by firms to transfer data reinforce its preference for local data storage. Arbitrary enforcement and uncertainty about how these laws work make firms risk averse, leading them to store data locally even if the data could potentially be transferred (i.e., de facto data localization).

China is also working to normalize data localization in the global digital economy, as data naturally flows across borders absent artificial barriers and controls. Whether it is successful has enormous economic, social, and political implications. This battle over the flow of data is critical for shaping the future of the internet and dictating the terms of success in today's data-driven economy, which increasingly depends on how effectively firms can leverage data to generate

---

[1] Ouyang Shijia and Chen Jia, "New Guideline to Better Allocate Production Factors," *China Daily*, April 10, 2020, https://www.chinadaily.com.cn/a/202004 /10/WS5e903fd7a3105d50a3d15620.html.

[2] "Xi Jinping's Assault on Tech Will Change China's Trajectory," *Economist*, August 14, 2021, https://www.economist.com/leaders/2021/08/14/xi-jinpings-assault-on-tech-will-change-chinas-trajectory.

[3] Xi Jinping (speech at the opening ceremony of the World Internet Conference, Wuzhen, December 16, 2015), available at https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony.

[4] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," Information Technology and Innovation Foundation (ITIF), July 19, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

insights and unlock value. China uses strict control over data to manage online discourse, with obvious implications for human rights like freedom of speech and association, as well as the spread of misinformation globally. Economically, for firms to maximize value from both data-driven innovation and digital trade, they need to be able to transfer data freely across borders. Yet China uses data localization and other restrictive policies as part of an evolving toolbox of digital protectionism. Many of the world's leading technology firms, such as Amazon, Dropbox, Facebook, Google, and Twitter, as well as a range of news services and search engines, are already banned or blocked in China.[5] As is discussed in chapter 2, Beijing uses these restrictions to protect Chinese tech firms from foreign competitors that would otherwise use data transfers to bring their global information technology and data analytics systems to bear in the Chinese market.

Given that the concept is still developing, coming late to the issue of global data governance has not disadvantaged China. However, its growing advocacy on data governance is not happening in a void. Australia, European Union countries, Japan, Singapore, the United States, and others are advocating for their preferred approaches to data privacy, cybersecurity, digital trade, and other data-related issues. This debate is increasingly fierce and contested. While there are well-established rules about how the internet functions at the technical level, at the policy and application level there is a clear vacuum. There are few international norms, binding rules, or agreements governing how organizations collect, use, protect, store, and share data, or regarding what happens when data is transferred across borders (if it is allowed to be transferred at all). There is no single international forum that manages global data governance. Instead, the data is governed by a disparate group of multistakeholder forums, domestic laws, and a few international agreements and sets of principles.[6] This lack of rules and the fragmented governance have provided China an opportunity to advocate for a restrictive approach based on state sovereignty.

This chapter analyzes how China's restrictive approach to domestic data governance defines its international advocacy efforts and considers how these efforts are playing out in multilateral organizations and forums. It highlights cases of direct engagement and advocacy by both China's government and firms, followed by an analysis of Beijing's approach to negotiating data-related provisions in trade agreements. The chapter concludes with recommendations for the United States and like-minded countries that support an open, rules-based, and competitive digital economy and internet to counter efforts by China to expand data localization and other restrictive policies.

China's Restrictive Domestic Data Governance Framework Defines Its International Agenda

China's sovereignty and control-focused approach to international data governance is based on its restrictive domestic data governance framework, which has been refined and strengthened since the Great Firewall of China was launched over two decades ago. More recently, a deluge of new laws, regulations, and investigations dealing with data privacy, data protection, cybersecurity, artificial intelligence (AI), competition, national security, and other issues have emerged. The Cybersecurity Law, Personal Information Protection Law, and Data Security Law provide the legal

[5] Nigel Cory, "Censorship as a Non-Tariff Barrier to Trade," testimony before the U.S. Senate Subcommittee on Trade, Washington, D.C., June 30, 2020, available at https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff.

[6] These include the Organisation for Economic Co-operation and Development's privacy principles, the Asia-Pacific Economic Cooperation's Cross-Border Privacy Regime, the Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("Convention 108"), and various WTO agreements.

foundation for data governance in China, all of which allow broad state discretion.[7] These laws regulate consumer and commercial uses of data but do not create meaningful constraints on the state in relation to access, use, or enforcement practices. A defining characteristic of Chinese laws and regulations is that they provide legal space for the state to intervene.

The location of data storage is central to China's concept of cyber sovereignty. For example, data localization facilitates surveillance and control over digital content and online discourse. China treats local data storage as the norm and the free flow of data as the exception, asserting that data privacy and cybersecurity are associated with location, which contrasts with most other countries that contend that responsibility for privacy, cybersecurity, or other issues should flow with data wherever it is stored. Data localization is both explicit (codified in Chinese laws and regulations) and de facto. The regulations to transfer data are so complicated, onerous, and uncertain that firms have no realistic choice but to store data locally so as to avoid fines and other penalties.

China has expanded local data storage and control to a growing range of specific data types and services relating to health, genomics, banking, insurance, payments, mapping and location services, and scientific data domains.[8] There are also local data storage requirements for broad categories of data deemed important or strategic that cover a range of largely commercial services. For example, the legal fiction of "important data" is a broad category in the hierarchical data classification framework in the Cybersecurity Law. In many ways, this is a nationalization policy that gives the government arbitrary authority to deem any data as important for national or state interests and exert provenance over it. China does not want to separate its definitions and treatments of commercial and strategic data largely because its broad definition of national security is such that most data is dual-use or, put otherwise, falls into both categories.

China uses data localization and asymmetric internet access (e.g., the Great Firewall) to keep foreign firms, digital goods, and services out, while allowing its own firms to expand overseas. This strengthens Chinese firms while also enhancing China's political control over its internet. In trade negotiations, this position is disingenuous in that China essentially wants to maintain strict political control and protectionism at home while securing unconstrained market and internet access for its firms and their digital goods and services abroad. Yet China criticizes other countries targeting Tencent, Alibaba, or other leading Chinese tech firms. And while its domestic economic interests—characterized by the rise of these and other innovative tech firms—increasingly align with the need to create a framework that allows greater global data flows and digital economic competition and trade, they still do not outweigh the domestic political imperative for strict control.[9]

More recently, China has explicitly turned its digital governance efforts outward to shape the global regime. Its global data advocacy took an evolutionary step forward with the 2020 launch of GIDS.[10] GIDS was clearly designed in response to the Trump administration's Clean Path and Clean Network initiatives, which targeted Chinese firms and their involvement in many digital

---

[7] Aynne Kokas, "China's 2021 Data Security Law: Grand Data Strategy with Looming Implementation Challenges," China Leadership Monitor, December 1, 2021, https://www.prcleader.org/kokas; and Rogier Creemers and Graham Webster, "Translation: Personal Information Protection Law of the People's Republic of China—Effective Nov. 1, 2021," DigiChina, August 20, 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021.

[8] Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally."

[9] The Chinese government, as well as the private sector, is not a monolith, and there is an ongoing internal debate about China's restrictive approach to data flows. See, for example, Wenjie Yang, "Re-examine the Rationality of Requesting Data Localization on the Grounds of National Security," Internet Law Research Center, Institute of Information and Communication Technology, November 11, 2021, https://www.secrss.com/articles/35978.

[10] Ministry of Foreign Affairs of the People's Republic of China (PRC), "Global Initiative on Data Security," September 8, 2020, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html.

and telecommunications services.[11] China characterizes GIDS as an initiative to safeguard global data and supply chain security, promote development of the digital economy, and provide a basis for international rulemaking for data.[12] But in reality, the initiative embodies China's conceptualization of data, cybersecurity, and sovereignty. GIDS uses language and tools from Beijing's existing policies: strong localization requirements and the right for jurisdictions to govern data and the digital economy as they wish based on "mutual respect."[13] In a 2020 speech on GIDS, Chinese foreign minister Wang Yi explicitly advocated (without a hint of irony) against digital protectionism and data localization while also championing the centrality of sovereignty and the state's ability to manage the internet and protect data without restrictions.[14] This highlights China's efforts to shape the narrative around data governance and security to achieve multiple competing outcomes regarding digital trade, data-driven innovation, data flows, and a state-centered and -controlled internet. These goals, however, are contradictory. China seeks to restrict and control foreign companies operating within its borders, while ensuring that Chinese companies expanding abroad do not face equivalent restriction or overseas control. This asymmetric approach to data governance unfairly advantages Chinese companies while hindering their competitors.

How China Advances Its Agenda through International Data Governance Norms, Principles, and Agreements

Beijing's strategy for influencing international data governance is multifaceted and evolving. China provides visiting delegations a Chinese model of internet and data governance and positions its core laws and regulations as alternatives to European and U.S. efforts to regulate the protection, collection, storage, transfer, and analysis of data. But its efforts to influence international data governance extend more broadly. These involve bilateral infrastructure and commercial projects, regional and multilateral organizations, private-sector firms, and domestic agencies. For example, the Cyberspace Administration of China has made influence over global internet governance a key goal in developing China's status as a cyber great power.[15] This section examines specific cases at the United Nations, the G-20, and the International Telecommunications Union (ITU) to demonstrate how China uses not only government-to-government engagement and trade negotiations to pursue its data governance objectives but also private tech firms.

Expand and "Flood the Zone": China's Push for Cyber Sovereignty and an Expansive Digital Agenda at the United Nations

China, along with Russia, has dedicated growing diplomatic attention and resources to the United Nations because of the organization's central role in cyber and internet governance,

---

11 U.S. Department of State, "The Clean Network," https://2017-2021.state.gov/the-clean-network/index.html.

12 Comments by foreign ministry spokesperson Zhao Lijian at a press conference on September 8, 2020.

13 "China's Global Initiative on Data Security Has a Message for Europe," Mercator Institute for China Studies (MERICS), September 24, 2020, https://merics.org/en/analysis/chinas-global-initiative-data-security-has-message-europe; and Daniel Castro and Nigel Cory, "'Clean Network' Initiative Risks Undermining U.S. Digital Trade," ITIF, August 31, 2020, https://itif.org/publications/2020/08/31/clean-network-initiative-risks-undermining-us-digital-trade.

14 Graham Webster and Paul Triolo, "Translation: China Proposes 'Global Data Security Initiative,'" New America, September 7, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-proposes-global-data-security-initiative.

15 "深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作" [In-Depth Implementation of General Secretary Xi Jinping's Strategic Thinking on Strengthening the Country through the Internet, and Solid Progress in Network Security and Information], *Qiushi*, September 15, 2017, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.

especially negotiations to frame a new and potentially expansive cybercrime treaty. In particular, China seeks strong, explicit references to state sovereignty in cyber governance and is increasingly using GIDS to advocate for this and its broader vision for data and internet governance.

China favors multilateral institutions like the United Nations (and the ITU, as is discussed in chapter 3 and in more detail below) because they provide governments with voting power, allowing a focus on state sovereignty. Government-based institutions also make it easier for China to marginalize public- and private-sector advocacy groups that oppose its policies and often prefer the alternative multistakeholder model of internet governance. The large membership in these organizations allows China to use its full toolbox of incentives to get other countries to support its proposals and positions. The United Nations and ITU also favor scale. China can, as one government official put it, "flood the zone" by ensuring that it has as many participants and proposals in as many forums as possible.[16] Beijing often, but not always, sides with Moscow, which supports a state-controlled internet and has long used the United Nations to advocate for its preferred approach to cyber governance. There is, however, a difference between the two: while China floods the zone, Russia is savvier at developing and building support for its proposals. Though Beijing does not generally like being isolated on an issue (especially without Moscow), it is getting more comfortable spearheading arguments on cyber issues.

China wants to use cyber discussions at the United Nations to push a comprehensive agenda—or, as one official described it, "issue creep"—on cybercrime and cybersecurity to cover broader data and internet governance issues, even though these issues are not within the usual scope of the United Nations. Russia and China were instrumental in creating a new UN working group—the Open Ended Working Group (OEWG) on Information and Communication Technologies—that was more amenable to their interests and approach, as opposed to the smaller Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Indicative of its use of GIDS, OEWG proposals and discussions have often used similar terminology and concepts. In June 2021, China's UN ambassador Zhang Jun made the connection clear in referencing both the OEWG and GIDS and their core concepts in a speech at the UN Security Council.[17]

Furthermore, in 2021, China developed its first draft resolution on cyber issues for the UN Disarmament and International Security Committee (DISEC). China and Russia prefer to use this committee because its outcomes tend to be based on explicit references to nonintervention, central to cyber sovereignty. Initially, China circulated a proposal on the peaceful use of technology, which, despite its name, was actually directed at export-control restrictions imposed by the United States and other countries that target China and its firms.[18] Subsequently, it shared a draft DISEC resolution on GIDS in its first effort to embed GIDS and its concepts into the committee.

At first, the United States and like-minded countries did not fully appreciate what GIDS represented in Chinese cyber statecraft and were unprepared when China started pushing for this initiative and related concepts everywhere it could at the United Nations.[19] It took time for these countries, and the various agencies involved, to fully understand GIDS and its potential impact on

---

[16] Interview by the author.

[17] "张军：共同保障网络安全,携手维护国际和平" [Zhang Jun: Jointly Safeguard Network Security, Work Together to Maintain International Peace], Permanent Mission of the PRC to the UN, June 29, 2021, http://chnun.chinamission.org.cn/chn/hyyfy/202106/t20210629_9120677.htm.

[18] Interview by the author.

[19] Interview by the author.

the global internet. This should be a wakeup call. As is discussed in chapter 6, the United States and other liberal democracies will need to develop new mechanisms for coordinating a multilateral response to China's efforts in the United Nations.

"Death by a Thousand Cuts": How China Seeks to Expand Its Agenda

As with its standard-setting strategy discussed in the previous chapter, China's data governance strategy prioritizes the ITU because it is a government-based organization that also allows select private-sector participation and lends itself to broad, coordinated, and persistent engagement. The ITU is a little-known multilateral organization responsible for issues like setting certain technical standards. In contrast to the United Nations, the ITU has a designated role for private firms, whose involvement China coordinates as part of its strategy. In this way, the ITU scales even more readily than the United Nations since private firms—as "sector members"—have a seat at the table. In recent years, many Chinese companies have become sector members in ITU committees and study groups for technical standards, especially as they relate to smart cities and surveillance-related technologies.[20] As one official described, this public-private "death by a thousand cuts" is a coordinated strategy by China to get its preferred language embedded in agendas, discussions, and documents. Even if a major proposal is defeated, China can break it into many pieces and convince representatives to embed them in other committees and forums.

Similar to its support for an expansive agenda at the United Nations, China wants to expand the scope of the ITU to include digital trade and the broader digital economy even though the union's jurisdiction does not include internet architecture. As part of this effort, China is becoming more adept at building support for its proposals, including by using incentives to persuade other countries to front and support them. For example, Beijing wanted to push for broad digital economic discussions at the ITU but knew that with its chief role the initiative would likely fail. It wanted Asian and Australasian countries to jointly present the initiative but could not get consensus. So China convinced Malaysia to lead the effort. Similarly, in 2019, Huawei officials proposed a new top-down, centralized design for internet governance called "New IP (Internet Protocol)."[21] Thus, China used government and private-sector information and communications technology (ICT) projects to build support among African countries for New IP. Given the criticism and opposition to the proposal, China broke it into pieces to advocate in various ITU committees and study groups, making it harder for opposed countries to track and respond to each separate element. These individual elements also appear less concerning, even though when combined they collectively serve China's overarching goal.

Both of these are examples of China's approach of taking issues that are normally discussed at the WTO and technical, multistakeholder forums like the Internet Engineering Task Force and putting them on the ITU agenda (despite the fact that the ITU has hitherto not been involved in standard setting for internet traffic and digital trade). Thus far, China's efforts have largely proved ineffective. It struggles to build broad and genuine support for its proposals and often does not prepare well-supported and high-quality submissions. Europe, the United States, and others have benefited from this because it has allowed them to recognize China's attempts and oppose them. However, Beijing is no doubt learning and adapting.

---

[20] International Telecommunication Union, "List of Sector Members," https://www.itu.int/online/mm/scripts/gensel11.

[21] "A Brief Introduction about New IP Research Initiative," Huawei, https://www.huawei.com/us/technology-insights/industry-insights/innovation/new-ip.

China's ability to successfully advocate for its preferred approach at the ITU depends, in part, on an apathetic and passive membership in the organization. Liberal democracies need to re-engage across the board at these often bureaucratic, slow-moving, and frustrating institutions to ensure that each and every proposal is thoroughly vetted. Moreover, for these efforts to be truly successful, they must not merely be defensive reactions to malign Chinese proposals but offer positive alternatives. As is discussed in chapter 6, the United States and like-minded countries need to develop a new framework to provide a constructive and pragmatic agenda for the ITU, otherwise China may still win with its state-centric approach to data and internet governance.

China's Selective Attempts to Influence Data Discussions at the G-20

While the G-20 is not generally a forum for action or binding commitments, it has become a focal point in the conflict between China (and Russia) and the EU, Japan, the United States, and others on statements around global data flows and data governance. China has generally limited efforts by these countries to use G-20 meetings and statements to advocate for ambitious statements on the free flow of data. While China and Russia signed onto the Osaka Track framework (inspired by Japan's proposal for "data free flow with trust") to promote the drafting of international rules on the free movement of data, this does not mean they support its aims or how Japan and the United States interpret the framework. As with GIDS, China will define and apply these terms and concepts in its own way. Beijing's predictable opposition is why Washington does not prioritize the G-20 as a forum for meaningful debates around data flows and digital trade.

China will interpret G-20 statements and commitments in its own way given that they are nonbinding. However, Beijing is getting more proficient and creative in trying to embed its preferred terminology and concepts. For example, before 2020, Indonesia was not active on data and digital issues at the G-20, including on China's previous efforts to get GIDS and "data security" into G-20 statements. Yet after their cooperation on Covid-19 vaccine clinical trials and production, Indonesia started actively supporting the concept of data security in G-20 documents, including in the 2021 G-20 statement from Rome (though the final statement did not include a reference). There have been other anecdotal cases where Mexico and others made noticeable changes to their usual statements on data governance following Chinese vaccine diplomacy.

Direct Engagement by China's Government and Private Sector on Data and Digital Governance

China is directly and indirectly affecting individual countries' domestic development of data governance policies through both organic influence and direct, digital economic statecraft. Many countries (both developing and developed) see China's model of digital development and control as a success—one they want to replicate. Many are drawn to the approach because they too prioritize state-directed, protectionist economic policies and political control over free markets, open trade, and human rights. In this way, China has an indirect effect as countries voluntarily adopt similar policies. But Beijing also increasingly pursues digital economic statecraft as the CCP and private sector (both jointly and independently) advocate for their preferred data governance policies, often alongside China-supported ICT infrastructure deployments.

Government-to-government: Advocating for data localization regulations. In Africa, China is leveraging a combination of bilateral and regional government-to-government and Chinese

private-sector tech engagement to influence both hardware and data and digital policies.[22] Infrastructure is the starting point for extensive engagement and advocacy, and China offers preferential financing for its firms to construct submarine cables and 5G and other telecommunication networks.[23] But the scope of its engagement is evolving. Several countries, including Kenya, Nigeria, Sierra Leone, and South Africa, have considered or enacted data localization policies and embraced notions of cyber sovereignty at the same time that Huawei and other Chinese firms were building data centers and expanding cloud services.[24] Many countries are also considering using other China-related tech tools (e.g., surveillance) and digital regulations around content moderation (e.g., stifling free speech online).[25]

For instance, in 2015, China selected Tanzania as a pilot country for targeted capacity building, including on digital governance. Technical assistance from China influenced restrictions found in Tanzania's cybercrime law as well as other laws that resemble Beijing's restrictive control of digital content.[26] Huawei built much of Tanzania's ICT infrastructure as well as its national data center. China continues to use high-level engagement to build on this early success. In August 2021 the Cyberspace Administration of China hosted the ministerial-level China-Africa Internet Development and Cooperation on Digital Innovation Forum, where China outlined its various initiatives to build ICT and digital economic connectivity with Africa. Elsewhere, it funded a Huawei-built national data center for Senegal. As part of this project, Senegal decided to replicate China's approach of requiring that all data from state-owned enterprises and the government be stored locally.[27]

China's government and commercial engagement provides a foundation for engagement at the African Union as it considers developing a regional digital economic framework as a follow-up to the recently enacted African Continental Free Trade Area.[28] The initial debate has often revolved around the major data governance models—U.S.-style data-driven innovation and digital free trade, EU-type precautionary principle and restrictive regulations, and China-like digital control and protectionism—with many being drawn to the Chinese model. While the African Union and its members are obviously the final decision-makers, and there are many factors involved in building these frameworks, China is actively engaged in the debate alongside government and private-sector representatives from the United States, Europe, and elsewhere.

Private-sector advocates: Chinese firms advocating for data localization. Chinese tech companies play a key supporting role in advocating for the government's preferred approach to data governance, especially as it relates to data localization. Alibaba Cloud and Tencent Cloud are

---

22 Samantha Hoffman, "Double-Edged Sword: China's Sharp Power Exploitation of Emerging Technologies," National Endowment for Democracy, April 2021, https://www.ned.org/wp-content/uploads/2021/04/Double-Edged-Sword-Chinas-Sharp-Power-Exploitation-of-Emerging-Technologies-Hoffman-April-2021.pdf; and Khwezi Nkwanyana, "China's AI Deployment in Africa Poses Risks to Security and Sovereignty," Australian Strategic Policy Institute, Strategist, May 5, 2021, https://www.aspistrategist.org.au/chinas-ai-deployment-in-africa-poses-risks-to-security-and-sovereignty.

23 Cory and Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally."

24 See, for example, Chike Onwuegbuchi, "Stakeholders Seek Stronger Data Sovereignty Initiatives for Nigeria," *Guardian* (Nigeria), January 31, 2020, https://guardian.ng/technology/stakeholders-seek-stronger-data-sovereignty-initiatives-for-nigeria.

25 Tomiwa Ilori, "How Social Media Companies Help African Governments Abuse 'Disinformation Laws' to Target Critics," Rest of World, November 4, 2021, https://restofworld.org/2021/social-media-africa-democracy; and Rebecca Arcesati, "China's Evolving Role in Africa's Digitalisation: From Building Infrastructure to Shaping Ecosystems," Italian Institute for International Political Studies, July 29, 2021, https://www.ispionline.it/en/pubblicazione/chinas-evolving-role-africas-digitalisation-building-infrastructure-shaping-ecosystems-31247.

26 Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *Atlantic*, June 18, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033.

27 Ministry of Foreign Affairs (PRC), "Remarks by Assistant Foreign Minister Deng Li at China-Africa Internet Development and Cooperation Forum," August 24, 2021, https://www.fmprc.gov.cn/eng/wjbxw/202108/t20210825_9134689.html.

28 See African Union, "Decision on the African Continental Free Trade Area (AfCFTA)," February 9–10, 2020, available at https://www.tralac.org/documents/resources/cfta/3176-au-assembly-decision-on-the-afcfta-february-2020/file.html.

rapidly expanding in open cloud service markets around the world, especially in the Asia-Pacific, and have shown that they are willing to advocate for localization policies. They do this in part to differentiate themselves and seize market share from U.S. and other foreign cloud providers that generally oppose localization. The general manager of Alibaba Cloud India said the company, which has set up data centers in India, sees a big opportunity in the Indian government's push toward data localization.[29] Alibaba Cloud's president made similar comments, stating the "need to respect laws on data security and privacy. It is the most fundamental one. We insist on localization of data. Indian data should be stored in India. That is our principle."[30] Sometimes Chinese firms are more subtle and indirect, as in Chinese investors' advocacy for data localization by Indian payment firm Paytm during India's debate about payment data (which was ultimately enacted).

U.S. cloud service providers and other tech firms generally oppose data localization and expansive government requests for data as they add unnecessary costs and complexities to global IT systems and operations. U.S. firms want to leverage the distributed nature of the internet to provide their services globally rather than build out unique IT systems for every market. Major U.S. tech firms also tend to carefully review each government request for data to ensure it is legitimate and abides by local laws. This legalistic approach can be long and complicated if it involves data in multiple jurisdictions, which can frustrate local policymakers. U.S. firms have stated that they are not generally losing contracts to Chinese firms on price or services, but Alibaba's and Tencent's advocacy on data localization and seamless government access to data is proving successful in some markets (especially for government-contracted data and services). Many government officials around the world—particularly in law enforcement and national security agencies—prioritize control over data. Thus, a sales strategy of giving local governments what they want, in terms of local storage and control, can be effective.

Chinese tech firms' advocacy on data localization represents an alignment of commercial and government interests. Domestically, tech champions like Tencent and Alibaba are key beneficiaries of Chinese digital protectionism and asymmetric internet and data access.[31] Overseas, Chinese firms advocate for data localization as part of government-related efforts (as in Tanzania and Sierra Leone), but also independently. These firms sometimes self-brand projects as being related to the government's Digital Silk Road initiative in an effort to score political—and perhaps financial—support from Beijing. Alibaba Cloud and Tencent Cloud are major players globally but still lag behind AWS, Microsoft, and Google in size, capability, and coverage. Alibaba is the world's fourth-biggest cloud-computing service.[32] Tencent Cloud remains dependent on its protected home market, which alone gives it a larger worldwide market share than IBM or Oracle.

---

[29] Surabhi Agarwal, "Alibaba Cloud Sees a Bright Lining in Data Localisation," *Economic Times*, November 1, 2018, https://economictimes.indiatimes.com/tech/internet/alibaba-cloud-sees-a-bright-lining-in-data-localisation/articleshow/66454149.cms?from=mdr.

[30] R. Dinakaran, "Alibaba Ready to Comply with Govt Policy on Data Localization," *Business Line*, September 19, 2018, https://www.thehindubusinessline.com/info-tech/alibaba-ready-to-comply-with-govt-policy-on-data-localisation/article24987381.ece; and Mugdha Variyar, "Alibaba Backs Data Localisation in India; Looks to Grow Its Cloud Presence," *Economic Times*, September 19, 2018, https://economictimes.indiatimes.com/internet/alibaba-backs-data-localisation-in-india/articleshow/65869783.cms.

[31] Chen Weixuan et al., "宏观经济增长框架中的数据生产要素:历史、理论与展望｜企鹅经济学" [Data Production Factors in the Framework of Macroeconomic Growth: History, Theory and Prospects], Tencent Research Institute, June 12, 2020, https://tisi.org/14625.

[32] Jane Zhang and Minghe Hu, "Alibaba Says Its Cloud Computing Business Holds Tremendous Potential as China Picks Up Pace on Digitalisation Drive," *South China Morning Post*, February 3, 2021, https://www.scmp.com/tech/big-tech/article/3120289/alibaba-says-its-cloud-computing-business-holds-tremendous-potential.

China's Approach to Data Governance in Trade Agreements

China's approach to data and digital trade negotiations is evolving, but not in a direction that will allow the free flow of data. China will likely push for a vaguely defined, self-judging "national security" exception in any digital trade agreement so that it can keep its array of localization measures in place. Essentially, Beijing wants new digital trade agreements to conform to its restrictive approach to data governance.

Traditionally, China has refused to negotiate trade rules around data flows, data governance, and digital trade, citing sovereignty. This was due, in part, to losing a WTO dispute on its regulation of publications and audiovisual products in 2010. China's approach shows that Chinese policymakers cannot reconcile a strident view that sovereignty in the cyber realm supersedes the need to voluntarily limit it as part of international trade agreements or other international negotiations. Likewise, China has refused to join the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system, which it sees as a U.S. plot to steal its data.[33] It generally opposes efforts by small groups of countries to determine key norms and rules, especially if it is not part of the rulemaking. For example, Zhang Jun told the UN Security Council that "'small circles' should not decide cybersecurity governance, and interference in nations' internal affairs should be avoided."[34] This also presumably covers various efforts in the Asia-Pacific to create new digital trade rules that support the free flow of data and prohibit data localization.

However, China is increasingly interested in joining forums and agreements where small groups of countries are working together on new digital trade rules and mechanisms for cooperation on digital economic governance. In 2021, it applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA). The latter agreement involves Chile, New Zealand, and Singapore. China's interest is especially stark given the lack of U.S. involvement. Both agreements include strong, enforceable provisions on data flows and digital trade—and lack a self-judging national security exception—that would likely require Beijing to make substantive changes to domestic laws and regulations. DEPA is not just a trade agreement but a forum for cooperation on digital and data-related issues such as AI, data privacy, digital identities, e-invoicing, fintech and e-payments, and open government data.

Whether China's interest in joining the CPTPP and the DEPA is genuine or not, a case could be made that it wants to be involved in small Asia-Pacific initiatives that can evolve and shape regional rules. For example, the P4 trade agreement between Brunei, Chile, Singapore, and New Zealand eventually became the CPTPP. China's potential involvement in these agreements is likely based on the key caveat that there are broad, self-judging exceptions for privacy and national security that allow it to keep its myriad data localization and data restrictions in place. This again demonstrates how China wants to follow a separate set of rules domestically from the ones it advocates for abroad—open digital markets for Chinese firms, but a closed domestic market for foreign firms.

Another sign of China's evolving approach to data and digital trade is that it has made its first commitments on both issues in the Regional Comprehensive Economic Partnership (RCEP).

---

[33] Nigel Cory, "Why China Should Be Disqualified from Participating in WTO Negotiations on Digital Trade Rules," ITIF, May 9, 2019, https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.

[34] Amber Wang, "China's UN Envoy Calls for Equality in Shaping Cyberspace Norms," *South China Morning Post*, June 30, 2021, https://www.scmp.com/news/china/diplomacy/article/3139348/chinas-un-envoy-calls-equality-shaping-cyberspace-governance.

However, RCEP provisions on data flows are largely symbolic because they are not subject to dispute settlement, thus making them unenforceable, and are weaker than provisions in the WTO General Agreement on Trade in Services, to which China is a party.[35] However, China is not solely responsible for the RCEP outcome. India also pushed for the self-judging national security exception before ultimately deciding it did not want to join the partnership. The e-commerce chapter was concluded before India left negotiations, and the remaining parties decided that it would be too difficult to reopen the text. However, two key data-related provisions in the RCEP (Articles 12.14 and 12.15) notably include a trade test that acts as a guardrail against parties misusing legitimate public policy exceptions (like privacy and national security) to enact arbitrary, discriminatory, and disguised barriers to trade.

Similarly, China initially opposed the 2017 launch of the WTO's Joint Statement Initiative on E-commerce that was supported by the United States and dozens of other countries. Only in 2019 did China decide to join when it saw that members were serious about making progress and did not want to miss out on a chance to shape the rules. Thus far, China has been fairly constructive in discussions. As of April 2021, it had provided 4 of the 52 submissions. China has had the opportunity to grandstand and obstruct early discussions on data but has not succeeded, despite its first submission explicitly opposing talks on data and digital trade (it wanted talks to focus on goods-based e-commerce).[36] During plenary discussions early in negotiations, countries could not agree that data should be included. But in 2021, all 86 participating countries (including China) agreed that data is important to negotiations. Negotiators have been able to finalize multiple non–data specific provisions without opposition from China. While this may seem to be a low bar to clear, Beijing could have obstructed even these outcomes. Since then, the tone of discussions around data has changed, as countries realize that an agreement will have no credibility without data-related provisions. However, this is all a prelude to negotiations on actual text around data and how to design a framework that allows digital free trade, which is deliberately being left to the end due to sensitivity surrounding the issue.

When negotiations finally get to the issue of data and data flows, China's position will likely focus on two key components. The first centers on how parties negotiate exceptions to rules that protect data flows and prohibit data localization. Thus far, China has not been forced to articulate its position, as the United States and EU are at loggerheads over data flows and privacy. Similar to China, the EU wants a self-judging exception, but to protect privacy, allowing it to justify data localization in the name of privacy.[37] China's submission shows it wants a broad, self-judging exception for cyber and national security.[38] Until the U.S.-EU dispute is resolved, China does not need to make its position clear and will thus avoid the inevitable opposition to having a broad loophole for national security, privacy, and public morals. Second, China's approach will also depend on whether the final agreement includes tiered commitments, especially for developing countries. If such commitments are included and China is unhappy with the data-related provisions and exceptions, it could opt out by only agreeing to join the lower tier.

---

35 Regional Comprehensive Economic Partnership, "RCEP Agreement," https://rcepsec.org/legal-text.

36 WTO, "Joint Statement on Electronic Commerce: Communication from China," INF/ECOM/19, April 24, 2019.

37 Nigel Cory, "EU Digital Trade Policy Proposal Opens a Loophole for Data Protectionism," ITIF, July 16, 2018, https://itif.org/publications/2018/07/16/eu-digital-trade-policy-proposal-opens-loophole-data-protectionism.

38 WTO, "Joint Statement on Electronic Commerce: Communication from China," INF/ECOM/32, May 9, 2019.

China is making a canny and cynical series of strategic decisions in changing its approach on data flows and digital trade, especially given the lack of U.S. involvement and leadership. It is possible that China will sign on to ambitious provisions related to data and digital trade if it can get broad self-judging exceptions for national security and other interests that allow it to essentially circumvent the intended impact of these new rules. The odds of its success depend on strong and concerted U.S. opposition and coordination with liberal democracies on achieving an ambitious and meaningful outcome on data flows at the WTO and elsewhere.

Recommendations

The United States needs to develop a whole-of-government global digital strategy to counter China's growing and multifaceted efforts to advocate for a top-down, state-controlled internet. Data flows and data governance are two critical parts, but there are many others. The following recommendations specifically relate to international data governance.

First, the United States and like-minded countries need to pay more attention to the forums where China is seeking to influence local and international data governance, as each successful case adds up and over time benefits Beijing's strategic effort to advocate for a top-down, state-managed internet. The United States and others need to move on from a largely ad hoc response to a detailed and coordinated all-points strategy that responds to China at every forum and level (i.e., country, regional, and multilateral). Time is of the essence given the lack of concrete rules around data and the fact that so many countries are reforming domestic data governance laws and regulations. As countries develop these regimes, they are actively looking to leaders for ideas and guidance.

Further, realistic and constructive alternatives to the infrastructure and digital policy ideas China is promoting need to be offered. The United States, Australia, and others have started doing this, such as via the Blue Dot Network, but more needs to be done. Thus far, China has focused largely on ICT infrastructure, with a few instances where the government and private sector have supported restrictive digital regulations. Given these examples, it is feasible that Chinese-built ICT infrastructure and data centers will be increasingly deployed alongside China-inspired localization requirements that act as the leading edge for related digital technologies and policies. This risk is particularly acute for countries that have authoritarian tendencies. The challenge for the United States and others is to develop and deploy a more coordinated and effective approach to digital policies, such as data privacy, cybersecurity, content moderation, government access to data, and other digital issues, to compete with China's policies. This will not be easy, given that each country has its own strategy. But developing and advocating for alternative digital policies will be crucial as officials in countries look for pragmatic advice on how to address these pressing issues.

Second, the United States needs to broaden its cyber diplomacy engagement and educational outreach. It can no longer expect to shape the final outcome in negotiations with small groups of countries. Russia and China are playing the full field in terms of engaging all countries involved in UN and ITU discussions. The United States needs to do the same, much like U.S. partners that are more pragmatic and proactive in working with as many countries as possible to sway undecided countries before major decisions on cyber are made.

The United States also needs to prepare educational material and digital development assistance to build genuine support for its preferred policies. For example, Huawei's New IP proposal initially received reasonable support among African countries before they understood its full implications.

Education is the foundation for building coalitions around these new issues. Countries in Africa and other regions need assistance on digital economy, data privacy, and cybersecurity issues. Chinese companies have been capitalizing on this to expand the scope of the ITU in a way that suits China's broader objectives. The United States and others need to do more to ensure that these issues are addressed in the proper forum and receive greater support, such as digital development assistance through the U.S. Agency for International Development.

The United States also needs to devote more staff to actively engage in UN, ITU, and WTO discussions on digital and cyber issues. In many cases, the United States is missing in action, and if officials are there, they are not proactively providing material and ideas to drive the agenda. U.S. partners are often surprised at the lack of U.S. interest and pressure. Likewise, the United States needs to provide resources and support for private-sector participants to be consistently engaged at UN and ITU discussions. At the moment, there are few Western firms that consistently go to the ITU for standards work. Often there are only a handful of European and other officials present to oppose bad proposals, and it is difficult to hold the line against concerted Chinese efforts across the ITU's eleven study groups and other committee meetings.

Third, the United States and like-minded countries should proactively outline and advocate for an ambitious, binding set of rules to support data flows and prohibit data localization, with narrow, targeted exceptions for privacy and national security. Negotiations on these issues at the WTO are likely to come down to the scope of exceptions. Europe wants a broad self-judging exception for privacy, while China wants the same for national security. One option is using the UK–EU adequacy decision as the basis for a balanced framework. Reaching an agreement between the United States and EU on the issue of privacy is central to pressuring China to sign onto ambitious data flow provisions that would require it to remove the majority of its localization policies.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 5

Reshaping the Battlefield: The Security Implications of China's Digital Rise

Greg Levesque

GREG LEVESQUE is Co-founder and CEO of Strider Technologies. He is a leading expert on economic statecraft, working with Fortune 500 companies and government agencies in North America and Europe to identify, assess, and respond to security risks from nation-state sponsored commercial activity. He has working proficiency in Mandarin Chinese and can be reached at https://www.striderintel.com/contact.

EXECUTIVE SUMMARY

This chapter finds that China's digital ambitions—particularly the use of commercial entities as part of its strategy to achieve those ambitions—present an imposing threat to the market norms, values, and prosperity that undergird the existing global system and its security.

MAIN ARGUMENT

The threat posed by China's digital strategy is especially acute because of the nature of technologies catalyzing the fourth industrial revolution, which are enabled by a mutually reinforcing and interactive "digital triad" of information and communications technology infrastructure, big data, and artificial intelligence. By allowing states at the forefront of this revolution to formulate more effective responses through greater access to information and rapid analysis of data, while also influencing the information environment of adversaries, this triad converts data into a competitive battlespace extending across boundaries, domains of state interaction (e.g., military and commercial), and the real and virtual worlds. China aims to be the first country to merge the components of the digital triad to not only drive economic development and commercial value but also enhance the competitiveness of its diplomatic, military, and intelligence operations. Successfully combining and managing these technologies could very well grant China global technological superpower status, accompanied by all the negative externalities of an authoritarian nation-state's control over the international information system.

POLICY IMPLICATIONS

- China's digital strategy has the potential to undermine the ability of the U.S. and its allies to project diplomatic and military power in key regions around the world, as well as to reduce companies' abilities to operate in those markets.
- China's emphasis on leveraging corporate players and competing in commercial domains constitutes a different approach from that seen in past nation-state competition and recasts the corporate domain as a nation-state battlespace. Traditional modes and mechanisms of international competition, like military deployments and actions in institutions of multilateral governance, are insufficient to address Beijing's challenge, and new tools must be developed.

China's digital ambitions—particularly the use of commercial entities as part of its strategy to achieve those ambitions—present an imposing threat to the market norms, values, and prosperity that undergird the existing global system and its security. This is a multilevel threat: Beijing's efforts to claim the architecture of a digital world endangers the ability of both international militaries and commercial players to operate competitively. It also endangers individuals' privacy, the integrity of the information they receive, and the interactions on which the digital world depends.

The threat posed by China's digital strategy is especially acute because of the nature of technologies catalyzing the fourth industrial revolution, which are enabled by a mutually reinforcing and interactive "digital triad" of information and communications technology (ICT) infrastructure, big data, and artificial intelligence. By allowing states at the forefront of this revolution to formulate more effective responses through greater access to information and rapid analysis of data, while also influencing the information environment of adversaries, this triad converts data into a competitive battlefield extending across boundaries, domains of state interaction (e.g., military and commercial), and the real and virtual worlds.[1] China aims to be the first country to merge the components of the digital triad to not only drive economic development and commercial value but also enhance the competitiveness of its diplomatic, military, and intelligence operations. Successfully combining and managing these technologies could very well grant China global technological superpower status, accompanied by all the negative externalities of an authoritarian nation-state's control over the international information system.

How the United States and its allies choose to interpret and respond to the digital ambitions of the People's Republic of China (PRC) will determine how the ongoing fourth industrial revolution affects the balance of power in years to come. The contest for influence over the emerging global digital ecosystem will define 21st-century global strategic competition. This chapter seeks to underline this point by illustrating the immediate security implications of Beijing's digital strategy. It details the security threats that could emerge from a China-controlled digital architecture and the information advantage and coercive leverage such control would grant Beijing. This chapter also explores Beijing's use of commercial entities to execute its digital strategy and assesses the challenge this poses for both increasing international recognition of China's actions and formulating a competitive response.

Digital China and the Security Implications of Modern Economic Statecraft

The PRC is constructing a global digital architecture to shape, manage, and control the international information environment by developing and exporting coercive tools of control.[2] These activities threaten the existing international system and the norms on which it rests. They also threaten international security along traditional military dimensions, as well as economic, informational, and political ones. Beijing's particular approach to digital competition risks obscuring the nature, immediacy, and severity of the threat. As illustrated in earlier chapters,

[1] For an expert assessment of China's industrial policy and the reinforcing dynamics of ICT infrastructure, data, and artificial intelligence, see Barry Naughton, *The Rise of China's Industrial Policy: 1978 to 2020* (Mexico City: National Autonomous University of Mexico, 2021).

[2] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," Australian Strategic Policy Institute, Policy Brief, no. 21, 2019.

China pursues its digital ambitions through commercial as well as government actors, projecting power in domains and through players that are not traditionally considered within the framework of national security. These gray-zone activities represent a core pillar of Beijing's approach to competition in the digital era. They demand that the United States and other liberal democracies acquire a broader perspective of security and competition, one that accounts for not only traditional military and intelligence concerns and actors but also economic and political ones. The core security implications of Beijing's digital ambitions as they apply to, and take advantage of, both traditional and nontraditional security domains include the following:

- A state-driven agenda that forces companies to pursue government interests, blurring the lines of traditional commercial competition and converting the commercial domain into a battlespace—which presents an immediate national security concern.
- The use of global digital systems, including commercial platforms, to acquire superior information—and therefore an advantage in military, commercial, and political competition—as well as to restrict, deny, or distort other nations' access to information.
- The use of global digital systems to shape the international information environment, including through dissemination of propaganda and disinformation.
- Efforts to dominate critical nodes in strategic, digital-relevant industry chains and infrastructure and convert them into coercive leverage, political influence, and outsized economic returns.
- Efforts to undermine the incentives and legal structures that drive Western innovation, chiefly the concept and protection of intellectual property (IP) rights, and in the process unfairly advantage China's development of advanced technologies.

The rest of this chapter also emphasizes Beijing's expanding use of commercial actors for national strategic ends and the resultant redefinition of commercial activity as a domain of battle. This is a redefinition with which the United States and other liberal democracies are only beginning to wrestle and that demands a new generation of competitive frameworks.

A Clear Agenda and Expansive Footprint

The risks identified in the preceding section are not just notional. They are evident in the digital architecture China is already developing and its discourse that explicitly describes an agenda for digital control to advance strategic ambitions. When engaging with the international system, Beijing touts the economic and social benefits of its investments in digital infrastructure and the positive role of Chinese companies in emerging economies around the world. But the reality is more nuanced. Generally speaking, these activities answer to the Chinese government's foreign policy objectives and agenda. In 2018 the China Academy of Information and Communication Technology, a scientific research institute under the PRC's Ministry of Industry and Information Technology, described the strategic underpinnings of the "going out" of Chinese ICT companies as follows:

- Safeguard China's national security by establishing an autonomous and controllable closed-loop digital ecosystem with communications equipment and internet applications that improve the level of network information security.
- Advance PRC international influence and soft power by expanding the global network layout and controlling capabilities of telecommunications equipment, expanding foreign exchanges

and cooperation, building a community of shared interests and shared destiny in the network age, and expanding the influence of Chinese culture and ideology.

- Resolve domestic overcapacity issues within China's ICT industry to provide revenue growth for Chinese companies and consolidate China's position as the industry's global leader.[3]

This framing makes clear that China's digital "going out" policy serves a larger strategic agenda intended to shape the international community according to Beijing's vision. The called-for construction of a Chinese-led, closed-loop digital ecosystem is already underway, creating the foundation of a network-led "community of shared interests and shared destiny." The United States and other liberal democracies should take note of this strategic objective.

Countries concerned about China's growing digital influence should also note the wide-ranging network of actors supporting Beijing's agenda. International focus has oriented around Huawei and other national champions, but a bevy of lesser-known state-backed corporations also support Beijing's digital ambitions abroad. They assist PRC efforts to achieve information superiority, form critical nodes in strategic digital-relevant industry chains, and execute national strategies. Some state-backed corporations have been formed with the sole purpose of constructing and managing a hub-and-spoke arrangement of integrated information technology platforms and networks. These networks span the internet, telecommunications, financial payments, big-data centers, submarine cables, and cloud computing.

Beijing has already made extensive inroads. Current initiatives in the Digital Silk Road appear focused on integrating China with neighboring countries in the Association of Southeast Asian Nations (ASEAN) and Eurasia. The China-ASEAN Information Harbor Digital Economy Alliance represents one such initiative led by the PRC government to form a digital infrastructure ecosystem interweaving China with Southeast Asian nations that could in time serve as a bulwark hindering U.S. commercial pursuits and establishing new standards and norms for digital operators in the region. First proposed by the Cyberspace Administration of China and the Guangxi regional government in 2015, the alliance pursues an ambitious plan to "deepen network interconnection and information exchange" between China and ASEAN countries. This has led to the construction and management of a "new internet exchange" hub in Nanning by China's three state-owned telecom operators, as well as submarine fiber-optic projects and a big-data information exchange platform to "explore new models of big data utilization" and "guide relevant government departments."

Demonstrating the nontraditional role enterprises are playing in implementing the PRC government's strategy, the alliance is led by China-ASEAN Information Harbor Company (China Eastcom), a state-controlled information technology company approved by the State Council and based in Guangxi.[4] China Eastcom does not appear to operate according to market directives. Instead, it is tasked with constructing an "international communication network system and network hub with Guangxi as the core, facing ASEAN and serving China's southwest

---

[3] Chen Hui and Dong Jianjun, "加快推进'一带一路'信息通信业走出去" [Accelerate the Advancement of "One Belt One Road" Information and Communication Industry's Going Out], China Academy of Information and Communication Technology, November 14, 2018, http://www.caict.ac.cn/kxyj/caictgd/201811/t20181114_188712.htm.

[4] "广西壮族自治区人民政府办公厅关于印发 中国—东盟信息港建设实施方案 (2019—2021年)"[Notice of the General Office of the People's Government of Guangxi Zhuang Autonomous Region on Printing and Distributing the Implementation Plan for the China-ASEAN Information Port Construction (2019–2021)], General Office of the People's Government of Guangxi Zhuang Autonomous Region, June 27, 2019, http://www.gxzf.gov.cn/zfgb/2019nzfgb/d14q_35435/zzqrmzfbgtwj_35436/t1514610.shtml; and the China-ASEAN Information Harbor website, http://www.caih.com.

and central south."[5] The company, with support from Guangxi and central government agencies, is driving China-ASEAN network integration and information exchange to promote the Digital Silk Road. Foreign governments appear unaware of the company's true origins and objectives.[6]

China Eastcom is not an outlier. Another company, Silk Road Information Port Co., serves a similar purpose. Based in Gansu Province, it is a state-owned enterprise operating as a "strategic fulcrum" to advance transnational cooperation and the formation of a "Silk Road information corridor" for Central and West Asia, as well as the Middle East.[7] The company is overseen by the vice provincial governor Zhang Shizhen and owned by eight provincial-level state-owned enterprises, including China Unicom and China Telecom.[8]

Constructing a Digital Infrastructure for the "Information Advantage"

As this report has demonstrated, China is developing and exporting a network of digital infrastructure globally. This includes physical infrastructure as well as virtual platforms (discussed in chapters 1 and 2, respectively). These are predominately built by national commercial champions under Beijing's direction; they are tools in a national geopolitical agenda rather than products of organic market activity. This digital infrastructure may allow China to gain global information advantages that both support its own security apparatus and threaten the security of its competitors. Construction of digital infrastructure abroad promises Beijing superior access to information, including in a manner that supports and informs military and intelligence operations. As discussed in the following section, this infrastructure also promises China the ability to restrict, distort, or deny information—and therefore the virtual activity that depends on that information.

This first-order security threat—as well as the surveillance implications of China's control over its commercial champions—is well illustrated by a series of cyberespionage campaigns targeting the African Union over the past ten years. In March 2018, French newspaper *Le Monde* revealed that between 2012 and 2017 confidential data on an African Union ICT system provided by Huawei had been routed to a server in Shanghai each evening.[9] Two years later, in December 2020, Japan's Computer Emergency Response Team alerted African Union officials that Chinese hackers were stealing massive amounts of camera footage from the African Union headquarters. The headquarters had been constructed by the state-owned China State Construction Engineering Corporation in 2012 and still retained Chinese technicians to help maintain its digital systems.[10]

This example of Beijing's intelligence services leveraging overseas digital infrastructure constructed or operated by Chinese companies to collect high-value information is not an outlier. It is a matter of law. Article 7 of China's 2017 National Intelligence Law requires "any organization

---

[5] See the Cyberspace Administration of China, http://www.cac.gov.cn/dmxxg.htm.

[6] China-ASEAN Information Harbor website; and Li Sugen, "广西布局数据中心,以南宁为核心打造国家级新基建算力基地" [Layout of Data Centers in Guangxi, with Nanning as the Core to Build a National-Level New Infrastructure Computing Base], Nanning TV News, August 11, 2020, http://www.nntv.cn/news/m/2020-8-11/1597114907639.shtml.

[7] See "战略" [Our Strategy], Silk Road Infoport Co. Ltd., http://www.silkip.com/zl/zl1.

[8] "甘肃省人民政府关于 省长、副省长、秘书长工作分工的通知" [Notice of the People's Government of Gansu Province on the Division of Work of the Provincial Governor, Deputy Governor and Secretary General], Gansu Provincial Government, August 30, 2021, http://www.gansu.gov.cn/gsszf/c100054/202108/1792301.shtml.

[9] Ghalia Kadiri and Joan Tilouine, "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin" [In Addis Ababa, the African Union Headquarters Spied On by Beijing], *Le Monde*, January 26, 2018, https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

[10] Raphael Satter, "Suspected Chinese Hackers Stole Camera Footage from African Union—Memo," Reuters, December 16, 2020, https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB.

or citizen" to "support, assist, and cooperate with state intelligence work."[11] Article 28 of its Cybersecurity Law requires network operators to "provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[12]

China's presence on the African continent is expansive and growing. The extent of the presence indicates the pervasiveness of China's information threat. Chinese ICT firms, led by Huawei, established a major foothold in African telecommunications infrastructure long before the formal announcement of the Belt and Road Initiative. Some date Huawei's first forays into African countries back to 1996.[13] And its digital infrastructure construction has propagated over the last quarter-century: as of 2021, Huawei alone had built 50% of the African continent's 3G networks and 70% of its 4G networks.[14] The Cyberspace Administration of China is now pursuing the China-Africa Partnership Plan on Digital Innovation to solidify China's position on the continent, which includes preparations to expand Chinese digital platforms as well as construct physical infrastructure like smart cities and 5G networks.[15] Entrenching PRC ICT firms in Africa is a clear policy objective for Beijing and is viewed as a means to compete with Washington to expand China's influence and control over emerging global digital architecture.[16]

Shaping the Information Environment

The information advantage that China's digital infrastructure provides does not end at information collection. Beijing can also distort, restrict, or deny information to its competitors, whether those be governments, militaries, or commercial actors. Smart logistics hubs and IT logistics standards (discussed in chapter 3) offer ripe examples. These systems depend on data to enable streamlined movement and exchange. Beijing could use control over Chinese-built logistics infrastructure and platforms to cut users off from necessary data streams. This is already happening as a result of its Personal Information Protection Law, which went into effect in November 2021.[17] Doing so could force operations at a targeted port to shut down, leave a shipping company's fleets stranded in the middle of the ocean, or even stall a government's customs processes. More subtle than outright restriction, Beijing could also distort the information streams on which this infrastructure relies. For example, incorrect information could be fed into customs databases, permitting the inflow of illicit goods. As these examples indicate, China's global digital architecture allows it to shape the digital environment—not only to obstruct competitors' activities

---

11 National People's Congress of the People's Republic of China (PRC), "中华人民共和国国家情报法" [National Intelligence Law of the People's Republic of China], June 12, 2018, http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml.

12 Cyberspace Administration of China, "中华人民共和国网络安全法" [Cybersecurity Law of the People's Republic of China], November 7, 2016, http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

13 Jevans Nyabiage and Jodi Xu Klein, "Years before China's Belt and Road Plan Got Its Name, Huawei Was Driven to Seek Emerging-Market Contracts," *South China Morning Post*, April 16, 2020, https://www.scmp.com/business/companies/article/3080076/years-chinas-belt-and-road-plan-got-its-name-huawei-was-driven.

14 Jie Xi, "Analysts: China Expanding Influence in Africa via Telecom Network Deals," Voice of America, August 14, 2021, https://www.voanews.com/a/economy-business_analysts-china-expanding-influence-africa-telecom-network-deals/6209516.html.

15 China will work with Africa to formulate and implement the China-Africa Partnership Plan on Digital Innovation. See Ministry of Foreign Affairs (PRC) website, August 24, 2021, https://www.fmprc.gov.cn/eng/wjbxw/202108/t20210825_9134687.html.

16 "中非数字合作前景广阔" [Bright Prospects for China-Africa Digital Cooperation], *People's Daily*, September 27, 2021, http://world.people.com.cn/n1/2021/0927/c1002-32237623.html; and Mohammed Yusuf, "China's Reach into Africa's Digital Sector Worries Experts," Voice of America, October 22, 2021, https://www.voanews.com/a/china-reach-into-africa-digital-sector-worries-experts/6281543.html.

17 Jonathan Saul and Eduardo Baptista, "Off the Grid: Chinese Data Law Adds to Global Shipping Disruption," Reuters, November 17, 2021, https://www.reuters.com/world/china/off-grid-chinese-data-law-adds-global-shipping-disruption-2021-11-17.

but also to fuel Beijing's champions. This threatens the integrity of global information (and the decisions built on it) at the personal, corporate, and government levels.

At the personal level, for example, China can use its platforms to spread propaganda or disinformation, replacing fact with its own narrative. TikTok underlines the immediacy and significance of this danger. In the first quarter of 2020, TikTok was the most downloaded app in the world.[18] In October 2020, it surpassed Instagram to become U.S. teenagers' second-favorite social media app after Snapchat.[19] TikTok is owned and controlled by ByteDance, a Chinese company, and in August 2021 the Chinese government, through a state-owned entity, claimed a board seat and stake in ByteDance.[20] ByteDance—and through it the Chinese government—are reportedly able to access the information of U.S.-based TikTok users.[21] In addition, TikTok serves as an active platform of Chinese propaganda internationally: at the behest of the Chinese government, the platform censors videos on sensitive subjects ranging from Tiananmen Square to pro-democracy movements in Hong Kong.[22] The service also has the ability to promote Chinese propaganda and disinformation. Kara Frederick, a fellow at the Center for a New American Security, observed in a 2020 interview: "If the CCP decided [through] ByteDance to feed you propaganda, you're addicted.…It is there, and you're going to get more and more and more. And there, they can tweak and see what you like, what you don't like."[23]

At the corporate level, Beijing might use its digital infrastructure to artificially enhance the competitiveness of its national-champion companies at the expense of other international players. For example, Chinese transaction and industrial platforms tend to include credit ratings. As these proliferate internationally, Beijing might inflate the ratings of its favorite players to make them the preferred choices for customers.

Finally, at the government level, China's control over digital architecture—and corresponding ability to shape information—would allow it to redirect military forces that depend on Chinese information systems, whether by adjusting their routing or feeding them false instructions. Or, as previously noted, Beijing might be able to skew customs information to allow the entry of illicit or tariffed goods into other countries. China's propaganda and dissemination of disinformation could also help stir up popular unrest or shape voter preferences, skewing the incentives and priorities of democratic governments.

Concrete Footholds: Leverage over Value Chains and Infrastructure

The security implications of Beijing's digital strategy also apply to the tangible production of digital technologies. China seeks to foster dependence on it by controlling value chains for emerging industries, which grants coercive leverage. Beijing has already shown that it is willing to

---

18 Kim Lyons, "TikTok Says It Has Passed 1 Billion Users," Verge, September 27, 2021, https://www.theverge.com/2021/9/27/22696281/tiktok-1-billion-users.

19 Salvador Rodriguez, "TikTok Passes Instagram as Second-Most Popular Social App for U.S. Teens," CNBC, October 6, 2020, https://www.cnbc.com/2020/10/06/tiktok-passes-instagram-as-second-most-popular-social-app-for-us-teens.html.

20 "Beijing Takes Stake, Board Seat in ByteDance's Key China Entity—the Information," Reuters, August 16, 2021, https://www.reuters.com/technology/bytedance-says-china-unit-holds-local-licences-response-media-report-2021-08-16.

21 Lyons, "TikTok Says It Has Passed 1 Billion Users."

22 Rebecca Jennings, "What's Going On with TikTok, China, and the U.S. Government?" Vox, December 16, 2019, https://www.vox.com/open-sourced/2019/12/16/21013048/tiktok-china-national-security-investigation; and Alex Hern, "Revealed: How TikTok Censors Videos That Do Not Please Beijing," *Guardian*, September 25, 2019, https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing.

23 Brit McCandless Farmer, "How TikTok Could Be Used for Disinformation and Espionage," CBS News, November 15, 2020, https://www.cbsnews.com/news/tiktok-disinformation-espionage-60-minutes-2020-11-15.

use this leverage. In 2010, for example, China restricted rare earth exports to Japan in retaliation for disputes over the sovereignty of the Senkaku Islands.[24]

More than a decade later, China continues to control global rare earth production, as well as the upstream and downstream value chains, despite widespread awareness of the vulnerability this creates. In 2018 the U.S. Department of Defense concluded that China poses a "significant and growing risk to the supply of materials deemed strategic and critical to U.S. national security." Not only does Beijing dominate upstream mining of critical minerals, but it is also "increasingly dominating downstream value-added materials processing and associated manufacturing supply chains."[25] Such control gives China a key advantage: foreign military or technological challenges have little credibility if they depend on core inputs from Beijing.

This dependence extends well beyond rare earths. A similar industrial asymmetry applies across critical value chains of the digital era. China's primary Internet of Things module manufacturer, Quectel, controls more than a third of the global market,[26] while China's Bitmain and MicroBT, which manufacture bitcoin mining units, have effectively no market competition.[27] Even further upstream, China dominates global production of the basket of minerals necessary for emerging technologies, including cobalt, lithium, and nickel.[28]

This control over key industrial production is no accident. Beijing's science and technology planning consistently emphasizes not only developing emerging technologies, scaling them, and setting their rules, but also developing integrated and relatively autonomous value chains. For example, Xi Jinping explained in a 2016 speech that without a solid manufacturing base for strategic technologies, Chinese technological capacity would be "a waste of work," and that "in the global information field, the ability to integrate innovation chains, production chains, and value chains has increasingly become the key to success or failure." He explained that "the final result of technology research and development in core technology should not only be technical reports, scientific research papers, and laboratory samples but should [also] be market products, technical strength, and industrial strength."[29] In other words, technological capacity requires manufacturing capacity.

China's integrated circuit program—and the supporting role of government-guidance funds—illustrates this emphasis on industrial capacity, as well as the creative measures Beijing implements in pursuit of it. China has developed a system of government guidance funds that are tasked with allocating state capital within specific industry verticals to scale up Chinese capacity and independence in strategic and high-tech industries. To date, more than $670 billion has been raised

---

24 Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010, https://www.nytimes.com/2010/09/23/business/global/23rare.html.

25 U.S. Department of Defense, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (Washington, D.C., September 2018), 96.

26 Soumen Mandal, "Quectel Widens Gap with Competition in Global Cellular IoT Module Market During COVID-Hit Q2 2020," Counterpoint Research, October 28, 2020, https://www.counterpointresearch.com/quectel-widens-gap-with-competition-in-global-cellular-iot-module-market-during-q2-2020.

27 Wolfie Zhao, "Bitcoin Mining Unit Manufacturer MicroBT Nibbles at Bitmain's Market Share," CoinDesk, February 16, 2020, https://www.coindesk.com/business/2020/02/17/bitcoin-mining-unit-manufacturer-microbt-nibbles-at-bitmains-market-share.

28 "China's Head Start: CCP Industrial Policy for Global Automotive Ascendance," Horizon Advisory, June 18, 2021, available at https://issuu.com/horizonadvisory/docs/horizon_advisory_-_china_s_head_start.

29 Xi Jinping, "习近平在网信工作座谈会上的讲话全文发表" [The Full Text of Xi Jinping's Speech at the Forum on Cybersecurity and Informatization Work] Xinhua, April 25, 2016, http://www.xinhuanet.com//politics/2016-04/25/c_1118731175.htm.

across 1,741 guidance funds, including at least $60 billion specifically allocated to the integrated circuity industry via the National IC Industry Investment Fund (Big Fund).[30]

The Big Fund poses real threats to the global semiconductor industry and U.S. national security. Chips are an integral component in advanced technology supply chains and military platforms ranging from aircraft carriers to satellites to missile systems. China has invested over $100 billion into the semiconductor industry, while also heavily subsidizing the purchase of Chinese chips domestically and targeting foreign semiconductor firms to acquire IP. This undermines U.S. and European economic competitiveness and innovation, potentially driving some firms out of business or forcing them to exit key markets, which is China's ultimate goal. In February 2018, Chen Datong, a founding partner of Hua Capital and manager of the Chinese government's semiconductor industry investment funds, delivered a speech in which he stated that the Big Fund aims to subvert the global semiconductor industry by creating overcapacity, just as China did in the solar and LED industries.

A New Technological Race and Changing Innovation Incentives

At the same time, Beijing's approach to the digital revolution is also transforming the context in which innovation takes place and the incentives undergirding it. Acquisition of foreign IP through both licit and illicit means and the subversion of strategic industries through overcapitalization are core elements of PRC digital strategy. China is willing to risk undermining the fundamental drivers of global innovation in order to impede other countries' ability to compete with it in the technological race underway.

While China is not alone in conducting economic espionage, the scope and scale of its activities are generating unmatched economic and national security risks to the United States and its allies and partners. China has developed a systematic approach to identifying, targeting, and acquiring IP and talent from around the world. IP theft erodes the long-term competitiveness of global companies, especially as stolen IP is absorbed and repurposed by Chinese firms to compete in global markets. In 2016 the U.S. Trade Representative's Section 301 investigation into Chinese trade practices assessed the cost of PRC IP theft for the U.S. economy at $400–$600 billion a year.[31] Meanwhile, the FBI has reported that it opens a new economic espionage investigation tied to China every ten hours.[32]

China's IP theft targets extend well beyond the United States. In its 2020 annual report, the Canadian Security Intelligence Service, Canada's premier intelligence agency, called out China for covertly gathering "political, economic, and military information in Canada...in support of… state development goals."[33] In 2020 the European Commission proposed hiring "civilian spy catchers" to protect research and innovation developed within research universities from being

---

[30] Ngor Luong, Zachary Arnold, and Ben Murphy, "Chinese Government Guidance Funds: An Analysis of Chinese-Language Sources," Center for Security and Emerging Technology, Georgetown University, March 2021, https://cset.georgetown.edu/wp-content/uploads/CSET-Understanding-Chinese-Government-Guidance-Funds.pdf; and Wei Sheng, "China's Second Chip-Focused 'Big Fund' Raises $29 billion," Technode, October 28, 2019, https://technode.com/2019/10/28/chinas-new-chip-focused-big-fund-raises-rmb-204-billion.

[31] Office of the United States Trade Representative, "Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of The Trade Act of 1974," March 22, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[32] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Director of the U.S. Federal Bureau of Investigation, July 7, 2020, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

[33] Canadian Security Intelligence Service, "The Threat Environment," *CSIS Public Report 2020*, April 2021, https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html.

stolen.[34] Similarly, Japan has begun paying its companies to reshore manufacturing capabilities out of China. In October 2021, Tokyo appointed a new minister of economic security to—among other things—counter economic espionage.[35]

However, China is not slowing its theft of foreign technology. In fact, its "innovation-driven development strategy," unveiled in 2016, turbocharges foreign technology acquisition programs, introduces new tools for repurposing foreign IP, and channels state and foreign capital into priority emerging technology sectors to wrest dominance from foreign innovation leaders.[36] Acquisition of foreign IP often follows a government-prescribed process of introducing, digesting, and assimilating foreign technologies that lead to re-innovated Chinese products. According to Tai Ming Cheung, this policy encourages the "going out" of Chinese firms to gain access to foreign R&D and technology. It also seeks to entice foreign companies to establish R&D facilities in China.[37]

PRC IP theft undermines the revenue, talent, future economic growth, and economic competitiveness of core industry players. Over time, and with no meaningful counterresponse, China's industrial policy could subvert the incentive structures that underpin innovation—the engine of economic and military power—including the competitive and financial returns inherent in ingenuity and the laws that protect global markets.

Conclusion: Viewing the Commercial Domain as a 21st-Century Battlespace

If China's digital strategy were to succeed, it would undermine the ability of the United States and its allies and partners to project diplomatic and military power in key regions around the world, as well as reduce companies' ability to operate in those markets. China's digital strategy creates the prospect of a Chinese-led digital bloc that operates telecommunications, financial payments, e-commerce, logistics, internet, and satellite navigation separate from the rest of the world. As former Australian prime minister Malcolm Turnbull articulated, we do not need a "smoking gun" when assessing China's intent; we can see that the country has a loaded gun and do not "want someone with very different values than ours to have the ability to pull the trigger."[38]

Yet China's loaded gun (and its implications) has thus far evaded large-scale recognition, let alone a meaningful and coordinated response. In part, this is a function of China's emphasis on leveraging corporate players and competing in commercial domains. Corporations are the defining instruments of 21st-century strategic competition. They wield significant influence over society and political institutions; retain massive amounts of data globally, including on people; and are the primary incubators of cutting-edge innovations that will define the next era of economic

---

[34] Andrew Rettman, "Universities in EU on Alert to China Spy Threat," EUobserver, April 23, 2020, https://euobserver.com/foreign/148164.

[35] Mary Hui, "Japan Minted a New Economic Security Minister to Fix Supply Chain Disruptions," Quartz, October 8, 2021, https://qz.com/2070498/japan-has-a-new-economic-security-chief-to-secure-supply-chains; and "Japan Starts Paying Firms to Cut Reliance on Chinese Factories," Bloomberg, July 18, 2020, https://www.bloomberg.com/news/articles/2020-07-18/japan-to-pay-at-least-536-million-for-companies-to-leave-china.

[36] Greg Levesque, "What Keeps Xi Up at Night: Beijing's Internal and External Challenges," testimony before the U.S.-China Economic and Security Review Commission, Washington, D.C., February 7, 2019, https://www.uscc.gov/sites/default/files/Levesque_USCC%20Testimony_Final_0.pdf.

[37] Tai Ming Cheung, "Critical Factors in Enabling Defense Innovation: A Systems Perspective," *SITC Research Briefs* 10 (2018), https://escholarship.org/uc/item/170219mp. Cheung notes that the primary types of innovation outcomes in China's defense innovation system "are advanced imitation and incremental innovation, although there are growing signs of higher levels of innovation outcomes and crossover and architectural innovation."

[38] Interview with Malcolm Turnbull at the Halifax International Security Forum, YouTube, November 20, 2021, https://www.youtube.com/watch?v=MRoGkpCdNSU.

and military winners and losers. It makes sense, then, that governments should try to harness the competitive forces of corporate actors to strengthen diplomatic maneuverability and military capability. Yet this constitutes a different approach than that of past nation-state competitions and demands a change in the framework used to assess Beijing's global influence—and the threats it creates.

Economic statecraft is traditionally defined in the West as a suite of policy tools, including sanctions, export restrictions, and investment screening. China pursues a broad, ambitious version of this by using commercial entities to implement its national strategic objectives domestically and abroad. Since 2013, Beijing has expended significant resources to consolidate control over the management and activities of Chinese corporations, turning them into arms of national power.[39] Under Xi Jinping, the PRC government has rolled back market reforms implemented in the early 2000s under then premier Zhu Rongji, directing more than $1 trillion in domestic mergers across strategic industries like railways, chemicals, and shipping. The Chinese Communist Party (CCP) has also consolidated control over the management decisions of both state-owned and ostensibly private corporations like Alibaba.[40] Xi stressed CCP leadership over state-owned enterprises in October 2016, declaring that they "should become important forces to implement decisions of the CCP Central Committee…to enhance overall national power, economic and social development, and people's wellbeing."[41]

China's use of corporate players as tools to achieve its digital ambitions, along with its recasting of the corporate domain as a nation-state battlespace—demonstrated in the Military-Civil Fusion strategy—obscures the threatening nature of the country's digital strategy. As this chapter has demonstrated, these efforts directly contribute to Beijing's strategic ambitions to gain greater control over the global digital domain, and by doing so shift the global balance of power in its favor. Liberal democracies must recognize China's use of the corporate sector in its digital strategy as a threat and counter with their own national security strategies.

As the case study in the **Appendix** that follows highlights, Military-Civil Fusion in the digital era also turns national power projection into a value-redeeming proposition. China's approach demands the development of new tools to respond. Traditional modes and mechanisms of international competition, such as military deployments and actions in institutions of multilateral governance, are insufficient to address Beijing's challenge. Effectively mitigating the risks of China's growing digital influence will be difficult. The concluding chapter of this report attempts to provide a framework for how states concerned about China's growing influence over international digital architecture can begin to collectively address these challenges.

---

[39] Another likely factor driving Beijing's consolidation of commercial actors is the disruptive effect of information technology platforms, which are controlled by corporations. The role of social media platforms during the Arab Spring offers a case in point.

[40] "China's Rulers Want More Control over Big Tech," *Economist*, April 8, 2021, https://www.economist.com/business/2021/04/08/chinas-rulers-want-more-control-of-big-tech.

[41] "Xi Stresses CPC leadership of State-Owned Enterprises," *Global Times*, October 11, 2016, https://www.globaltimes.cn/content/1010778.shtml.

APPENDIX: CASE STUDY OF HOW BEIDOU INFLUENCES THE STRATEGIC, MILITARY, AND ECONOMIC ENVIRONMENTS

On July 31, 2020, CCP general secretary Xi Jinping ascended a podium in front of a bright red digital screen in Beijing's Great Hall of the People to address a group of CCP and People's Liberation Army (PLA) dignitaries. Xi's words were displayed in Chinese and English on the screen behind him as he spoke: "The BeiDou-3 Navigation Satellite System is formally commissioned!"[42]

Covid-19 restrictions left his audience unusually small, but Xi's rhetoric was not dampened. He extolled the commissioning of BeiDou-3 as an event that "fully embodied the political advantages of China's socialist system in concentrating its efforts on major events, [one that is] important for enhancing China's comprehensive national strength and promoting China's economic development and people's livelihood."[43] He praised the project's scientists and technicians for "carrying forward the spirit of 'Two Bombs, One Satellite'"—harkening back to the development of the PRC's first artificial satellite, atomic bomb, and intercontinental ballistic missile (ICBM). State media outlets were equally effusive about the event. One commentary in the *People's Daily* asserted that "the completion and commissioning of the global BeiDou-3 Navigation Satellite System is an important milestone for China to climb the peak of science and technology and become a power in space."[44]

The fanfare was merited. The successful launch of the final satellite in the third phase of the BeiDou constellation (hence BeiDou-3) on June 23, 2020, made China the third individual nation (after the United States and Russia) to put a complete satellite navigation system with global reach into orbit. This case study examines the motivations behind China's initiation of the BeiDou project and its security implications.

Overview of the BeiDou Navigation Satellite System

The third, global phase of the BeiDou constellation consists of 30 satellites launched between November 5, 2017, and June 23, 2020, from the Xichang Satellite Launch Center in China's southwestern Sichuan Province. This phase builds on the 15 existing satellites of the BeiDou-2 constellation, which provides navigation services to the Asia-Pacific. Altogether, BeiDou's combined second and third phases include 8 satellites in geostationary orbit, 27 in medium Earth orbit, and 10 in inclined geosynchronous orbit. Another 5 BeiDou-3 experimental satellites—3 in medium Earth orbit and 2 in inclined geosynchronous orbit—also exist within the constellation, albeit on a different signal system.[45]

BeiDou's satellites and launch vehicles were produced by the China Academy of Launch Vehicle Technology, a subsidiary of the China Aerospace Science and Technology Corporation (CASC)—the PRC's primary state-owned space program contractor. Research and development

---

[42] "习近平出席建成暨开通仪式并宣布北斗三号全球卫星导航系统正式开通 李克强韩正出席仪式" [Xi Jinping Attended the Completion and Opening Ceremony and Announced the Official Opening of the BeiDou-3 Global Satellite Navigation System; Li Keqiang and Han Zheng Attended the Ceremony], Xinhua, July 31, 2020, http://www.xinhuanet.com/politics/2020-07/31/c_1126310703.htm.

[43] Ibid.

[44] "大力弘扬新时代北斗精神" [Vigorously Promote the Spirit of BeiDou in the New Era], *People's Daily*, August 1, 2020, http://opinion.people.com.cn/n1/2020/0801/c1003-31806203.html.

[45] See Test and Assessment Research Center of the China Satellite Navigation Office website, http://www.csno-tarc.cn/system/constellation&ce.

was conducted primarily by the Fifth Academy of CASC, also known as the China Academy of Space Technology. A rich ecosystem of research institutions and commercial enterprises exists to develop and market applications for BeiDou technology, such as a network centered on the BeiDou Aerospace Satellite Technology Application Group, which includes CASC, the China Aerospace Science and Industry Corporation (CASIC), the Institute of Remote Sensing and Digital Earth of the Chinese Academy of Sciences (CAS), the Institute of Computing Technology of CAS, the State Administration for Science, Technology and Industry for National Defense, the Smart City Working Committee, Beihang University, Zhejiang University, Jilin University, and the Hunan Institute of Technology.

BeiDou and China's Global Power

BeiDou is an inherently dual-use system: Chinese state media has identified its navigation services as central to "national defense mobilization," while also noting applications in consumer smartphones, public transportation, and agricultural monitoring.[46] As a result, BeiDou and its security implications have to be considered within the framework of both military and commercial or civilian competition. The system is a core pillar and archetype of China's Military-Civil Fusion strategy.[47]

State media has asserted that "the establishment and development of a fully autonomous navigation satellite system is…a requirement for national security and military modernization."[48] Initially, BeiDou was framed as a defensive effort. As reported by state-run news outlet Xinhua, "if a country relies completely on the United States' GPS system for navigation, positioning, and timing, it means that the prerequisite for that country's economic development and security is the GPS navigation system that provides goods and services for it."[49] One retrospective published in an online newspaper under the state-owned Shanghai United Media Group identifies two critical moments in Beijing's 1994 decision to initiate the BeiDou project: the United States' use of GPS-guided precision munitions during the 1991 Gulf War and the July 1993 *Yinhe* incident, during which a Chinese freighter lost its ability to navigate after the United States temporarily suspended GPS coverage over the Indian Ocean.[50] Other state media outlets have described the BeiDou system as "the fundamental lifeline for the enhancement of weapon effectiveness and the safeguarding of national security."[51]

However, BeiDou's offensive applications are also clear. China's Dong Feng 31-A ICBM is now guided by the BeiDou system—a development that has caused consternation among defense

---

46 "航天科技五院: '中国坐标'闪耀星空" [Fifth Academy of Aerospace Science and Technology: "Chinese Coordinates" Shine in the Stars], Xinhua, July 31, 2020, http://www.xinhuanet.com/politics/2020-08/17/c_1126374691.htm; "北斗+国防动员, 这条路有多远" [BeiDou + National Defense Mobilization, How Far Is the Road], *People's Daily*, April 11, 2017, http://military.people.com.cn/n1/2017/0411/c1011-29201434.html; and State Council Information Office (PRC), "大部分智能手机均支持北斗功能" [Most Smartphones Support BeiDou Function], August 3, 2020, http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/42311/43394/zy43398/Document/1684840/1684840.htm.

47 Greg Levesque, "Military-Civil Fusion: Beijing's 'Guns and Butter' Strategy to Become a Technological Superpower," Jamestown Foundation, October 8, 2019, https://jamestown.org/program/military-civil-fusion-beijings-guns-and-butter-strategy-to-become-a-technological-superpower; and Greg Levesque, "Commercialized Militarization: China's Military-Civil Fusion Strategy," National Bureau of Asian Research, June 30, 2021, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy.

48 "说说导航卫星的那些事儿" [Talk about Those Navigation Satellite Things], Xinhua, April 8, 2015, http://www.xinhuanet.com//mil/2015-04/08/c_127668203.htm.

49 Ibid.

50 Shi Qinghao, "中国为什么要建立北斗卫星导航系统?" [Why Did China Build the BeiDou Satellite Navigation System?], China News Service, October 12, 2020, http://www.chinanews.com/gn/2020/10-12/9310486.shtml.

51 Wu Xuan, "北斗导航战略意义: 是维护国家安全的根本命脉" [The Strategic Significance of BeiDou Navigation: It Is the Fundamental Lifeline of Maintaining National Security], China News Service, November 1, 2012, http://www.chinanews.com/gn/2012/11-01/4295094.shtml.

planners in the United States. This is only one of several ties between the system and the PRC's ballistic missile infrastructure. For example, the Yuan Wang–class tracking ships that are used to track BeiDou satellites and other Chinese spacecraft are also used to track and analyze ICBM launches. These ships report to the PLA Strategic Support Force, which manages the BeiDou system and is responsible for space, electronic, and cyber warfare.

BeiDou is progressing beyond a mere "lifeline" for China's national security to an effective tool in the global expansion of Chinese power. Chinese discussions of BeiDou also underline the extent to which China sees the digital contest as a zero-sum game. The chief designer of the BeiDou-3 constellation has stated that its goal is not to function as one of several global satellite navigation systems but rather to supplant GPS as the number-one navigation system on (and above) the planet.[52] Should China succeed in doing so, it would erode the asymmetric military and foreign policy advantages the United States and its partners currently claim based on GPS's position as the de facto global standard. Just over a year into BeiDou-3's full operability, the PLA has already demonstrated its ability to mask troop movements by restricting the use of BeiDou in conflict zones. That this development coincides with (and has hindered) enhanced surveillance by Indian forces of PLA positions along the Line of Actual Control hints at the increased flexibility an independent global satellite navigation system now offers Chinese military planners.

A Chinese military that is no longer reliant on GPS navigation services would be able to disrupt GPS services with minimal interruption to its own operations. The Russian legislature's passage in July 2019 of a law enshrining cooperation between Russia's GLONASS system and BeiDou caused concern among some U.S. analysts, given the country's history of jamming and spoofing GPS signals over large areas. Greater integration between the two services would free up resources in both countries to coordinate global-scale GPS disruption operations, complicating the United States' and its partners' ability to jointly project military power in a timely fashion. The resulting degradation of deterrence could spell disaster for those parts of the world in which the expectation of rapid U.S. military intervention has long maintained peace and stability, such as the Taiwan Strait. Even without the threat of GPS disruption, deployment of BeiDou has set off alarms in Taipei. In an August 2021 report, Taiwan's Ministry of National Defense warned that the system allows Beijing newfound reconnaissance capabilities, while the PLA's precision-guided weapons can now "paralyze" the island country's defense infrastructure.[53]

The proliferation of BeiDou-enabled military technology likewise affords regional powers aligned with the PRC greater ability to maneuver outside of U.S. constraints. As early as August 2020, Indian media reported that Pakistani authorities intended to adopt BeiDou for both civilian and military purposes, with the country "completely [switching] to the BeiDou navigation system for all its critical military platforms."[54] Pakistan's diminished reliance on GPS means diminished U.S. leverage in the event of a conflict between Pakistan and India. This would decrease military stability in an already volatile South Asia at a time when the United States seeks to deepen its security ties with India to balance against China.

---

52 "中国的北斗卫星导航系统已经改目标了: '要当世界第一'" [China's BeiDou Satellite Navigation System Has Changed Its Goal: "To Be the World's First"], Sina, October 24, 2020, https://finance.sina.com.cn/tech/2020-10-24/doc-iiznctkc7361443.shtml.

53 Liam Gibson, "China Can 'Paralyze' Taiwan's Defenses, Threat Worsening: Ministry of National Defense," *Taiwan News*, September 2, 2021, https://www.taiwannews.com.tw/en/news/4280653.

54 Abhishek Bhalla, "Chinese BeiDou: The New GPS for Pakistan Military," *India Today*, August 21, 2020, https://www.indiatoday.in/world/story/chinese-BeiDou-the-new-gps-for-pakistan-military-1713725-2020-08-21.

This pattern could repeat itself across multiple regions of the world as other countries defect to BeiDou to get out from under GPS hegemony, especially those countries adversarial to U.S. interests. In March 2021 the Iranian government signed a 25-year agreement with China granting Iran's armed forces access to the BeiDou network. Chinese commentators were quick to assert that this agreement would enhance Iran's military position in the Middle East, to the detriment of the United States.[55]

The BeiDou system is also essential to China's ambitions in space. The PRC is eager for recognition as a space power. State newspapers translate and reprint international media praise for the Chinese space program after events like BeiDou's commissioning and the return of the *Shenzhou* 12 manned spaceflight.[56] To this end, the CCP has targeted the aerospace sector in general, and satellite equipment and applications in particular, for "vigorous development" in its marquee technological development plans such as Made in China 2025 and the Strategic Emerging Industries initiative.[57] Xi Jinping himself has linked China's rise as a space power to his overarching goal of bringing about "the great rejuvenation of the Chinese nation," claiming that "the aerospace dream is an important component of [China's] dream of [becoming] a powerful country."[58] An independent global satellite navigation system is for China's leadership a step toward the realization of that dream.

BeiDou and Its Role in Advancing PRC Foreign Policy Initiatives

In addition to China's vision for itself in space, the BeiDou system has quickly become integrated into the country's foreign policy and military ambitions. This is a mutually reinforcing dynamic: China's international engagement and investment serve as avenues through which to expand BeiDou's reach and user base. The system's proliferation locks in Chinese influence globally, paving the way for additional engagement and investment. State media has proclaimed the system as not merely "China's BeiDou" but "the world's BeiDou"—a milestone in the country's "opening up" and newfound international stature.[59] China has identified a host of externally oriented strategies that benefit from BeiDou. This makes the security implications even more acute: the system is folded into, and a core part of, Beijing's major strategies and programming for internationalization. From the point of design, BeiDou is proliferating in lockstep with China's global influence.

For example, BeiDou is a key component of China's Belt and Road Initiative (BRI). BRI is Xi Jinping's flagship foreign policy program and constitutes an immense network of physical and virtual infrastructure integrating the Chinese economy into the continental economies of Africa and Eurasia—and those economies into China's—to be completed by the PRC's centennial in 2049.

---

55 "美国制裁也没用, 伊朗正式启动中国北斗导航, 俄: 中东美军要遭殃" [U.S. Sanctions Are Useless, Iran Officially Launched China's BeiDou Navigation, Russia: The U.S. Military in the Middle East Will Suffer], NetEase, April 25, 2021, https://www.163.com/dy/article/G8EDMOP605159866.html.

56 State Council (PRC), "北斗给全球用户带来巨大福利" [BeiDou Brings Huge Benefits to Global Users], August 10, 2020, http://www.gov.cn/xinwen/2020-08/10/content_5533578.htm; and "外媒看中国: '中国在太空探索领域取得了长足进步'" [Foreign Media Look at China: "China Has Made Great Strides in Space Exploration"], China News Service, September 20, 2021, https://www.chinanews.com/gn/2021/09-20/9570028.shtml.

57 State Council (PRC), "国务院关于印发'中国制造2025'的通知" [Notice of the State Council on Issuing "Made in China 2025"], May 19, 2015, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm; and State-Owned Assets Supervision and Administration Commission of the State Council (PRC), "发展战略性新兴产业" [Develop Strategic Emerging Industries], December 10, 2020, http://www.sasac.gov.cn/n2588025/n2588134/c16190953/content.html.

58 "习近平的 '航天情'" [Xi Jinping's "Aerospace Love"], Xinhua, April 12, 2021, http://www.xinhuanet.com/politics/xxjxs/2021-04/12/c_1127322037.htm.

59 "中国的北斗 世界的北斗" [China's BeiDou the World's BeiDou], Xinhua, August 10, 2020, http://www.xinhuanet.com/2020-08/10/c_1126346487.htm.

The expansion of BeiDou services into countries that have signed on to BRI, and the displacement of GPS in those countries as a result, has been described as a key opportunity for the initiative.[60] By April 2019, more than 800 people from over 40 countries had received BeiDou-related training in China, with the State Council Information Office describing this trend as "BeiDou shining down on the Belt and Road Initiative."[61] By the June 2020 launch of the final BeiDou-3 satellite, PRC state media boasted that "BeiDou has provided services and related products to more than 100 million users in countries and regions along the Belt and Road and exported [those services and products] to more than 120 countries and regions."[62]

Of the countries participating in BRI, Beijing's "space cooperation" efforts have particularly targeted those on the African continent, with the first "overseas BeiDou [applications research] center" being located in Tunisia. Chinese experts have led BeiDou training sessions in Tunisia, Sudan, Egypt, Algeria, and Morocco.[63] In 2015 the CCP pledged to provide satellite television to 10,000 villages across the African continent; by 2020, 8,162 villages in nineteen countries had received this service.[64] Other BeiDou services are rapidly growing in popularity in regional countries such as Ethiopia. According to the state-run *China Daily*, this indicates that "Beijing has made progress in the battle for global data dominance."[65] China also helped develop and launch Ethiopia's first two satellites and provided meteorological satellite data–receiving equipment to Mozambique. In 2021, Beijing cited the "solutions based on the BeiDou system that have already been applied in many African countries" when it announced that it would establish the "China-Africa Digital Innovation Partnership Program…[to] strengthen digital infrastructure, develop a digital economy, carry out digital education, enhance digital inclusion, co-create digital security, and build a cooperative platform [between China and the nations of Africa]."[66]

The growing BeiDou presence in Africa offers a ripe example of Beijing's larger playbook for expanding its influence and control over global physical and digital infrastructure (discussed in chapters 1 and 2) and in setting the technical standards, norms, and preferences (discussed in chapters 3 and 4) that will shape the future of the digital domain. This example also underscores China's ability to lock in information superiority, influence over digital environments, and competitive advantages for state-influenced Chinese companies to pursue Beijing's objectives within the commercial battlespace.

BeiDou as an Economic and Financial Accelerant

BeiDou does not just provide China with competitive military capabilities. The commissioning of the third phase of the satellite system has created enormous economic development and commercial opportunities for the PRC, including opportunities that can in turn be converted

---

60 "北斗系统在'一带一路'中的机遇和挑战" [Opportunities and Challenges of the BeiDou System within the "Belt and Road Initiative"], China Satellite Navigation Conference, February 14, 2017, https://www.beidou.org/newsdetail_413.html.

61 State Council Information Office (PRC), "北斗卫星 闪耀一带一路" [BeiDou Satellites Shine along the Belt and Road], April 8, 2019, http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/39595/40268/xgbd40275/Document/1652292/1652292.htm.

62 "人民日报评论员: 大力弘扬新时代北斗精神" [People's Daily Commentator: Vigorously Promote the Spirit of BeiDou in the New Era], Xinhua, July 31, 2020, http://www.xinhuanet.com/politics/2020-07/31/c_1126311510.htm.

63 "在遥远的突尼斯, 你能很'北斗'" [In Distant Tunisia, You Can Be Very "BeiDou"], BeiDou Satellite Navigation System, April 5, 2019, http://www.beidou.gov.cn/yw/xwzt/dejzabdhzlt/gdxw/201904/t20190408_17760.html.

64 "China Advances Space Cooperation in 2020: Blue Book," Xinhua, March 3, 2021, http://www.xinhuanet.com/english/2021-03/10/c_139799766.htm.

65 "日媒: 在165个国家, 中国北斗令美国GPS相形见绌" [Japanese Media: In 165 Countries, China's BeiDou Eclipses U.S. GPS], *China Daily*, November 26, 2020, https://cn.chinadaily.com.cn/a/202011/26/WS5fbf5ecda3101e7ce9731dd5.html.

66 Ministry of Foreign Affairs (PRC), "中方将与非洲制定实施'中非数字创新伙伴计划'" [China Will Formulate and Implement the "China-Africa Digital Innovation Partnership Program" with Africa], August 24, 2021, https://www.mfa.gov.cn/ce/cebw//chn/zfgx/t1901528.htm.

into military development. Even five years prior to the completion of BeiDou-3, the system had already started generating $31.5 billion in annual revenue for online clients, including Chinese defense industry conglomerates like CASIC and China North Industries Group Corporation, an arms manufacturer.[67] By the end of 2020, sales of BeiDou-compatible chips and other products exceeded 150 million units, with analysts predicting that total sales in 2021 would exceed 436 million units.[68] The China Satellite Navigation Office valued the overall output of China's satellite navigation industry to be over $62.5 billion, with an annual growth rate of 20%. The overall value of BeiDou's services is projected to reach nearly $156 billion by 2025, spurring the creation of a "smart device" industry worth $469 billion by 2035.[69]

This outlook points to a core, and often unrecognized, element of China's Military-Civil Fusion strategy and its interplay with the country's digital strategy. In the past, countries' power projection and security apparatuses have tended to be expensive propositions. Beijing's approach to digital competition has turned its domestic and international power projection into profit-generating propositions for its corporations. The dual-use nature of information technology systems means that they can serve commercial ends while propping up a national security system. And throughout, they collect and transfer data—the new, determinative factor of production.

In short, the completion of China's BeiDou satellite system introduces new security threats for the United States arising from reduced global dependence on GPS—as well as from the options that this reduced dependence creates for adversary states to target GPS systems. BeiDou's completion also marks a significant turning point in Beijing's effort to secure influence over the emerging digital architecture.

---

[67] Gao Yuan, "Sky's the Limit for BeiDou's Clients," *China Daily*, November 16, 2015, http://www.chinadaily.com.cn/bizchina/tech/2015-11/16/content_22464083.htm.

[68] "全面融入生活'+北斗'持续活跃—北斗将如何影响你我?" [Comprehensive Integration into Life "+ BeiDou" Continues to Be Active—How Will BeiDou Affect You and Me?], Xinhua, May 18, 2021, http://www.xinhuanet.com/2021-05/18/c_1127462217.htm.

[69] "我国北斗产业总值到2025年将达万亿元" [The Total Value of China's BeiDou Industry Will Reach One Trillion Yuan by 2025], Xinhua, May 26, 2021, http://www.xinhuanet.com/politics/2021-05/26/c_1127494085.htm.

THE NATIONAL BUREAU *of* ASIAN RESEARCH

NBR SPECIAL REPORT #97 | MARCH 2022

CHAPTER 6

Crafting a Competitive Response: A Framework for Countering China's Digital Ambitions

Matt Turpin

MATT TURPIN is a Visiting Fellow at the Hoover Institution specializing in U.S. policy toward the People's Republic of China, economic statecraft, and technology innovation. Formerly, he was the China director at the U.S. National Security Council. He can be reached at <mturpin@stanford.edu>.

EXECUTIVE SUMMARY

This chapter argues that as the Chinese Communist Party (CCP) makes the world increasingly illiberal through its efforts to control the global digital ecosystem, democracies should work together to establish platforms, systems, and infrastructure that reinforce liberal democratic values.

MAIN ARGUMENT

The People's Republic of China (PRC) and the corporate entities that the CCP increasingly controls are building digital platforms and infrastructure that risk becoming the "operating system" for a new, illiberal international order—and, in the process, cementing the CCP's leadership over the fourth industrial revolution. The characteristics of this operating system reflect the choices and interests of the CCP. To achieve this, the party has launched an ambitious campaign to develop, export, set the rules of, and maintain control over both the physical and digital networks of the fourth industrial revolution. This would enable its creation of a system that makes the world safe for authoritarianism by legitimizing the party's governance model, cementing an advantage for Chinese commercial and military actors, and, more broadly, locking in the party's control over information. This presents a challenge to the incumbent international system and the freedoms, opportunities, and security that it undergirds, while also weakening liberal societies' multilateral leadership over the global system. Countries concerned with the PRC's digital rise must actively compete with Beijing for the architecture of the fourth industrial revolution and construct a positive alternative that privileges liberal democracies while undermining authoritarian regimes.

POLICY IMPLICATIONS

- Democratic policymakers and business leaders must accept that Beijing's alternative system and its challenge to the global architecture are a present reality, not a future condition. Recognizing this truth is the most important step in designing and perpetuating government policies and business models that will succeed in the world as it is rather than what some desire it to be.
- Liberal democracies and like-minded countries need to develop a "common operating picture" to better understand the technological, industrial, and commercial systems that shape the digital ecosystem.
- An effective response to China's digital strategy requires efforts to ensure that the digital ecosystem of the future reinforces democratic values and the rule of law.

The People's Republic of China (PRC) and the corporate entities that the Chinese Communist Party (CCP) increasingly controls are building digital platforms and infrastructure that risk becoming the "operating system" for a new, illiberal international order—and, in the process, cementing Chinese leadership over the fourth industrial revolution. The characteristics of this operating system reflect the choices and interests of the CCP. The party's digital architecture is meant to advantage authoritarian regimes over democratic societies, Chinese companies over their international competitors, and the Chinese narrative over fact and freedom of expression. As a result, the party's digital ambitions challenge the international system that citizens of democracies around the world are accustomed to, as well as the freedoms, opportunities, and security that it undergirds. This happens at a time of global reshuffling, catalyzed by the emergence of data as a factor of production, that raises the stakes and severity of the CCP's challenge.

The first section of this chapter considers the challenge that the PRC's efforts to control the global digital ecosystem poses to the liberal international order. The following section then considers policy options for how democracies can work together to counter China's digital ambitions by establishing digital platforms, systems, and infrastructure that reinforce liberal democratic values.

The PRC's Digital Challenge to the Liberal International Order

The incumbent liberal international system was established following World War II. It is based on the Bretton Woods agreements, which promoted efficient foreign commerce, and global norms articulated in the United Nations Charter that center on individual rights, limited government, self-determination, multilateral institutions to negotiate disputes between states, and collective security to deter conflict. This system privileges democracies over authoritarian regimes and functions as an instrument to compel authoritarian governments to adopt economic and political reforms.

With the end of the Cold War—and the emergence of the third industrial revolution that accompanied it—this liberal international system expanded to become a nearly global system, defined by a newly cemented international architecture. Most countries of the former Soviet bloc sought to adopt the liberal operating system. Simultaneously, the rise of digital infrastructure began with the expansion of computing and communications networks. As countries and their citizens went online, the values and norms of the liberal international system—transparency, rule of law, market economics, separation of powers, limited government, and independent journalism—spread across borders.

For a one-party state like the PRC, this encroachment and expansion of the liberal international order posed an existential threat to the ruling regime. It locked in multilateral leadership on the part of liberal societies over the global system—which the PRC was hard-pressed to challenge within the paradigm of the third industrial revolution. This incumbent international system also threatened authoritarian control, suggesting to Chinese citizens that economic and political liberalization went hand in hand and that "progress" meant adopting the political and societal norms of the liberal international system. The CCP desired the benefits of access and understood that China needed to engage economically and diplomatically with the broader international system. But the party also remembered Chairman Mao Zedong's warnings of the dangers of

"peaceful evolution" to its exclusive hold on power.[1] By the end of the first decade of the 21st century, the CCP had grown increasingly obsessed with the threat of its own downfall, as well as with the pernicious effects of liberal ideology embedded in the international system.[2] The party also became fixated on how the nascent fourth industrial revolution could challenge the incumbent global system and privilege a new set of illiberal norms.

Given these fears and desires, the CCP set out on an audacious path: re-engineer the operating system of the international order into something that advantages Beijing's regime, advances an illiberal worldview, and provides the party greater control of resources, industry, and information. To achieve this, the CCP launched an ambitious campaign to develop, export, and set the rules of—while maintaining control over—both the physical and digital networks of the fourth industrial revolution. From the party's perspective, this strategy to impose its values and interests on the international system through increased influence over the digital domain has two important benefits. First, it insulates the CCP from challenges to its domestic legitimacy by interrupting the spread of "Western constitutional democracy," which in the party's view has a number of distinct characteristics, including "the separation of powers, the multi-party system, general elections, independent judiciaries, [and] nationalized armies."[3] Second, it secures PRC leadership internationally and makes the world safe for authoritarianism by legitimizing its governance model, cementing an advantage for Chinese commercial and military actors, and, more broadly, locking in the party's control over information.

The party's leaders have expressly rejected a digital operating system that favors a liberal international order for one that is deeply illiberal. Beijing is intent on coercing the world to adopt its platforms and infrastructure, and the asymmetries they create, effectively forcing one of two outcomes: surrender to the party's system or to a balkanized digital world. As the previous chapters have made clear, the PRC is positioning itself to advance its national economic, social, and military modernization initiatives by manipulating the rapid changes underway across information technology, telecommunications, and big data.

The PRC has been waging its campaign to control the broader digital ecosystem for over a decade. The CCP is intent on forcing the world to either adopt its platforms and infrastructure or settle for a long-term, drawn-out campaign in which Beijing pressures countries and companies to adopt and perpetuate its model. Perhaps the most important first step for democratic policymakers and business leaders is to accept that Beijing's alternative system and its challenge to the global architecture are a present reality, not a future condition. Recognizing this truth is the most important step in designing and perpetuating government policies and business models that will succeed in the world as it is, rather than what some desire it to be.

Liberal democracies must abandon the fantasy that the CCP can be persuaded in any meaningful way to drop its challenge to the liberal international order and the digital infrastructure beneath it. The days of business and political leaders imagining that convergence and market access are just over the horizon are over. Liberal countries must actively compete with the CCP for the architecture of the fourth industrial revolution by constructing a positive alternative that

---

[1] John S. Van Oudenaren, "Beijing's Peaceful Evolution Paranoia," *Diplomat*, September 1, 2015, https://thediplomat.com/2015/09/beijings-peaceful-evolution-paranoia.

[2] See Tanner Greer, "Xi Jinping in Translation: China's Guiding Ideology," Palladium, May 31, 2019, https://palladiummag.com/2019/05/31/xi-jinping-in-translation-chinas-guiding-ideology; and "Document 9: A ChinaFile Translation," ChinaFile, November 8, 2013, https://www.chinafile.com/document-9-chinafile-translation.

[3] "Document 9: A ChinaFile Translation."

privileges democracies and undermines authoritarian regimes. This does not mean scrapping the existing system and starting from scratch—there are existing norms, standards, and infrastructure that can serve as cornerstones. Rather, this effort will demand employing regulatory tools like export controls, investment security mechanisms, and restrictions on data and capital flows, as well as interventions in the market such as the restoration of industrial and manufacturing bases independent of Beijing and standards organizations not co-opted by the CCP. The question remains: can democratic governments, along with their companies and citizens, build the next generation's digital operating system to protect global norms, prosperity, and security—even as the CCP seeks to undermine them?

There is good reason to believe that policymakers and national leaders are already taking the necessary steps. For example, President Joe Biden emphasized this point in his June 2021 executive order on protecting the data of U.S. citizens from foreign adversaries:

> The Biden Administration is committed to promoting an open, interoperable, reliable, and secure Internet; protecting human rights online and offline; and supporting a vibrant, global digital economy. Certain countries, including the People's Republic of China, do not share these values and seek to leverage digital technologies and Americans' data in ways that present unacceptable national security risks while advancing authoritarian controls and interests.[4]

The goal is to define a global architecture for the digital era that fosters a multipolar community of independent countries, settling disputes through negotiation, transparency, and the rule of law—as opposed to a community of clients in which an illiberal hegemon seeks to safeguard its ruling party and rejects the idea that political legitimacy springs from the consent of the governed. The CCP has concluded that controlling the commanding heights of digital infrastructure and platforms, at a time when the global order is being redefined, provides the tools to achieve its objective of building an illiberal international system.

While recognizing what needs to be done is an important first step, policymakers, business leaders, and citizens must embark on the hard work of translating these aspirational goals into a functioning digital infrastructure that serves the combined interests of stakeholders in a liberal multilateral system. The following recommendations outline a framework for a competitive response—one that begins with understanding the problem at hand, seeks to shore up elements of the existing system that can be defended or reclaimed, and works to build new elements where necessary.

Recommendations

Align data privacy laws. One of the greatest impediments to formulating a common approach among democracies in dealing with the digital challenge posed by the PRC is a lack of common legislation around data privacy. In this area, the United States is a laggard and would benefit from following the European Union's lead. The EU General Data Protection Regulation (GDPR) offers a roadmap for how Washington could standardize the piecemeal collection of state laws into national legislation that would allow citizens the right to take legal action against companies that

[4] "Fact Sheet: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries," White House, Press Release, June 9, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/09/fact-sheet-executive-order-protecting-americans-sensitive-data-from-foreign-adversaries.

release or fail to protect their data. It could also be used to require comprehensive reporting of data breaches beyond the narrow requirements in place today. As the former principal deputy director of national intelligence pointed out in a recent article, U.S. adoption of a GDPR-like law is "the first practical step the [United States] should take."[5]

Develop a "common operating picture" for the technological, industrial, and commercial systems that create and operate digital infrastructure. Before governments can take action, they must understand the challenge and their competitive environments: policymakers require a common operating picture of the technological, industrial, and commercial ecosystems that develop, manufacture, and maintain the digital infrastructure that their economies, militaries, and political systems rely on. Without this kind of detailed knowledge, it is extremely difficult to understand where opportunities and vulnerabilities will arise or how policies will shape the character of these systems.

To assess, defend, and develop their digital infrastructure and platforms, countries need to understand how existing frameworks operate; the innovation, industrial base, and supply chains that support them; and the standards and governance systems that define them. They also need to be able to detect changes that cause vulnerabilities. They need to recognize how the commercial entities operate and what incentivizes certain business models over others, which requires an understanding of both hardware and software development and operation, as well as the commercial dynamics. As the last decade has made abundantly clear, the control and manipulation of these systems can have profound effects and are as important as any physical piece of infrastructure.

For many of us, our relationship with digital infrastructure starts and ends with our smartphone or Wi-Fi router, which leaves us blind to the myriad of hardware, software, and commercial service providers that operate this system behind the scenes. The opaqueness of this infrastructure creates vulnerabilities, whether from a lack of knowledge of the software bill of materials that helped enable Russia's SolarWinds hack, the PRC's nearly decade-long compromise of over a dozen managed-service providers with the APT-10 hack, or the alleged hardware hack by the PRC using Supermicro.[6]

One set of U.S. initiatives that could be emulated is the combination of the 2019 supply chain executive order (EO 13873) and the 2020 creation of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Team Telecom"). These two actions gave the U.S. federal government authority to review the provision of information and communications technology (ICT) equipment and services, as well as to provide national security and law-enforcement expertise to the Federal Communications Commission as it reviews and approves license applications. The ability to perform these two interrelated tasks requires a detailed understanding of the technological and commercial aspects of the ICT industry. This allows the U.S. government to make risk mitigation judgments about current and emerging threats, perceive business and supply chain risks, and shape market choices in ways that privilege democratic values.

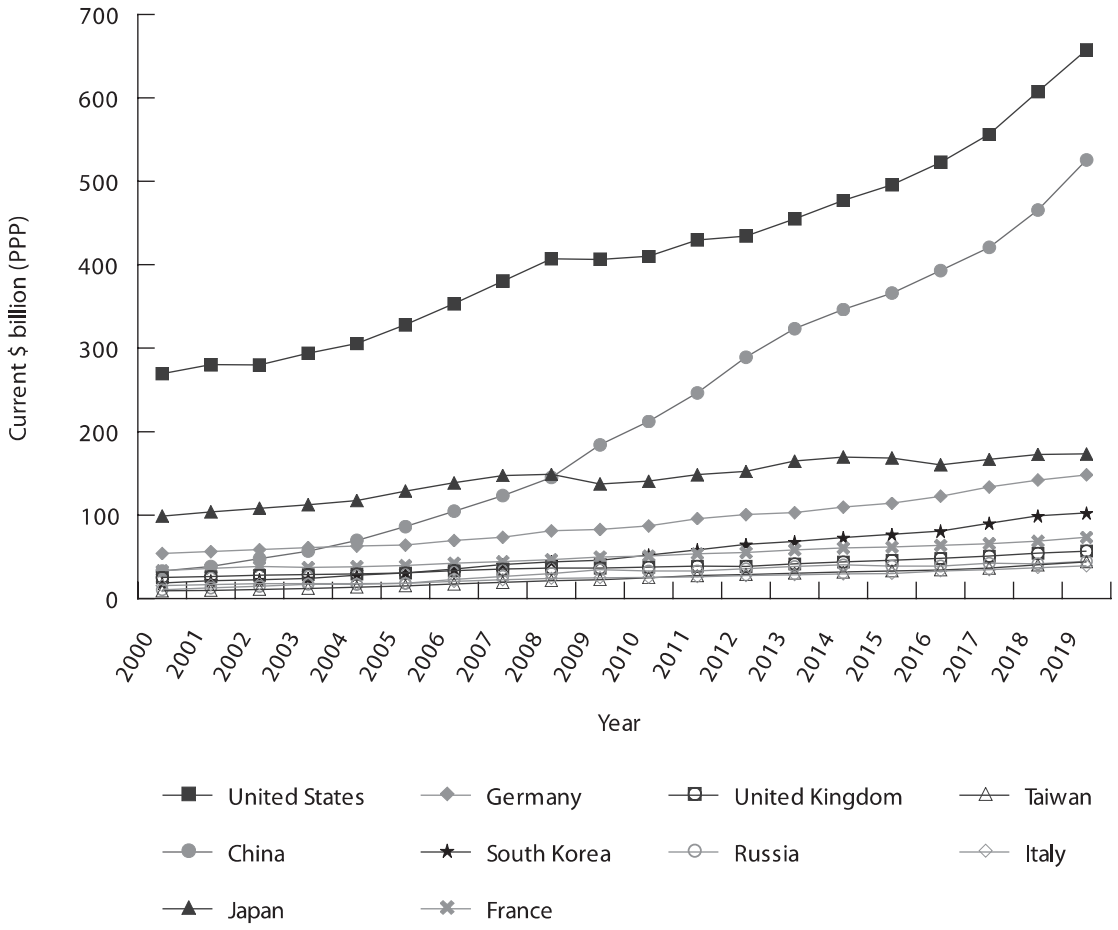
---

[5] Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning," *Foreign Affairs*, December 14, 2021, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

[6] See, for example, Dina Temple-Reston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," National Public Radio, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; Brian Barrett, "How China's Elite Hackers Stole the World's Most Valuable Secrets," *Wired*, December 20, 2018, https://www.wired.com/story/doj-indictment-chinese-hackers-apt10; and Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg Businessweek*, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Commit to higher expenditure levels on research and development. Total global spending on R&D has more than tripled over the past two decades, increasing from $677 billion annually in 2000 to $2.2 trillion by 2019. However, this is almost entirely due to increases by the United States and China. Countries like Japan, Germany, South Korea, France, and the United Kingdom have made only modest increases to their R&D spending over the same period (see **Figure 1**).[7] Other democracies must do more to ensure that open societies dominate breakthroughs in science and technology, as well as bring them to market and allow commercial entities to scale.[8] This entails

FIGURE 1 R&D expenditures of selected countries, 2000–2019



SOURCE: "Main Science and Technology Indicators," Organisation for Economic Co-operation and Development (OECD), https://stats.oecd.org/Index.aspx?DataSetCode=MSTI_PUB.

NOTE: PPP stands for purchasing power parity. PPP is used to determine the relative value of different currencies and adjust data from different countries to a common currency to allow direct comparisons among them.

[7] John F. Sargent Jr., "Global Research and Development Expenditures: Fact Sheet," Congressional Research Service, R44283, September 27, 2021, https://sgp.fas.org/crs/misc/R44283.pdf.

[8] U.S. National Institute of Standards and Technology, "Commerce's NIST Announces Actions to Stimulate Commercialization of Federally Funded R&D," December 6, 2018, https://www.nist.gov/news-events/news/2018/12/commerces-nist-announces-actions-stimulate-commercialization-federally.

not just investing in R&D but also prioritizing applied and experimental research—both areas that the United States and other democracies have traditionally de-emphasized relative to basic research.

One encouraging trend is the establishment of the European Innovation Council, which applies money from the EU budget to invest in technology innovation. This goes beyond grants for basic research to make venture capital–like investments through equity in European start-ups so that they can scale their innovations. The European Innovation Council envisions assisting start-ups through mentorship of founders and aligning private investment.[9] Japan has also made recent progress in this area. In one of his first major policy speeches, Prime Minister Fumio Kishida committed to an R&D fund of approximately $90 billion to "fund research and development in advanced science and technology, including in the areas of digital, green, artificial intelligence (AI), quantum, bio, and space."[10]

Countries must also take reasonable precautions to ensure that the CCP cannot gain unequal access to the fruits of these investments. This means adopting or expanding deemed export rules to control the release of technology and know-how. It would also involve a tightening of what qualifies for a "fundamental research exclusion" at universities and research institutions. For too long the PRC has been permitted access to the rest of the world's R&D ecosystem without granting reciprocal access to its innovation base.

Rebuild electronics manufacturing outside the PRC.[11] Simply making scientific breakthroughs and patenting intellectual property is insufficient. Democracies must also possess the industrial and manufacturing base to bring ideas to market and ensure that they are applied in ways that reinforce, rather than undermine, liberal values—as well as maintain the independence necessary to prevent the PRC from using industry supply chains to develop coercive leverage. This means developing alternative manufacturing and industrial bases that are not dependent on the PRC. The vast majority of global manufacturing for electronics, as well as other digital-relevant industries, takes place on the PRC's east coast. While the United States, Japan, Europe, South Korea, and Taiwan continue to make the most advanced and critical components for electronics, they have largely surrendered the building blocks of these industries and are dependent on the PRC as the principal buyer of advanced components. This creates a vicious cycle in which the CCP plays advanced component manufacturers off of one another, incentivizing and coercing them to turn over technology and know-how in exchange for market access, including through forced technology transfer.[12]

This hyper-concentration of electronics manufacturing within the PRC did not happen through the invisible hand of market forces but through the visible interventions of CCP industrial

---

[9] Margrethe Vestager, "Speech by Executive Vice-President Vestager at the European Innovation Council Summit," European Commission, November 24, 2021, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_6290.

[10] Fumio Kishida, "Policy Speech by Prime Minister Kishida Fumio to the 205th Session of the Diet," Prime Minister of Japan and His Cabinet, October 8, 2021, https://japan.kantei.go.jp/100_kishida/statement/202110/_00005.html.

[11] The rise of electronics manufacturing services (EMS) and contract electronics manufacturing companies in the late 1990s exploded with the PRC's accession to the World Trade Organization. The business model for the EMS industry took advantage of the unique conditions inside the PRC with massive economies of scale, the subsidized procurement of raw materials, the availability of cheap labor with few protections for workers or the environment, and a government that was intent on moving up the value chain of an industry it saw as strategically significant for both economic prosperity and national security. The electronics manufacturing industry serves as the nexus for networking and communications equipment, medical devices, consumer electronics and home appliances, industrial equipment, automotive and maritime equipment, and computers.

[12] Office of the U.S. Trade Representative, "Findings of the Investigation Into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," March 22, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

policies. These policies were designed to localize manufacturing, along with the technological and industrial processes and their associated supply chains, within the PRC.[13] Democracies cannot take advantage of science and technology breakthroughs if they lack the comprehensive manufacturing and industrial base to actualize the advances through new products and services that span the commercial and national security spaces. In fact, it is increasingly difficult to justify to taxpayers within democracies why they should fund R&D in these fields when the benefits of new industries and jobs accrue to an adversary. Achieving this recommendation requires a combination of inducements and impediments for businesses to shift manufacturing away from the PRC.

Establish new standard-setting bodies and block PRC influence. Advocates for an open civil society must employ or create—and fund—new groupings and forums dedicated to developing and proposing new technical and policy standards recommendations that reinforce their values. Participation by the PRC and other authoritarian regimes must be limited to late-stage negotiations. If the PRC decides to adopt alternative standards, it can do so. A 2021 U.S. Interim National Security Guidance document emphasized the need for like-minded countries to work together to achieve this goal: "We will shape emerging technology standards to boost our security, economic competitiveness, and values. And, across these initiatives, we will partner with democratic friends and allies to amplify our collective competitive advantages."[14]

This endeavor should be paired with efforts to defend existing domestic and international standards bodies from China's malign influence. Democracies should terminate bilateral standards cooperation with the CCP and its government-controlled entities. They should also bar domestic standards organizations from including, as members, PRC entities that have been designated as tied to the Chinese military, engaged in human rights abuses, or are under CCP control.[15]

In addition, advocates for an open civil society should push back against overreach from multilateral bodies in which the PRC has established undue influence. For instance, the UN International Telecommunication Union (ITU) is not the appropriate venue for developing or implementing ICT standards. ITU continues to serve an important role in deconflicting radio spectrum and satellite orbits, but its latest efforts to expand into ICT standard setting, AI norms, and facial recognition rules should be resisted.[16] These are functions that are best left to other multilateral institutions, including potentially new organizations that are developed by coalitions of like-minded countries committed to democratic values.

Reconstruct a digital ecosystem that reinforces democratic values and the rule of law. As the first two chapters have pointed out, democracies need to invest in and build a positive counterpart and

---

[13] See Barry Naughton, *The Rise of China's Industrial Policy: 1978 to 2020* (Mexico City: National Autonomous University of Mexico, 2021). Naughton argues that the PRC's distinctive "government-steered market economy" represents a new type of economic system that warrants attention from policymakers given the significant ramifications it has for the global economy. For more on the disruptive effects of PRC industrial policies, see European Chamber of Commerce in China, "China Manufacturing 2025: Putting Industrial Policy Ahead of Market Forces," March 7, 2017, https://www.europeanchamber.com.cn/en/china-manufacturing-2025; and World Trade Organization, "China's Trade-Disruptive Economic Model: Communication From the United States," July 16, 2018, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W745.pdf.

[14] Joseph R. Biden Jr., *Interim National Security Strategic Guidance* (Washington, D.C., March 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[15] The fact that a standard-setting organization, like the O-RAN Alliance that was set up to reduce dependency on Huawei, includes multiple Chinese state-owned enterprises suggests the need to reimagine how democracies cooperate to set standards that reinforce liberal values. According to the O-RAN Alliance website, the following Chinese state-owned or CCP-controlled entities are members or contributors: China Mobile, China Telecom, China Unicom, Beijing University of Posts and Telecommunications, CAICT (the Chinese Academy of Information and Communications Technology), CICT (China Information and Communication Technologies Group Corporation), Nanjing Diange Communication Technology Co. Ltd (Digitgate), Inspur, Wuhan Gewei Electronic Technologies Co. Ltd, State Grid Information and Communication Industry Group Co. Ltd, Suzhou Zhizhu Communication Technology Co. Ltd, Tsinghua University, Tongyu, Communication, and ZTE.

[16] James Kynge and Nian Liu, "From AI to Facial Recognition: How China Is Setting the Rules in New Tech," *Financial Times*, October 7, 2020, https://www.ft.com/content/188d86df-6e82-47eb-a134-2e1e45c777b6.

challenger to the PRC's global digital architecture. Rather than try to persuade the CCP to accept liberal norms and abandon its quest to build a digital ecosystem that reinforces an authoritarian governance model, democracies should set about building an alternative system and exclude the PRC from gaining nonreciprocal access. If democracies fail to create their own ecosystem, countries will be left with no choice but to accept the party's operating system. U.S. national security adviser Jake Sullivan articulated this concept in a July 2021 speech:

> The first wave of the digital revolution promised that new technologies would favor democracy and human rights. The second wave saw an authoritarian counterrevolution. And the question now is whether we can engineer a third wave of the digital revolution—a turn in which we forge a democratic technological ecosystem characterized by resilience, integrity, and openness with trust and security, that reinforces our democratic values and our democratic institutions.[17]

Employ coordinated regulatory and policy tools across democracies to provide advantages to like-minded countries while disadvantaging authoritarian regimes and their corporate entities. Through fits and starts, democracies have begun to coordinate various tools like export controls, investment screening, anti-dumping/countervailing duties, and sanctions (both financial and visa restrictions). This nascent coordination should accelerate and become formalized under a new grouping. This grouping should include the EU, Japan, India, South Korea, Taiwan, the United Kingdom, Israel, Canada, Australia, and the United States—nearly 2.5 billion people. These democracies include the most relevant elements of global technology and digital leadership and should generally pursue a common agenda for the application of regulatory and policy tools. No one nation in this group can dictate the agenda. Reaching a consensus should require compromise on the part of all participants.

Expand digital trade provisions to include more democracies. Among democracies, localization requirements, data barriers, and discriminatory treatment of digital products, platforms, and components should be removed. Both the digital trade chapter within the United States–Mexico–Canada Agreement and the U.S.-Japan Digital Trade Agreement offer a roadmap for expansion. To achieve the scale for an alternative digital ecosystem, democracies must resist the urge to recreate, through protectionism, every portion of the digital infrastructure stack themselves. Using comparative advantage within the community of like-minded nations, while denying access and advantage to the PRC, is a more effective approach. The effort by France in 2019 to impose a digital services tax aimed exclusively at U.S. technology companies and in violation of its own international trade agreement commitments is just one example of the kind of activity that undermines the creation of a digital ecosystem that protects the liberal international order and multilateral institutions.[18] Germany's Digitalization Act, passed in January 2021, also targets large U.S. digital platforms and tech companies and will likely prove equally harmful.[19]

---

[17] Jake Sullivan, "Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit," White House, Press Release, July 13, 2021, https://www.whitehouse.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit.

[18] Office of the U.S. Trade Representative, "Section 301 Investigation: Report on France's Digital Services Tax," December 2, 2019, https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdf.

[19] Michael J. Esser et al., "The New German Digitalization Act: An Overview," Latham and Watkins, January 20, 2021, https://www.lw.com/thoughtLeadership/the-new-german-digitalization-act-an-overview.

Ideally, democracies would formalize frictionless data transfers between like-minded states and impose significant data restrictions on authoritarian regimes and their commercial entities. Continuing to allow Beijing to benefit from a one-way valve of data flows undermines free and open societies.[20] If the PRC continues to construct its own digital ecosystem, then it should not benefit from a digital ecosystem established around liberal values. Japan's Data Free Flow with Trust initiative provides a path to establish a baseline for democracies while excluding those nations that fail to observe standards built to shore up the liberal international order. Other examples include the March 2020 Australia-Singapore Digital Economy Agreement, which sought to remove barriers to digital trade.[21] Countries could also build on the U.S.-led Clean Network initiative, which includes 60 partner nations and seeks to set high standards for telecommunications infrastructure and networks. The concept for this arrangement arose from an international forum of democracies hosted by the Czech Republic in May 2019 to establish criteria for security and trust in telecommunications networks and the associated infrastructure.[22] Like-minded countries must willingly set aside parochial disputes among themselves, adopt "good enough" solutions, and begin implementing an alternative digital ecosystem that reinforces shared interests and values.

There is reason to be optimistic given actions across Europe, Asia, and the Americas over the past few years.[23] For example, the India-Japan memorandum of understanding to enhance cooperation in the field of ICT was signed on January 15, 2021.[24] The agreement focuses cooperation on 5G infrastructure security, submarine cables, and smart cities. It provides a framework for how the world's largest democracy and the third-largest economy can build the next generation digital infrastructure. In September 2021, South Korea initiated the process to join the Digital Economy Partnership Agreement, a plurilateral agreement between Singapore, New Zealand, and Chile intended to strengthen digital trade and establish standards for digital cooperation.[25] Germany's efforts to create a standardization roadmap for AI could help the EU, the United States, and others define principles for AI development that reinforce, rather than undermine, the rights and interests of individuals.[26] The EU GDPR, 2019 Cybersecurity Act, and Digital Services Act all acknowledge the necessity of creating "a safer digital space in which

---

20 U.S. Trade Representative Katherine Tai made this sentiment clear following the G-7 trade ministers meeting in October 2021: "We are concerned with the increasing use of digital trade measures to undermine freedom of speech and expression, as well as government use of surveillance systems that run counter to our shared norms and values, including human rights and a free and open internet. Our commitments on digital trade should contribute to inclusive growth and support innovation and align with a worker-centric, human-centric trade policy, and that the gains from digital trade are equitably distributed." Office of the U.S. Trade Representative, "Statement from Ambassador Katherine Tai on the G7 Trade Ministers Meeting," October 22, 2021, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/statement-ambassador-katherine-tai-g7-trade-ministers-meeting.

21 Department of Foreign Affairs and Trade (Australia), "Australia-Singapore Digital Economy Agreement Fact Sheet," December 8, 2020, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-singapore-digital-economy-agreement-fact-sheet.

22 Government of the Czech Republic, "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World," May 3, 2019, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

23 As a candidate, President Biden stressed the need for democracies to build an alternative digital infrastructure: "As new technologies reshape our economy and society, we must ensure that these engines of progress are bound by laws and ethics, as we have done at previous technological turning points in history, and avoid a race to the bottom, where the rules of the digital age are written by China and Russia. It is time for the United States to lead in forging a technological future that enables democratic societies to thrive and prosperity to be shared broadly." Joseph R. Biden Jr., "Why America Must Lead Again," *Foreign Affairs*, March/April 2020, https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.

24 "India and Japan Sign MoU to Enhance Cooperation in the Field of ICT," Ministry of Communications (India), Press Release, January 15, 2021, https://pib.gov.in/PressReleasePage.aspx?PRID=1688812.

25 "Korea Initiates Process to Join Digital Economic Partnership Agreement (DEPA)," Ministry of Trade, Industry and Energy (South Korea), Press Release, September 13, 2021, https://english.motie.go.kr/en/pc/pressreleases/bbs/bbsView.do?bbs_cd_n=2&bbs_seq_n=870.

26 "German Standardization Roadmap on Artificial Intelligence," DKE German Commission for Electrical, Electronic and Information Technologies of DIN and VDE, November 2020, https://www.din.de/resource/blob/772610/e96c34dd6b12900ea75b460538805349/normungsroadmap-en-data.pdf.

the fundamental rights of all users of digital services are protected."[27] These and many more initiatives by democracies have much in common and share foundational values that could serve as the bedrock for a new digital ecosystem.

Conclusion

The coming decades will require democracies to work together to recreate an international system that privileges their values. As the PRC accelerates its efforts to build an alternative digital system for an illiberal international order and it gains acceptance from other authoritarian regimes, those countries that value rule of law, transparency, individual rights, and free markets will need to act in concert. Democracies will be forced to confront a competitive world in which the PRC and other authoritarian regimes seek to drive wedges in open societies and coerce acceptance of an illiberal order. Resisting those efforts will require leadership from multiple capitals, business leaders, and wider civil society. The sooner those leaders align policies, manufacturing, and R&D toward a common digital infrastructure that excludes the PRC, the more likely democratic nations will be able to protect the interests of their citizens.

[27] European Commission, "The Digital Services Act Package," October 21, 2021, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

NBR THE NATIONAL BUREAU *of* ASIAN RESEARCH

Seattle and Washington, D.C.

1414 NE 42ND STREET, SUITE 300
SEATTLE, WASHINGTON 98105 USA
PHONE 206-632-7370, FAX 206-632-7487

1819 L ST NW, NINTH FLOOR
WASHINGTON, D.C. 20036 USA
PHONE 202-347-9767, FAX 202-347-9766

NBR@NBR.ORG, WWW.NBR.ORG