THE DIGITAL SILK ROAD

THE DIGITAL SILK ROAD

China's Quest to Wire the World and Win the Future

JONATHAN E. HILLMAN

PROFILE BOOKS

First published in Great Britain in 2021 by
Profile Books Ltd
29 Cloth Fair
London
EC1A 7JQ
www.profilebooks.com

First published in the USA in 2021 by HarperCollins Publishers

Designed by Kyle O'Brien

1 3 5 7 9 10 8 6 4 2

Printed and bound in Great Britain by
Clays Ltd, Elcograf S.p.A.

A CIP catalogue record for this book is available from the British Library.

ISBN 978 1 78816 685 0
Export ISBN 978 1 78816 958 5
eISBN 978 1 78283 796 1
Audio ISBN 978 1 78283 931 6

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author's.

Center for Strategic and International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202.887.0200
www.csis.org

For Liz

CONTENTS

INTRODUCTION

This book was born at 195 Broadway, a twenty-nine-story building wrapped with Roman columns in New York City's bustling financial district. Long before my U.S. publisher, HarperCollins, moved in, it was the headquarters of American Telephone and Telegraph, better known as AT&T, and the site of several historic transmissions: the first sustained transatlantic radio communication in 1923, the first transatlantic phone call in 1927, and the first two-way videophone call in 1930. During the Cold War, AT&T adopted the slogan "Communications is the foundation of democracy," and for most of the twentieth century, 195 Broadway stood at the center of an expanding communications empire.

As this century unfolds, communications are racing faster, reaching further, carrying more—and increasingly coming from China. In 2017, Chinese engineers used a special satellite to hold the first intercontinental, quantum-encrypted video conference, a major step toward constructing an unhackable network. In 2018, Huawei and Vodafone demonstrated one of the first 5G wireless calls. The same year, Hengtong Group celebrated foreign sales of 10,000 kilometers of subsea fiber-optic cable, the systems that carry the vast majority of international data. Communications, the Chinese Communist Party (CCP) is proving, does not have a political preference. It is a powerful tool, for liberation or repression, depending on who controls it.

Just three decades ago, China was completely dependent on foreign companies for all these capabilities. Huawei was a middling

reseller. China's most advanced communications satellites were made in the United States. The world's subsea fiber-optic cable providers were exclusively from the United States, Europe, and Japan. Lacking these systems, let alone the ability to produce them, China's first connection to the global internet came through a Sprint satellite network in 1994. Since then, China has leapt from customer to supplier, from copycat to innovator, from network offshoot to operator.

China's rapid rise is overshadowed only by its global ambitions for the next three decades. Chinese leader Xi Jinping has called for his country to dominate advanced technology manufacturing by 2025, to lead standard setting by 2035, and to become a global superpower by 2050. Xi is mobilizing companies to pour resources into developing digital infrastructure at home and sell more of their products overseas through his Belt and Road Initiative. The Digital Silk Road, part of that initiative and the focus of this book, connects China's bid for technological independence at home and its quest to dominate tomorrow's markets.

History cautions that much more than sales figures are at stake. AT&T applied its expertise to help develop nuclear weapons, a missile warning system, and a secret communications network for Air Force One, among other national security projects. "The blessing of the state, implicit or explicit, has been crucial to every twentieth-century information empire," observes Tim Wu, a Columbia Law professor who joined President Biden's National Economic Council, in *The Master Switch*. Now a new information empire is emerging with vast support from the Chinese state. These pages describe its contours and grapple with its consequences.

While I was writing this book, the stakes became even starker as the COVID-19 pandemic paralyzed the physical world. The streets of New York and so many other cities became quiet, and during the darkest of those days, everything seemed dangerously brittle if not already broken: health systems, supply chains, and financial markets. Digital infrastructure, normally out of sight and out of mind, suddenly

felt like the one system that did not fail. It provided a lifeline to family, friends, work, school, food, entertainment, and more. The digital world roared ahead.

Out of necessity, my journey to understand digital infrastructure became even more virtual. Instead of flying to Los Angeles to tour one of the world's busiest internet exchanges, and the gateway for massive data flows to and from Asia, I took an online tour of the facility and then continued onward to Cape Town to visit one of Africa's largest data centers—all while eating lunch from my desk. I enrolled in online courses on surveillance systems offered by China's largest camera manufacturer, gaining access that would have been difficult, if not impossible, in person. I became a beta user of Starlink, Elon Musk's mega-constellation of satellites that aims to deliver broadband to the farthest reaches of the Earth.

These virtual excursions had their limits. I couldn't wander, as I had grown accustomed to doing while visiting Chinese infrastructure projects around the world before the pandemic. I couldn't bump into fellow classmates between lessons and learn about them and why they were taking the course. Even the most high-definition video can't capture the smell of a place or the feel of rain, sun, and wind. Yet the opportunities were still amazing—the information I accessed, the places I saw, the people I met, all safely amid a global pandemic.

But life did not migrate online for everyone, nor in the same way for those privileged to have access. Roughly half of humanity still lacks internet access. In China, nearly a billion people have access, but foreign connections are so restricted that most people are essentially using a separate internet. The pandemic also opened the floodgates for more pervasive and sophisticated forms of surveillance. Chinese surveillance cameras landed everywhere, from the European Parliament to Alabama's public schools, armed with thermal imaging to detect fevers.

With its reach expanding rapidly, China may seem destined to host the headquarters of the next information empire. Huawei's sprawling

European-style campus in Dongguan, an hour outside Shenzhen, already makes AT&T's Roman touches look modest. But the United States still occupies a position of strength. Among its many advantages are world-leading research universities, innovative companies, deep pools of private capital, openness to immigrants, and a global network of partners and allies. The question is whether the United States can rise to the challenge, rebuilding at home while leading a coalition of countries that offers real benefits to the developing world.

After a year of remote work, the very idea of a physical headquarters feels outdated. But this journey has taught me that the digital world is becoming even more heavily dependent upon physical systems. Nearly every device, and every network node, still falls within the physical or legal boundaries of a sovereign state. As more of daily life depends on digital infrastructure, and more physical objects are connected, it is not merely different versions of the internet that are emerging but different worlds. Communications has a foundation, and the competition to control it is underway.

THE DIGITAL SILK ROAD

CHAPTER ONE

THE NETWORK WARS

If history is written by the victors, so are fantasies of the future. Among the most alluring and dangerous of these tales, born in the blinding glow of Cold War victory, was the idea that communications technology would inevitably promote liberty. As former U.S. president Ronald Reagan told a London audience in 1989, "More than armies, more than diplomacy, more than the best intentions of democratic nations, the communications revolution will be the greatest force for the advancement of human freedom the world has ever seen."[1]

Having recently left office, Reagan was triumphant. America was ascendant, its archrival gasping. The Soviet Union led the world in steel, oil, and nuclear weapons production, but Soviet computers were two decades behind their U.S. counterparts. Heavy industry, Soviet leaders were discovering, matters less in the information age. "The biggest of big brothers is increasingly helpless against communications technology," Reagan boasted.

Democracy was on the march in Hungary and Poland, and Reagan even saw it sprouting in China, where authorities had brutally suppressed demonstrations in Beijing and other cities weeks earlier. Nicholas Kristof, then Beijing bureau chief for the *New York Times*, witnessed the violence in Tiananmen Square and later wrote, "The Communist Party signed its own death warrant that night."[2] Foreign correspondents and diplomats debated whether the Party could last weeks, months, or a year.[3]

Even as the CCP defied those expectations, predictions that technology would bring about its demise only became more popular. By 1993, illegal satellite dishes were popping up faster than the government could tear them down. "The information revolution is coming to China, and in the long run it threatens to supplant the Communist revolution," Kristof wrote.[4] Satellites failed to deliver that change, but then came the internet, and bloggers were cast as the new freedom fighters.

Few were as courageous and inspiring as Li Xinde, author of *Chinese Public Opinion Surveillance Net*. Li was investigating reports of government corruption, posting his findings online, and then moving on before local authorities could arrest him. "It's the Chinese leadership itself that is digging the Communist Party's grave, by giving the Chinese people broadband," Kristof wrote in a 2005 profile of Li titled "Death by a Thousand Blogs."[5]

But the fantasy that connectivity favors liberty has long faded. In its place, a much darker reality is unfolding. Democracy is retreating, and digital authoritarianism is on the march.

The CCP is harnessing communications technology to cement its control at home and expand its influence abroad. Like a medieval castle, China's domestic internet has only a handful of entry points, giving Beijing an unrivaled ability to monitor, censor, and cut off network traffic. Surveillance cameras armed with artificial intelligence (AI) have blanketed public spaces, logging faces, automating ethnic profiling, and contributing to the imprisonment of over a million Muslim minorities.

China has become not only the biggest of big brothers but also the world's largest provider of communications technology. Huawei has operations in more than 170 countries, but it is hardly China's only digital giant. Two Chinese companies, Hikvision and Dahua, churn out nearly 40 percent of the world's surveillance cameras. Hengtong Group supplies 15 percent of the world's fiber optics and is one of the world's four suppliers of submarine cables, which carry 95 percent of

international data. China's global navigation satellite system, Beidou, provides more extensive coverage over 165 of the world's capital cities than does America's GPS.[6]

From outer space to the ocean floor, these connections are all part of China's Digital Silk Road, or DSR. Amorphous by design, the DSR sits at the intersection of Chinese leader Xi Jinping's signature policy efforts. It was first mentioned in 2015 as a component of China's Belt and Road Initiative, Xi's vision for moving China closer to the center of everything through infrastructure projects, trade deals, people-to-people ties, and policy coordination. Dangling promises of investment and speaking to the aspirations of the developing world, China has convinced 140 countries to sign onto the Belt and Road.[7]

Like the Belt and Road, the DSR is a China-centric concept wrapped in warm and fuzzy rhetoric about cooperation and mutual benefits. There are no formal criteria for what qualifies as a project, but as Chinese technology companies encounter greater scrutiny abroad, the concept has proved a savvy marketing tool. The "Silk Road" imagery evokes a romanticized version of ancient times: camel caravans on the move, cultures mingling, ideas flowing. In reality, it advances "Made in China 2025," another of Xi's signature initiatives, which aims to capture market shares in high-tech industries that amount to global domination.

Before the DSR was formally unveiled, China's digital reach extended quietly into American communities. Rural carriers in a dozen U.S. states purchased Huawei equipment.[8] China Telecom and China Unicom, the country's two largest state-owned telecommunications companies, won licenses to carry international calls within the United States. Along with China Mobile, they connect with other networks in nearly twenty U.S. cities. Hikvision cameras watch over apartment buildings in New York City, a public school in Minnesota, hotels in Los Angeles, and countless homes.

Having awoken to the dangers of allowing its chief competitor's technology in U.S. networks, Washington has started severing these

connections. The U.S. Congress banned carriers that receive federal funding from purchasing Huawei equipment, and the Commerce Department prohibited U.S. companies from selling components to Huawei. The New York Stock Exchange delisted China Telecom, China Unicom, and China Mobile. The Federal Communications Commission (FCC) is revoking China Telecom and China Unicom's licenses.[9] After struggling to identify Hikvision cameras, the U.S. government has removed them from its facilities. All five companies, and hundreds more Chinese entities, have been sanctioned by the United States for offenses ranging from supporting the Chinese military to committing human rights abuses.[10]

The United States has also been playing defense abroad. The global reach of U.S. sanctions prevents any company, U.S. or foreign, from selling components to Huawei that rely on U.S. intellectual property. Publicly and privately, U.S. officials have lobbied foreign leaders and companies to avoid using Chinese suppliers. The State Department's "Clean Network" Initiative, launched in the Trump administration's final year, aimed to limit Chinese suppliers of 5G equipment, Chinese carriers, Chinese cloud providers, Chinese apps, and Chinese involvement in underseas cables.[11]

Convinced it cannot rely on access to U.S. technology, China is pushing ahead with major investments at home. Xi has called for $1.4 trillion in spending through 2025 on "new infrastructure," which includes 5G systems, smart cities, cloud computing, and other digital projects.[12] In March 2021, China approved its Fourteenth Five-Year Plan, a blueprint for the country's development, which for the first time declared technological self-reliance a "strategic pillar."[13] Xi has also called for China to follow an economic model of "dual circulation," a concept that aims to continue China's exports to foreign markets while reducing its reliance on foreign technology domestically.[14] As China bolsters its capabilities at home, it will have more to offer overseas.

The DSR is already accelerating in the wake of the COVID-19

pandemic. While exposing the risks of physical connectivity, the pandemic also raised the costs of being on the losing side of the digital divide. Better-connected economies were able to handle massive transitions to the virtual world. The roughly half of humanity that remains unconnected to the internet had fewer options. The pandemic's financial shock has left developing countries cash-strapped with even less room to borrow. Compared to the large transport and energy projects that characterized the Belt and Road's early years, digital projects are often cheaper and faster to complete.

With these lines drawn, the stage is set for competition between the United States and China to intensify in third markets. Warnings from U.S. officials about the risks of Chinese communications technology are now echoed in Australia, Japan, South Korea, and large parts of Western Europe. But the United States has been less effective in offering affordable alternatives. China is exploiting that opening by pushing deeper into developing and emerging markets, where affordability trumps security. A world of competing digital ecosystems, each with its own equipment and standards, is taking shape. Practically everyone is caught in the middle.

Despite extolling the importance of networks for years, leading thinkers largely failed to consider the possibility of a world in which the United States is not the dominant hub. China's rise and reach beyond its borders is now eviscerating long-held assumptions about technology and liberty, Western primacy, and the very nature of power. Journalists and academics have been grasping for the right words to describe this contest. Is it a trade war? A new Cold War? The reality is more complex, and the stakes fundamentally higher. The United States and China are fighting for control over the networks of tomorrow.[15]

The Network Wars have begun. This book shows how we arrived at this point, provides a tour of the battlefield, and explains what the United States must do to win.

THE RECKONING

The story of how we arrived here is uncomfortable, which is why there have been few honest accountings. Rather than probe how the United States contributed to China's technological rise, Washington and Silicon Valley mostly prefer to tell stories that minimize their failures. There are many variations, but a common theme is that China cheated its way to the top. This sense of unfairness is easy on the American psyche, letting everyone off the hook, but it raises the risk of repeating past mistakes. Complaining offers no strategic insights for competing.

There was plenty of lying, cheating, and stealing. But as the following chapter recounts, what is even more shocking is the myriad of legal opportunities that China exploited. Chinese officials masterfully dangled the prospect of access to China's market, maximizing concessions as foreign companies willingly undercut each other to hand over their intellectual property and enter into partnerships with Chinese firms. With generous state support, those partners eventually became their competitors. Everything was for sale, including the management practices that transformed Huawei from a disorganized copycat into a global juggernaut.

What made these mistakes possible was not merely foreign greed and Chinese savvy but also a powerful and genuinely held belief in the liberalizing effects of communications technology. The collapse of the Soviet Union appeared to prove that communications technology shifted power from governments to individuals, allowing them to speak freely, organize, and hold officials accountable. Every new type of connection, from the fax machine to the internet to the cell phone, was hyped as offering an express lane for carrying liberty around the world.

Few ideas have been as powerful, persistent, and wrong in recent history. It was powerful because it brought a wide range of political philosophies into alignment with the commercial interests of U.S. companies on the vanguard of developing communications technolo-

gies. Despite a few powerful warnings, such as those offered by scholars Rebecca MacKinnon and Evgeny Morozov, this view persisted because of this alignment of interests and the allure of believing that the United States could do good by doing well around the world, regardless of local context.[16] And it was wrong because it confused means and ends, overlooking how these tools could be used differently.

Among the faithful were not only Reagan and Kristof, a conservative and liberal, but also John Perry Barlow, a libertarian who captured the feeling of America's internet pioneers in what he titled famously "A Declaration of the Independence of Cyberspace." "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind," he began. "On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[17]

Barlow was not merely saying that governments lacked legitimacy in the information age, but writing his ode to internet freedom in 1996, he pointed out that they also lacked the capabilities to rule cyberspace. "You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear," he explained. "Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions."

But Chinese strategists knew better. Where Reagan, Kristof, and Barlow saw the unstoppable march of freedom, Chinese officials saw a struggle for power. Shen Weiguang, one of China's founding fathers of information warfare, explained in a lecture to the Chinese National Defense University in 1988, "Countries with advanced networking technology rely on networks to expand their 'information territory' to many other countries and threaten the latter's 'information sovereignty.'"[18] As the Cold War was ending, the battle for information territory was just beginning.

The CCP took predictions of its death by communications technology all too seriously. "The Western world's information strategy is

composed of a public opinion offensive and ideological infiltration, the cultivation of forces within the socialist countries to act as agents to whip up hostilities, the practice of economic coercion, and the practice of outright subversion and creation of all manner of division," Shen cautioned in 1989.[19] But unlike their Western counterparts, Chinese officials did not view these outcomes as inevitable. They set out to build networks that served their own goals.

The Party began asserting its absolute authority over online activities in 1994, a year before the internet was commercially available to the public.[20] These restrictions grew over the years, and in 2005 the Chinese government released what Reporters Without Borders dubbed the "11 Commandments of the Internet." The list banned information that "endangers national security," "subverts the government," "undermines national unity," "disseminates rumors," or "undermines social stability."[21] The rules were wide-ranging and intentionally vague, giving authorities ample room for interpretation. This was Barlow's declaration turned upside down, a vision of cyberspace with the state at its core.

Having publicly articulated different plans for the internet, Chinese authorities faced the colossal technical challenge of building it and enforcing these edicts. Many observers thought that was impossible. "In the new century, liberty will spread by cell phone and cable modem . . . Imagine how much it could change China," U.S. president Bill Clinton said in 2000 while advocating for China's admission to the World Trade Organization. "Now, there's no question China has been trying to crack down on the Internet. Good luck! That's sort of like trying to nail Jell-O to the wall," he said to laughter and applause.[22]

But foreign companies provided the hammer, trading control over their technology for access to China's domestic market. When Chinese state security services sponsored an expo in Beijing called "Security China 2000," more than 300 foreign companies, including many U.S. companies, rushed to pitch their wares.[23] Publicly, foreign technology

companies cast their offerings as essential for opening Chinese society. Executives proclaimed they were exporting not just goods but also values. But as they fought for a slice of China's market, they were jeopardizing both their profits and principles.

As optimism was peaking, Chinese authorities were busy modifying foreign technology for their own ends. Li's main blog was taken down weeks after Kristof's profile, but they both remained undaunted. "I have more than 50 different sites set up. I regularly maintain about three at a time. If they shut one down, I replace one," Li explained.[24] Kristof still believed that technology was weakening the Communist Party. "This is a cat-and-mouse game . . . But the larger truth is that the mice are winning this game, not the cats," he wrote in 2008.[25]

But at that point, China was moving from copycat to innovator and winning a much bigger game. The global telecom competition had become a war of attrition, and overextended Western companies were retreating from the network hardware business. Chinese firms had graduated from being entirely dependent on foreign companies to eating their market share. The epic collapse of the Canadian telecom giant Nortel, examined in the following chapter, overlapped not coincidentally with Huawei's meteoric rise. Huawei scooped up Nortel's brightest minds and tapped them to develop next-generation wireless networks.

While American leaders were busy singing the praises of connectivity, the United States was not investing enough in actually connecting the world, including rural and lower-income communities at home. Shunning big government and industrial policy, Washington assumed market forces would succeed. But as Western firms raced to roll out high-speed internet, they focused primarily on larger, richer markets, creating digital divides. Connectivity disparities arose between developed and developing countries, between urban and rural areas, and between rich and poor. China turned these fault lines into runways for its tech giants. Now they are cleared for takeoff.