THE TELECOMMUNICATIONS INDUSTRY IN US–CHINA CONTEXT

Evolving toward Near-Complete Bifurcation

National Security Report

Paul Triolo

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

THE TELECOMMUNICATIONS INDUSTRY IN US–CHINA CONTEXT

Evolving toward Near-Complete Bifurcation

Paul Triolo

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

The views in this document reflect the opinions of the author alone and do not represent any institutional position held by APL.

NSAD-R-20-061

Contents

Foreword

This paper is part of the "Measure Twice, Cut Once: Assessing Some China–US Technology Connections" research series sponsored by the Johns Hopkins University Applied Physics Laboratory.

As competition has intensified between the United States and China, actions to disengage their technology establishments from one another have also intensified. The two countries' systems for research and development, production, and sale of cutting-edge technologies have been substantially, though by no means uniformly, commingled. More recently, there have been concerted efforts by both nations' governments to reverse some or all of that commingling. Policymakers' priorities include perceived risks to national security, worry about economic disadvantage from proliferation, and concern about uses of technologies that intentionally or indifferently may harm civil liberties or the environment.

To explore the advisability and potential consequences of decoupling, the Johns Hopkins University Applied Physics Laboratory commissioned papers from experts in specific technology areas. In each of these areas, the authors have explored the feasibility and desirability of increased technological separation and offered their thoughts on a possible path forward. Other papers in this series include:

- *Two Worlds, Two Bioeconomies: The Impacts of Decoupling US–China Trade and Technology Transfer* by Rob Carlson and Rik Wehbring
- *The History and Future of US–China Competition and Cooperation in Space* by Matthew Daniels
- *Symbiosis and Strife: Where Is the Sino–American Relationship Bound? An Introduction to the APL Series "Measure Twice, Cut Once: Assessing Some China–US Technology Connections"* by Richard Danzig and Lorand Laskai
- *An Entwined AI Future: Resistance Is Futile* by Christine Fox
- *Cutting off Our Nose to Spite Our Face: US Policy toward Huawei and China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools* by Douglas B. Fuller
- *Addressing the China Challenge for American Universities* by Rory Truex
- *US–China STEM Talent "Decoupling": Background, Policy, and Impact* by Remco Zwetsloot

Summary

The telecommunications sectors in the United States and China have a long history of interconnection, but both countries are now developing policies with the effect of decoupling technology stacks, supply chains, and markets. Once in motion, these policies will be difficult to reverse, given the political distrust that has engulfed the bilateral relationship and emboldened extreme views on both sides about each other's hegemonic intentions. The costs to both countries' innovation systems and to global value chains built up over decades will be significant. Over the next five years, a full bifurcation may take the industry back to the days of separate and competing national standards, problems with interoperability, and the end of a globalized value chain with all its attendant benefits in terms of cost, innovation, and compatibility. The growing cleavage between the two telecommunication systems will have broad ripple effects across a great number of technological sectors, including an intensifying struggle over the future of the internet.

The challenge for US policymakers over the next decade will be to counter China's early lead in 5G while simultaneously enabling interoperability and a globalized supply chain. This will require perceptive domestic industrial policies, substantial investment, and skillful diplomacy that values and refreshes global multi-stakeholder governance and standards-setting processes. Navigating this complex geopolitical, technical, and economic landscape will be hugely difficult for existing US institutions and will require US officials to reimagine how the United States sets telecommunications policy.

China: From Total Dependence to Large-Scale Dominance

The US and Chinese telecommunications equipment sectors have coevolved over the last quarter century. During this period, the US government and industry view of China's capabilities has shifted—once seen as completely laggard, China is now viewed as an eight-hundred-pound powerhouse bent on global tech domination over the next twenty-five years. This period also saw the demise of a host of major US and North American telecommunications systems integrators—companies like Lucent, Motorola, and Nortel that were once major suppliers to China's telecommunications sector—and the rise of powerful Chinese rivals that have gradually squeezed out all foreign rivals. By early 2020, the level of integration between the two sectors had been largely reduced to involving only semiconductors and software. Broader and deeper deleveraging, even full decoupling, is in the cards in the near term and beyond.

This evolution of China's involvement in global telecommunications can be divided into four periods, with each succession characterized by reduced dependence on foreign companies.

(1) Pre-1990

Total reliance on foreign suppliers for telecommunications equipment: no competition on the carrier side. China's Ministry of Posts and Telecommunications (MPT) has long served as both the regulator and operator of the country's public switched telephone network. In both roles during this period, MPT relied heavily on foreign telecom equipment, limited initially to Siemens, NEC, and Alcatel, but then expanded to include Lucent, Ericsson, and Nortel.[1] The same pattern could be seen in the underlying transport network equipment, which manages data streams and is closer to the physical layer, including fiber optic cables; this equipment was also provided by foreign suppliers.

(2) 1990–2005

The beginnings of bifurcation: China fosters domestic champions on the equipment side. The Chinese government began subsidizing domestic players in earnest. In 1993, Huawei developed its C&C08[2] switch, a product that rapidly gained market share at the expense of foreign brands. Huawei impressed Chinese leader Jiang Zemin, who reportedly agreed with its founder's assertion in 1994 that "switching equipment technology was related to national security, and that a nation that did not have its own switching equipment was like one that lacked its own military."[3]

By 2000, Chinese players, principally Huawei, ZTE, Datang, and Great Dragon, had become serious competitors to the likes of Lucent, Nortel, Siemens, and Alcatel for large stored program control switches, along with transport equipment such as add drop multiplexers using wavelength-division multiplexing (WDM) and then dense WDM, fiber optic cable, and other fixed-line telecommunications equipment.[4] Expansion of carrier competition led to the establishment of China Unicom and the separation of MPT's operational side into a dominant player, China Telecom.

This period saw the launch of mobile telecommunications in China, which would eventually come to dominate the sector. In 1997, Huawei debuted its first wireless products as well as Global System for Mobile communications–based infrastructure and launched major efforts to begin penetrating foreign markets. While the company's foreign sales were

[1] See, e.g., IGI Consulting, *China Telecom 2000*, 130–132; and Yan and Pitt, *Chinese Telecommunications Policy*, 50–55.

[2] See Tian and Chunbo, *Huawei Story*.

[3] Ahrens, *Case Study: Huawei*.

[4] See, e.g., Lei, "China's Optical-Network Evolution."

at first modest, its ability to undercut international prices and offer robust after-sale services helped it win contracts in countries such as Russia, Brazil, and South Africa. By the end of this period, Huawei's foreign contracts exceeded its domestic sales.

It was also during this period that Chinese companies took an increasing role in contributing to the global standards-setting process, after a difficult experience with third-generation (3G) mobile networks. China's approach to the 3G standards process was top-down and a poor fit for the realities of global standards setting. Industry took a backseat and Chinese officials led the way. The International Telecommunication Union (ITU) eventually accepted a Chinese standard, Time Division Synchronous Code Division Multiple Access (TD-SCDMA), handing the Chinese government a victory. However, none of the major carriers wanted to adopt it. In 2009 the Ministry of Industry and Information Technology (MIIT) issued a license to China Mobile, which built out a network based on the standard, but by then the industry was already moving to 4G and China Mobile phased out the older 3G network.

After being largely left out of the standards process for 3G, Huawei, with its large investments in R&D, positioned itself to shape the international standards-setting process.

(3) 2005–2015

The acceleration of bifurcation: Chinese companies expand their influence in mobile communications standards. During this period, Huawei and ZTE rose as global competitors while China saw the rapid, robust growth of mobile telecommunications networks in its domestic market. Huawei and ZTE came to dominate China's new mobile telecommunications sector across the board. Along with the growth of Chinese companies in other key sectors such as fiber optic cable systems infrastructure and data centers, these developments eliminated almost all Western equipment from China's fixed-line networks.

After being largely left out of the standards process for 3G, Huawei, with its large investments in research and development (R&D), positioned itself to shape the international standards-setting process during this period. With backing from Beijing, Huawei actively engaged in 4G standards setting and claimed nearly a quarter of 4G patents.[5] Experience during this period provided Huawei with knowledge about how to play in the global standards and patents arena, and Huawei, along with other Chinese telecom major players such as ZTE and the mobile carriers, determined the shape of 5G standards within the process established by the ITU and the 3rd Generation Partnership Project (3GPP).[6]

Huawei's rise also increased tensions with both international competitors and the US government. In late 2012, the US House Intelligence Committee issued a bipartisan report following a nearly yearlong investigation concluding that both Huawei and ZTE posed a national security threat to the United States, due to their alleged willingness to act on behalf of the Chinese government.[7] In addition,

[5] See AFD China, "Huawei Files 25% of the World's 4G Patents." This claim, made by Huawei, appeared in China IP News.

[6] The standards-setting process has been a long-term global and collaborative effort driven by groups of seasoned technical experts organized and overseen by the 3GPP. 3GPP's five hundred participating organizations develop standards for mobile networks based on performance and interoperability criteria established by the ITU.

[7] Rogers and Ruppersberger, *Investigative Report*. The relationship between Huawei and the Chinese government is a complex issue. There is no publicly available data suggesting that Huawei has engaged in malicious activity as a result of its role in servicing equipment in carrier networks. Huawei officials maintain they would not act against their clients, while US concern centers on the potential for Beijing to order the firm to

allegations about Huawei's business practices, including theft of rivals' intellectual property, also began to surface in the media. In 2014, T-Mobile sued Huawei for stealing technology related to a testing robot.[8] The US government's distrust of Huawei, and to a lesser degree ZTE, grew during this period, setting the stage for a showdown over global telecommunications network development, and Huawei's role in it, in the run-up to the 5G era.

(4) 2015–2020

Bilateral tensions push high levels of bifurcation: Chinese companies become dominant in mobile telecommunications infrastructure and consumer products and begin de-risking supply chains from US technology. Within a decade, Huawei and ZTE went from hardly making a dent in the global telecommunications market to dominating a combined 40–45 percent of the global mobile infrastructure.

No less important, the growing political and technology-based conflict between the United States and China, starting with the 2013 Edward Snowden revelations, pushed Beijing toward developing what it calls "secure and controllable" technology supply chains. At the same time, this period saw the maturation of Beijing's overall 5G deployment strategy, which raised hackles in Washington and brought to a head the conflict over Huawei's role in shaping global telecommunications, further pushing apart the countries' telecommunications industries.

While China's telecom equipment giants grew into global players, the US competitors to Huawei and ZTE virtually disappeared. By 2010, all the major US and North American systems integrators, Lucent,[9] Motorola,[10] and Nortel,[11] along with European players Siemens, Marconi, and Alcatel, had largely abandoned the field. Causes of the demise of the US systems integrators and vendors have been ably summarized by former senior US government official Tom Donahue, among others. Donahue observes a "perfect storm" of regulatory, technology, and economic shifts at the end of the 1990s,[12] including the breakup of the Bell System in 1984, economic downturns in 2001–2002 and 2008–2009, mismanagement at key companies, and failure to invest sufficiently in R&D for next-generation networks.

In late 2018, the US government belatedly awoke to the reality that the 5G era was coming and that the United States lacked companies that could challenge Huawei's dominant role in 5G. Huawei is able to provide end-to-end solutions for an increasing number of carriers in countries that have long been close US allies, including the other members of the Five Eyes (the United Kingdom, Australia, New Zealand, Canada). US concern focused first on Huawei's consumer handset expansion in the United States; during a 2018 congressional hearing, the heads of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, as well as the director of national intelligence, advised US citizens not to

take actions during a crisis or to facilitate access to its clients' data or networks. Huawei's business practices are a separate issue, which is sometimes linked in US officials' discussions about the national security threat they believe that Huawei poses. When White House officials were asked after May 2019 to clarify the justification for placing Huawei on the Entity List, one industry official told the author that he was given "seven completely different reasons."

[8] Tabuchi, "T-Mobile Accuses Huawei."

[9] Lazonick and March, "Rise and Demise of Lucent Technologies."

[10] See, e.g., Anderson, "10 Reasons Why Motorola Failed."

[11] See, e.g., Sturgeon, "Where Nortel Went Wrong." A number of other studies of Nortel's failure also cite a series of cyber intrusions into the firm's network that probably were intended to collect intellectual property and could have contributed to the firm's demise. The intruders were assumed to be Chinese state-backed actors.

[12] For a more detailed treatment of the demise of the US telecommunications systems integrator, see Donahue, "Worst Possible Day."

use products or services from Huawei.[13] Then at a secret July 2018 Five Eyes conclave of intelligence chiefs in Canada, an agreement was reached on a strategy to contain Huawei.[14]

Over the following two years, the United States ratcheted up a diplomatic and information campaign, led in part by the State Department and Secretary of State Michael Pompeo, to paint Huawei as an untrusted player that violated US sanctions, stole intellectual property from rivals, and would carry out both espionage and sabotage at Beijing's command. The effort culminated in the so-called Prague Proposals,[15] drafted at the US-convened Prague 5G Security Conference in May 2019. These laid out the case for including the political and legal structure of a vendor's country of origin in any assessment of the risk of using that vendor. Throughout 2019, European governments and the European Commission debated how to improve supply chain security for 5G in order to meet some of the US demands while preserving flexibility for their domestic carriers. Governments and business sectors remained split on the issue. For example, Germany, eager to avoid Beijing's wrath, has not pursued an outright ban of Huawei or ZTE in their networks.[16]

In late January 2020, Prime Minister Boris Johnson of the United Kingdom, the closest US Five Eyes ally, had decided to allow Huawei into its 5G networks,[17] with the proviso that carriers limit their use of Huawei to 35 percent of equipment in the radio access network (RAN). However, in June the UK government, amid another major debate about China and Huawei and fueled by rising anti-China sentiment around the COVID-19 pandemic and Beijing's actions in Hong Kong along with the new US restrictions on Huawei's supply chain, reversed this decision and set in motion a process that will remove all Huawei gear from the country's networks by 2027.[18] The initial UK decision was long in the making and involved in-depth studies of both supply chain security and the economics of the 5G supply chain. In addition, around the same time, the European Commission released a toolbox for mitigating 5G cybersecurity risks, which included a set of voluntary guidelines that member states in Europe had the discretion to implement.[19]

China has devoted more effort than any other country to preparing the ground for 5G. Beijing's approach to 5G reflects a major industrial policy that has been thoughtfully devised and methodically implemented.

The debate in Europe continued unabated during the first half of 2020. The German government led by Angela Merkel faces increasing pressure from the Bundestag to consider stronger restrictions on Huawei, while the business community and major carriers such as Deutsche Telekom are pushing against harsher measures. As of August 2020, governments in Europe were also becoming increasingly aware that US actions targeting Huawei's supply chains had cast doubt on the firm's ability to continue servicing existing and new contracts.[20]

Meanwhile, in China, the rollout of 5G had been in the works for some time, and Beijing is pushing forward despite the geopolitical winds swirling around its leading 5G companies.

[13] See Salinas, "Six Top US Intelligence Chiefs Caution."

[14] See Taylor and Germano, "Gathering of Spy Chiefs."

[15] See "Expressing the Sense," H.R. 575.

[16] For an excellent perspective on EU views on 5G and national security, see Kleinhans, *5G vs. National Security*.

[17] See Dickson and Cerulus, "Boris Johnson Allows Huawei."

[18] See UK Government, "Huawei to Be Removed."

[19] See European Commission, "Cybersecurity of 5G Networks."

[20] Stubbs and Holton, "UK Tells Telcos to Stockpile Huawei Gear."

China's 5G Strategy: Key Vendors and De-Risking Supply Chains

China has devoted more effort than any other country to preparing the ground for 5G. Beijing's approach to 5G reflects a major industrial policy that has been thoughtfully devised and methodically implemented. Recognizing China's failure in terms of standards setting around 3G and 4G, Beijing began laying the groundwork for the development and deployment of 5G networks in 2013, when MIIT, the National Development and Reform Commission (NDRC), and the Ministry of Science and Technology (MOST) established the IMT-2020 5G Promotion Group, an all-government, all-industry alliance to push 5G. IMT-2020, a term coined by the ITU, refers to the International Mobile Telecommunication system (or 5G), with a target deployment date in 2020. The Promotion Group's effort includes collaborative work with the European Union (EU), Japan, the United States, and South Korea.

Beijing structured the IMT-2020 5G Promotion Group as an all-government, all-industry alliance to capitalize on 5G. The group's membership includes all the top players in the Chinese telecom ecosystem: major research institutes and universities such as the China Academy of Information and Communications Technology and Beijing University of Posts and Telecommunications; the Chinese operators China Mobile, China Telecom, and China Unicom; infrastructure suppliers such as Huawei and ZTE; and mobile device makers such as Oppo, Xiaomi, and Vivo. The broad membership provided a unified platform for Chinese contributions to the 3GPP standards-setting process, ensuring that, this time, Chinese standards were not left out. More important, the Promotion Group provided a venue for planning China's strategy for rapidly deploying stand-alone 5G networks at scale.[21]

When Beijing began developing and implementing its 5G strategy, there were signs that the United States would not welcome the leading Chinese telecommunications vendors into the US market.[22] In January 2018, days after Huawei struck an agreement with AT&T to sell phones in the United States through the carrier, AT&T quickly scrapped the agreement after intense pressure from Congress and the National Security Agency.[23] Citing security concerns, Congress included a provision in the 2019 National Defense Authorization Act (NDAA), Section 889, that banned federal agencies and third parties receiving federal government funding from buying Huawei or ZTE products.[24] In July 2020 the Department of Defense issued detailed rules requiring contractors that sell goods and services to the US government to certify that they do not use products from Huawei or ZTE.[25]

Around this time, the US government began seriously scrutinizing the activities of Chinese telecommunication vendors and leveraging US export controls as part of a long-term process to restrict their access to US technology inputs. After a Reuters story[26] revealed that ZTE had violated the Iran Sanctions Act, the US Commerce Department Bureau of Industry and Security (BIS) placed ZTE and three other entities on the Entity List, requiring US suppliers to get a license to continue shipping key technologies subject to the export administration regulations to the firms, with a presumption of denial.[27] This was an unprecedented use of the Entity List against a large multinational corporation with a complex global supply chain. It signaled that the US government would increasingly target Chinese telecommunications and other technology firms.

[21] For more details, see Triolo and Allison, "Geopolitics of 5G."

[22] For more details, see Triolo, "China's 5G Strategy."

[23] Osawa, "AT&T Deal Collapse."

[24] "Trump Signs Bill," *Telecompaper*.

[25] Department of Defense, "Federal Acquisition Regulation."

[26] Freifeld and Jiang, "China's ZTE Pleads Guilty."

[27] BIS, "Additions to the Entity List."

The ZTE entity listing was part of a budding Washington consensus during the late stages of the Obama administration that China's assertiveness as a technology power posed significant national security threats to the United States. This narrative in Washington was bolstered by several major technology initiatives taken under General Secretary Xi Jinping, which portrayed Beijing's high-tech ambitions in zero-sum terms, including the National IC Investment Fund (2014),[28] the Made in China 2025 initiative (2015),[29] the Belt and Road Initiative (2013), and the National Artificial Intelligence Development Plan (2017).[30]

ZTE was once again allowed to place orders with US suppliers, but the damage had already been done. ZTE's heavy dependence on US suppliers, highlighted by the Entity List episode, sent a clear message.

ZTE, which was using more than two hundred US technology suppliers at the time, responded by sending a team of lawyers to Washington to admit guilt, pay a large fine, and accept a discipline regime for its executives. The firm appeared to be complying with the agreement until April 2018, when the new Trump administration determined that ZTE was out of compliance and slapped the company with a denial order.[31] This meant that no US firms could even apply for a license to continue supplying the firm, and ZTE quickly spiraled into financial trouble. ZTE was unable to purchase key hardware and software updates from US firms, and there were rumors that the networks of its major customers, such as China Mobile, were in danger of facing major operational problems as a result.

After several months of negotiations with Beijing over the denial order, in the context of ongoing trade talks, President Trump agreed to a deal that involved rescinding the denial order.[32] ZTE was once again allowed to place orders with US suppliers, but the damage had already been done. ZTE's heavy dependence on US suppliers, highlighted by the Entity List episode, sent a clear message. China's senior leaders and industrial ministries began working on a new long-term framework to ensure that other major Chinese technology companies could not be held hostage to US technology policies. China's other telecommunications giant, Huawei, redoubled its efforts to reduce dependence on US technology suppliers, and executives from several other companies, including Alibaba's Jack Ma, signaled that their companies would work to reduce dependence on the United States.[33]

As part of this effort, senior party and government officials in China established a leading small group (LSG)[34] focused on decoupling and announced a five-year dependency reduction initiative known as the Secure and Controllable program.[35] Its goal is to purge foreign hardware and software from government and critical infrastructure. The Huawei Entity List action in May 2019 and other events since have pushed Beijing to accelerate this process, which includes a plan that requires the government and critical infrastructure operators to make a set percentage of their purchases from domestic suppliers by 2021.

This program appears to be much broader and well resourced than the so-called De-IOE campaign that came after the 2013 Edward Snowden revelations. The De-IOE campaign primarily targeted

[28] "China Announces Measures," *China Daily*.

[29] Kennedy, "Made in China 2025."

[30] Webster et al., "Full Translation."

[31] Department of Commerce, "Secretary Ross."

[32] BIS, "Order Terminating Denial Order."

[33] Suzuki, "Jack Ma Calls for 'Inclusive Chips.'"

[34] A "leading small group" (direct translation from Chinese) is established at the super ministerial level to coordinate complex problems across agencies, usually for a temporary period to solve a particular problem.

[35] Informal discussions via email with industry observers.

Intel, Oracle, and EMC, aiming to replace them with homegrown and expanding technology players including Inspur, Huawei, and Alibaba. The goal of the current program is to build up a large group of domestic secure and controllable suppliers, initially for government and military customers and eventually for key critical infrastructure sectors, including telecommunications.[36] It includes initiatives from 2019 such as a mandate that each province must calculate the number of foreign computers in government ministries and set a timeline for replacing them. The Secure and Controllable program also includes orders to state-owned telecom carriers to "de-risk" their component supply chains by trying to reduce dependence on equipment using US semiconductors.

Chinese leaders have accelerated the program each time a major telecom-related event has occurred in the bilateral relationship. Notable reactions occurred, for example, after the arrest of Huawei chief financial officer Meng Wanzhou; the Huawei Entity List action and subsequent rules targeting HiSilicon, Huawei's key subsidiary and semiconductor design arm; and the breakdown of trade talks in May 2019. In addition, the Central Economic Work Group has a task force on decoupling and apparently a number of subgroups that are probably targeted at particular tech sectors. The decoupling debate is in high gear and covers both state-owned enterprises—specifically those under the State-owned Assets Supervision and Administration Commission (SASAC), including all the major telecommunications carriers and other key sectors such as aviation and energy—and private sector tech leaders.

Clearly this is a long-term project. Initiatives such as the 3-5-2 targets (percentages of procurement tenders—30, 50, 20 percent—going to Chinese companies in 2019–2020 and 2021) will be challenging to meet and are aspirational. The process will not be easy, particularly for areas such as enterprise software and semiconductor design automation tools.[37] But Chinese central organizations such as the NDRC, MIIT, SASAC, and the Ministry of Finance have been collecting data for years on the dependence of Chinese companies and are now really pushing forward action under increased pressure from the top. The United States' willingness to use tools such as the Entity List against virtually all of China's technology leaders—including ZTE, Huawei, Sugon, and in October 2019 eight leading Chinese artificial intelligence (AI)/computer vision companies—has had an undeniable intensifying effect.

In the midst of the coronavirus pandemic of early 2020, Beijing ordered 5G infrastructure vendors and telecommunications carriers to continue their aggressive plans to roll out high-speed mobile networks across the country, despite coronavirus-related disruptions to technology supply chains both within China and in surrounding countries.[38] "New" infrastructure such as 5G networks had become a pillar for Chinese stimulus as the country slowly recovered from the pandemic and associated economic shutdown.

The Chinese government has several levers it can pull to keep 5G deployments on track. The carriers leading the country's 5G build-out are state backed, as is China Tower, a key infrastructure firm providing base station and fiber back backhaul support. These companies' decisions about when and where to build will be directly guided by government priorities. Much of these infrastructure build-outs are free from heavy dependence on US technology, relying on China's robust fiber optic and fiber optical components industry. A public–private partnership with industry has also provided channels for clearly signaling government intent. The major infrastructure vendors, Huawei and

[36] Informal discussions via email with industry observers.

[37] Fuller and Triolo, "Ripple Effects"; and Fuller, *US Policy toward Huawei and China*.

[38] Triolo, Creemers, and Lee, "Beijing Authorities Push Rapid 5G Deployments."

ZTE, had been ramping up output to meet domestic demand for some time—providing a buffer against virus-related disruptions.

Accommodative credit policy for 5G-related firms and fiscal policy to support network construction will further shore up demand. China's first non-stand-alone 5G networks went live in November 2019, ahead of schedule. Major carriers China Unicom and China Telecom appeared to be on track to complete a substantial portion of the initial build-out by the end of September 2020 despite virus-related disruptions. The companies claimed in February 2020 that sixty-four thousand of a planned one hundred thousand 5G base stations due by the end of the first half of 2020 were already in place—extending coverage across most of the mainland's biggest cities and provincial capitals. China's largest carrier, China Mobile, aims to install another three hundred thousand 5G base stations by the end of 2020. Widespread deployments of stand-alone 5G (integral to several priority areas highlighted in China's Made in China 2025 industrial upgrade strategy) are also scheduled to ramp up quickly toward the end of 2020, but the process is likely to extend into 2021–2022, following a separate tender by the major carriers for industrial 5G infrastructure.

China Tower has continued installing base station and fiber optic infrastructure during the crisis. Barring a major new flare-up of virus cases that prolongs disruptions to supply chains, widespread coverage of Chinese cities via non-stand-alone networks will be completed by the fall of 2020.

Finally, in May 2020 Beijing rolled out a stimulus plan around "new infrastructure," focused heavily on 5G, AI, Internet of Things (IoT), and mobile edge computing. The term had first been mentioned at a Politburo Standing Committee meeting in March.[39] The NDRC also put its weight behind the plan just before the May National People's Congress, signaling top-level support and the priority Beijing will accord to telecommunications infrastructure in the wake of the pandemic.[40] While Chinese carriers had already deployed substantial 5G infrastructure as of the May National People's Congress, central authorities were eager to continue the momentum of the 5G rollout, pushing it deeper into China's second- and third-tier cities and countryside and into more state-owned enterprises and factory campuses.

A race was on: Huawei began a crash effort to design out US technology, particularly from its 5G base stations, while US companies continued to supply some key components, and China hawks searched for ways to plug what they viewed as loopholes in the export administration regulations.

The new infrastructure initiative is designed to accelerate the deployment of full stand-alone 5G networks—specifically the low-latency and IoT portions, focused more at the local level in Chinese provinces that are not well developed but are eager for digital transformation that will be enabled by 5G. Data centers that facilitate mobile edge computing—basically pushing some of the cloud-based capabilities that will be required to drive smart factories and cities out to the edge of networks—are also a big part of the new infrastructure push. Chinese officials also characterize the new infrastructure push as focused on the industrial internet and the industrial IoT, all part of a longer-term strategy to upgrade China's industrial base for the digital age.[41]

[39] See Li, "New Infrastructure."

[40] NDRC, "Press Conference on Macroeconomic Operations."

[41] Triolo and Sherlock, "'New Infrastructure.'"

Not Made in the United States 2025: Links Persist but Changes Are Rapid

As 2020 progressed, the downturn in US–China relations brought on by the pandemic provided an opportunity for China hawks in the United States to push a new Huawei-targeting agenda that involves cutting the company from its source of semiconductors. This approach, which has been under discussion since the summer of 2019, is likely to have huge ramifications for the relationship between the two countries' telecommunications supply chains.

Following the May and August 2019 Commerce Department actions[42] placing Huawei and a substantial number of subsidiaries on the Entity List,[43] US technology companies quickly determined that they could comply with provisions of the export administration regulations and still supply Huawei from overseas "non-US origin" locations. This rankled many in the administration eager to cripple Huawei's ability to continue as a leading supplier to China's 5G carriers. A race was on: Huawei began a crash effort to design out US technology, particularly from its 5G base stations, while US companies continued to supply some key components, and China hawks searched for ways to plug what they viewed as loopholes in the export administration regulations.

In January 2020, officials at the Commerce Department, led by then policy planning official Earl Comstock, pushed several new rules aimed at shutting off US technology flows to Huawei. Critically, they targeted the biggest single vulnerability in Huawei's supply chain: the dependence of Huawei's chip subsidiary HiSilicon on one firm for manufacturing semiconductors at cost and quality—Taiwan Semiconductor Corporation (TSMC). Semiconductor industry officials and trade groups mounted a concerted campaign to delay or water down these rules, arguing that they would force further "designing out" of US technology across China's telecommunications sector and beyond, cutting deeply into the revenue of leading US semiconductor companies like Qualcomm, Micron, and Intel, with subsequent effects reducing those firms' R&D budgets. The results, they argued, threatened the United States' global leadership of the semiconductor industry.

These arguments briefly found supporters at the Pentagon in the form of procurement and R&D officials, but a China hawk, former Undersecretary for Policy John Rood, overruled Department of Defense objections to the rules. For his part, President Trump appeared to briefly accept the industry arguments, evidenced by a February 2020 tweet that suggested he did not want to take steps to reduce US companies' ability to do business in China.[44] But as the spread of the coronavirus pandemic accelerated through March and April, President Trump's views on China took a decidedly negative turn. At a principals meeting in April 2020, the president approved a rule that was a turning point in the relationship between US and Chinese technology and telecommunications sectors. There may be no going back.

The HiSilicon Foreign Direct Product Rule

The rule narrowly targets HiSilicon and its affiliates. It requires third-party manufacturers of semiconductors destined for the designated company to apply for licenses—with the presumption of denial. The implication of this rule is to extraterritorially extend US export controls targeting Huawei, undercutting TSMC's ability to produce cutting-edge semiconductors for the company. In anticipation of this move, Huawei began stockpiling

[42] BIS, "Addition of Entities."

[43] BIS, "Addition of Certain Entities."

[44] Rappeport, "Trump Contradicts Advisers."

components and other semiconductors from its Taiwanese suppliers. However, with core chips for its 5G base stations and enterprise, cloud, and AI products relying on TSMC fabrication, ramping up production was not possible beyond small increments, leaving the company with a looming shortage. The only solution for Huawei will be to redesign everything it produces.[45] By June 2020, TSMC had indicated it would abide by the spirit of the law and halt work with Huawei on new semiconductor production. A senior Taiwanese government official indicated that although TSMC was no longer taking orders from Huawei, other clients had quickly taken up the freed capacity.[46]

ZTE may turn out to be one of the final remaining pieces of China's telecommunications sector that maintains close ties to US technology supply chains into the near to medium term.

As of May 2020, Huawei had moved some of its production of semiconductors to a domestic foundry, Semiconductor Manufacturing International Corporation (SMIC). However, SMIC lacks the capacity and equipment to produce advanced designs commercially below the seven-nanometer level and probably will not be able to get there in the near term. This is because last year US government officials reportedly pressured the Dutch government to cancel an SMIC license to purchase cutting-edge extreme ultraviolet lithography equipment from the world's only supplier, the Dutch firm ASML.[47] Without this technology, SMIC and Huawei/HiSilicon are stuck basically at the fourteen- to ten-nanometer node for producing advanced semiconductors. This will eventually render Huawei unable to compete with rivals Ericsson and Nokia and its domestic competitor, ZTE.[48]

Ironically, Huawei's rival, ZTE, a major supplier to China Unicom and China Telecom, continues to have full access to US technology and has gotten high marks for compliance with the 2018 agreement it signed with the Commerce Department to terminate the denial order against it. ZTE's ability to ramp up production to replace some Huawei 5G infrastructure deployments remains uncertain, as does its ability to maintain access to US technology over the long term. There was some speculation in Chinese social media about collaboration between Huawei and ZTE on 5G development and other areas such as semiconductor design in the wake of US actions against Huawei, but it appears unlikely that the two will seek to join forces, given ZTE's desire to maintain its good standing with US officials monitoring the agreement that removed the firm from the Entity List. ZTE may turn out to be one of the final remaining pieces of China's telecommunications sector that maintains close ties to US technology supply chains into the near to medium term.

With 5G deployments moving slowly in other markets, China's push for nationwide broadband 5G coverage and full stand-alone 5G deployments in late 2020 and throughout 2021 will help drive demand for a range of components for consumer and infrastructure devices. It will also drive demand for 5G smartphones, mobile applications, and other innovation on top of the country's 5G networks. On the procurement side, foreign firms

[45] BIS, "Export Administration Regulations: Amendments."

[46] See Blanchard, "Taiwan Minister Says TSMC Has Offset Lost Huawei Orders."

[47] Alper, Sterling, and Nellis, "Trump Administration Pressed Dutch Hard."

[48] SMIC's current high-end deep ultraviolet lithography equipment can theoretically be used for some layers down to seven nanometers using multiple patterning, but beyond that not it is not feasible to use commercially as the yield is far too low to achieve high volume and requires a move to extreme ultraviolet. (The author thanks Jimmy Goodrich for this observation.)

were granted a very small percentage of first-round 5G contracts involving first-tier cities. This is likely to continue in subsequent rounds for networks at the provincial level. The lion's share went to Huawei, with ZTE in second place. However, as of early May 2020, the new US export control restrictions targeting HiSilicon have thrown a major wrench into all of Beijing's 5G rollout plans, particularly for the full stand-alone network build-out slated to accelerate in early 2021.

US 5G Looks for a Way Forward

The lack of coherence in the US government's 5G strategy in the face of China's all-of-government approach and concern over Huawei is the result of a complex set of factors, including the absence of a US systems integrator, a general lack of diversity in the vendor space, and growing concern about the security of 5G networks globally dominated by Chinese companies.[49] Clarity is, however, emerging, and this clarity is intensifying separation of the telecommunications sector with China, particularly at the systems integrator level.

Former White House 5G czar Robert Blair, who was only in the role for several months, stressed during his short tenure that the administration has developed a three-pronged strategy for US 5G development: (1) maintain necessary 5G equipment manufacturing capabilities in the near term with existing trusted vendors; (2) provide a vision for a rapid innovation ecosystem with a combination of small companies, cloud computing companies, and traditional telecommunications companies; (3) partner over the next decade with European, Japanese, and South Korean government entities and companies to develop a standards process and vendor ecosystem almost totally independent of Chinese companies' influence.

Before any of this could happen, however, the Trump administration first needed to accelerate an important piece of unfinished business that highlights the rush to decouple the two countries' telecom sectors: getting rural US carriers to remove all or most existing Chinese telecommunications gear in their networks. While major carriers basically swore off using Chinese vendor gear following the 2012 House Intelligence Committee report, some 25 percent of the equipment used by members of the US Rural Wireless Carriers Association at the start of 2020 was from the two main Chinese vendors. For the most part, these rural carriers preferred Chinese gear because of its low cost and what they considered high levels of service and performance from the vendors.

Citing national security concerns, the Federal Communications Commission (FCC), in a landmark November 2019 decision, ruled that carriers could not use subsidies from the $8.5 billion Universal Service Fund to purchase equipment from either Huawei or ZTE.[50] The decision is sure to hasten rural carriers' moves away from Huawei and ZTE, since rural carriers need Universal Service Fund subsidies to buy new equipment. The FCC is also considering a plan to fund the removal and replacement of Huawei and ZTE equipment from US rural carrier networks, a process will likely be protracted and costly. Estimates of the replacement costs range from $1 to $4 billion.

The Trump administration is contemplating a much broader push to remove Chinese equipment from US infrastructure. As of March 2020, the US Commerce Department and other government entities have been weighing industry comments and considering how best to execute a new rule published in late 2019[51] intended to implement President Trump's 2019 executive order on

[49] For a full treatment of the US 5G strategy dilemma, see Donahue, "Worst Possible Day."

[50] FCC, "Protecting against National Security Threats to the Communications Supply Chain through FCC Programs; Huawei Designation; ZTE Designation."

[51] Department of Commerce, "Securing."

information and communications technology (ICT) supply chain security.[52] The rule's initial purpose was to provide a legal basis for the government to enact a ban on the use of Chinese telecom equipment in US rural wireless network upgrades. However, the rule could be applied more broadly, allowing the administration to force US suppliers to eliminate almost all Chinese components from their supply chain.

The broader US 5G strategy has developed in fits and starts through a complex series of channels between the administration, industry, and Congress.

Delays in this rulemaking highlighted the underlying challenges in implementing the executive order. US industry associations intensified their pushback against the proposed rule when they provided a number of suggested adjustments before the rule was scheduled to take effect. Industry was especially concerned about narrowing the rule's broad language and the scope of the Chinese tech firms to which it could apply. Whereas Huawei and ZTE are clearly the short-term targets, language in the rule would enable the Commerce Department to restrict the use of a broad range of technology from virtually any adversary nation.

Although the Commerce Department emphasized that the changes would be "minimally invasive" and executed with "surgical precision," business groups expressed concern about how far back in the supply chain companies would be obligated to record contributions to hardware and software development. Debate over implementation of the rule percolated through government agencies until May when the pandemic disrupted the operation of the federal government.

Further, the coronavirus outbreak disrupted a number of important meetings set for early 2020 that would have focused on fleshing out the overall 5G strategy of the United States. These included an FCC Forum on 5G Virtualized Radio Access Networks (often referred to as open RANs, or O-RANs) that was scheduled for mid-March[53] and a White House 5G summit organized by National Economic Council Director Larry Kudlow, a major O-RAN proponent.

The latter summit, which was scheduled for early April but was postponed, was set to include both mobile carriers and tech company suppliers to 5G systems, such as Qualcomm. It was also intended to address issues raised by Attorney General William Barr in February 2020 about how to consider shoring up European 5G equipment vendors via US government support or private equity investment. As of September 2020, it is not clear what outcome US policymakers will favor.

The broader US 5G strategy has developed in fits and starts through a complex series of channels between the administration, industry, and Congress. Although there has been some progress,[54] industry and Congress are increasingly concerned that the administration lacks a clear plan.

The Secure 5G and Beyond Act of 2020,[55] signed into law in March, called for wide-ranging consultations with the FCC, Commerce Department,

[52] See White House, "Executive Order on Securing Supply Chain." The costs to the innovation systems of both countries, and to broader global value chains built up over decades, will be significant, as over the next five years a more full bifurcation takes the industry back to the days of separate and competing national standards, problems with interoperability, and the end of a globalized value chain with all its attendant benefits in terms of cost, innovation, and compatibility.

[53] See FCC, "Forum."

[54] Pai, "Save the Date." In February 2020 the FCC voted along party lines to set new rules to make up to 280 megahertz of so-called C-band spectrum between 3.7 and 4.2 gigahertz available for use in next-generation 5G networks. An auction is set for December 2020.

[55] Secure 5G and Beyond Act of 2020.

and other key players to develop a strategy within 180 days of the bill's passage. Under the new law, the president and the National Telecommunications and Information Administration have joint responsibility for implementing the strategy. As of September 2020, the US telecommunications industry is divided over how fast to move toward virtualized networks, and interoperability standards remain under development. Large integrated players, such as Nokia and Ericsson, concerned about loss of market share, are opposed to moving quickly toward O-RAN deployments, while smaller US players such as Mavenir and Altiostar have built their businesses around virtualized networks and are pushing the FCC to do more to promote this approach. Integrated vendors are also using some open interfaces but believe that the current demand from carriers for high-performance, high-throughput 5G networks using proprietary semiconductors indicates where the market is and that broader O-RAN deployments are not possible for another two to three years.

Other important initiatives around virtualization are under development, including an enhanced Common Public Radio Interface (eCPRI). This interface is intended to govern communications between remote radio units and centralized baseband units. At present, this is a proprietary function that locks carriers into a single vendor—a significant hurdle for US rural operators and other carriers that are under pressure from the United States and other governments to migrate away from Huawei and ZTE for 5G networks. Work was underway by carriers and some vendors to ensure that eCPRI is both O-RAN and 3GPP compliant.[56]

Resolving these issues will be difficult and will require that regulators and industry groups come to a consensus on how the administration integrates these approaches into a broader 5G strategy. The White House 5G summit will be held once the pandemic is under control, but the issue of US government support for O-RAN is not likely to be resolved then.

Several other initiatives, described below, are helping to drive US 5G strategy development as of August 2020.

The 5G Clean Network Initiative

The new initiative laid out in early May by the State Department's 5G lead, Undersecretary Keith Krach, requires telecommunications carriers to ensure that US government users of 5G services are assured that their communications, and sensitive data passed between embassies, do not traverse the equipment of any untrustworthy vendor in the network, specifically the major Chinese vendors Huawei and ZTE—this was originally branded as Clean Path. The move appears to be designed to increase pressure on European governments to ban the Chinese vendors from 5G network rollouts. In August 2020 the State Department expanded the "clean" concept to include carriers, apps, app stores, cloud services, and fiber optic cable systems.[57] Authorities for implementing the clean policy remain unclear but will likely include the interim final rule for the May 2019 ICT supply chain executive order. This order was referenced in August when President Trump issued two new executive orders banning Chinese social media apps TikTok and WeChat from operating in the United States.[58]

Supply Chain Security for Advanced Communications Equipment

US officials are promoting this broader and less-defined pillar of the US 5G strategy as part of both the anti-Huawei campaign and more broadly as part of the evolving US industrial strategy around 5G. The new Commerce Department rule

[56] Hardesty, "What Is eCPRI?"

[57] See Department of State, "Clean Network."

[58] See, e.g., White House, "Executive Order on TikTok."

in mid-May targeting Huawei's chip design arm falls into this bucket. Krach linked TSMC's decision to site an advanced manufacturing facility in Arizona with the Commerce decision and the original Clean Path initiative as part of a "5G national security and global economic security trifecta." US officials also linked the decision to not extend the temporary general license for US suppliers of Huawei beyond August 2020 to the evolving US supply chain security strategy.

Development of US and Chinese Industrial Policies

At some point in the latter half of 2020, the United States will roll out a broader strategy targeting both Huawei and broader Chinese technology policies, putting the US 5G initiative under a broader US industrial policy umbrella. Critical in that regard will be the Global Economic Security Strategy (GESS), which is intended to flesh out the economic security pillar of the 2017 National Security Strategy[59] by developing a domestic industrial policy while also offering an alternative to China's Belt and Road Initiative and related strategies.

Broadly speaking, the GESS is intended to promote a US technology and industrial policy that can achieve traction with key US allies and partners while providing a counterweight to Chinese policies. The GESS is intended to be a holistic interagency strategy that includes bilateral and multilateral partnerships with other governments. But much of the GESS is a rebranding of existing US initiatives, and the strategy does not appear to include a fleshed-out plan for developing a commercial rival to Huawei for developing a global 5G network.[60]

Beijing for its part plans to roll out an ambitious new funding program for "new infrastructure,"

In April 2020 a little-noticed executive order restructured US government efforts to track and approve foreign telecom carriers applying for licenses to operate within the United States. The primary target is China.

which includes stand-alone 5G networks and mobile edge computing, to Chinese factories and state-owned enterprises. The plan, which includes nearly US $4 trillion over five years, was rolled out at the May National People's Congress. It is designed to put China's telecommunications sector development into overdrive but will depend in part on Huawei's ability to supply equipment and iterate designs. Major players Alibaba and Tencent will invest heavily in cloud, energy, and vehicle infrastructure, which Beijing bills as supporting the industrial internet.[61]

Looking Ahead

In addition to pressure on US technology and third-party companies to discontinue supplying Huawei and its key subsidiaries, other actions are working to further separate the telecommunications sectors at the carrier service and fiber optic cable landing station levels.

Carrier Separation Accelerates

Foreign telecommunications carriers that wish to terminate traffic for their customers in the United States are required to have a "Section 214" license before starting services. China Telecom and Unicom hold licenses issued under a vastly different climate in US–China relations. Chinese cellular giant China Mobile had filed a request for a 214 license

[59] White House, *National Security Strategy*.

[60] Author discussions with US government officials, May 2020.

[61] Liu, Li, and Ting-fang, "China Bets."

starting in 2013, and the FCC finally and formally declared the firm a national security threat and rejected the license request in May 2019.[62] The FCC language explaining the decision was similar to the language used in describing Huawei as a national security threat. The commission found "that due to several factors related to China Mobile USA's ownership and control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a mitigation agreement between China Mobile and the federal government."[63]

In April 2020 a little-noticed executive order[64] restructured US government efforts to track and approve foreign telecom carriers applying for licenses to operate within the United States. The primary target is China. The order formalized a key responsibility of the national security–focused US "Team Telecom"—an interagency team including the Departments of Justice, Homeland Security, and Defense—to review specific FCC license applications, including those submitted by foreign companies and for fiber optic undersea cables connecting the United States with other countries. Team Telecom had weighed in previously on the China Mobile section 214 license denial. Team Telecom was henceforth formally to be known as the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.[65] The new Clean Carrier initiative announced in August by Secretary of State Pompeo basically endorsed the recommendations made earlier to the FCC to revoke the operating licenses of the Chinese carriers.

In September 2019, US senators Chuck Schumer (D-NY) and Tom Cotton (R-AR) wrote to the FCC asking for a review of the Chinese licenses.[66] In mid-April, probably in response to this letter and other concerns expressed by some FCC commissioners, the US Justice Department issued a press release announcing that executive branch agencies had recommended that the FCC revoke and terminate China Telecom's license.[67] The release stressed that this action was being coordinated under the old arrangements with Team Telecom and not under the new committee structure as outlined in the April 4 executive order.

China Unicom is likely to suffer the same fate and lose its license in the coming months. As of September 2020, China's reaction remains unclear, though Chinese netizens in early April advocated retaliation against US companies, and Beijing is likely to be under further pressure to retaliate in kind. Currently, US global carrier AT&T operates a joint venture arrangement with China Telecom to serve US multinational corporations operating in China. AT&T's license is up for renewal this year, and Beijing could choose to disapprove this license in retaliation for all of China's major telecom carriers being eliminated from the US market. Finally, in late August the Department of Defense released a second list of Chinese companies with ties to China's military, including China Unicom—this left all three carriers under this designation, which could be used as a basis for taking further

[62] FCC, "FCC Denies China Mobile USA Application."

[63] FCC, "FCC Denies China Mobile USA Application."

[64] White House, "Executive Order on Committee for Assessment of Foreign Participation."

[65] The new committee, headed by Attorney General William Barr, who is increasingly active in telecommunications policy in areas including 5G strategy, will field referrals from the FCC on licensing. The committee itself is heavily composed of national security stakeholders. It includes only the defense secretary, the attorney general, and the homeland security secretary, with other leading departments having only an advisory and not an executive authority—this includes the Departments of State, Commerce, and Treasury; the Office of the US Trade Representative; and other senior officials such as the national security adviser and the chairman of the Council of Economic Advisers.

[66] See Senate Democrats, "Schumer, Cotton Request FCC Conduct Review."

[67] Department of Justice, "Executive Branch Agencies."

action against the firms.[68] The separation of the sectors at the operator level then could be nearly total by the end of 2020.

Transpacific Fiber Optic Cables

The eight-thousand-mile Pacific Light Cable Network project linking the United States and Hong Kong was nearly complete as of late 2019. Google and Facebook are major backers. However, in June 2020 Team Telecom recommended that the FCC deny a license to the Hong Kong portion of the cable, objecting both to Hong Kong as a landing venue and to Pacific Light Data Communication (PLDC)—a subsidiary of Dr. Peng Telecommunication and Media Group, a Chinese broadband provider—as a partner.[69] Team Telecom had typically approved similar projects with Chinese state-owned operators but is now seeking some type of mitigation strategy to ensure that the consortium could operate portions of the cable. All transoceanic cable projects originating in the United States are subject to high levels of US government scrutiny and approval. But usually there are conditions tied to the approval of such cables, similar to the process used by the Committee for Foreign Investment in the United States to approve foreign investment deals. In addition, there would probably be some level of ongoing inspection of cable operations that involves US government officials. Accustomed to the Chinese government blocking their content within China, tech actors such as Facebook and Google now face blockage of full deployment of network infrastructure by the US government if a China landing is involved. The now dark fiber optic cable link from Taiwan to Hong Kong has become another symbol of the increasing physical separation of the two countries' telecom sectors.

More generally, the FCC in early October 2020 released a detailed document entitled *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*.[70] The long document is an attempt to clarify how Team Telecom—now called the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector—determines approvals, through a lengthy review process, of applications for 214 US operating licenses for foreign carriers and submarine cable systems. The document seeks to "improve the timeliness and transparency of the process by which it seeks the views of Executive Branch agencies related to certain applications with foreign ownership." The document also refers in some detail to conditions under which the committee could recommend to the FCC action against existing license holders for submarine cable systems. This opens the potential for the FCC to revoke landing licenses for existing transpacific cable systems terminating in China, following the precedent set by the negative Pacific Light Cable Network license recommendation for the cable segment landing in Hong Kong. That recommendation has generated major concern within the cable industry about the potential for further action by the US government involving cable system landings in China operated by Chinese carriers or with Chinese investors.

The implications of further disruptions and uncertainty to the cable licensing process are profound for the ICT industry and the future of the internet itself. Undersea cable systems in the best of circumstances require massive investment, typically involving international consortia of investors and operators, long lead times, economies of scale, and a predictable regulatory approval process. With the demand for bandwidth already outstripping the capacity of existing cables, a US regulatory approach that sought to restrict cable landings in China would be highly disruptive for future cable

[68] Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999.

[69] Department of Justice, "Team Telecom Recommends."

[70] FCC, *Process Reform for Executive Branch Review*.

system planning. Given the massive increase in demand for data-carrying capacity resulting from the move online caused by the COVID-19 pandemic and other geographic factors like huge digital economy growth in Africa and Latin America, cable systems linking these markets with Europe and Asia will be built, and Chinese companies would take up the slack if US investors and operators are excluded from participating in key cable system development.[71] Policymakers should also consider the implications of reducing the availability and resilience of network connectivity between the United States and the Asia Pacific—for example, by excluding routes that in any way involve a China landing—which would also mean that global data storage and processing capacities would potentially migrate out of the United States to other parts of the world.

Next-Generation Mobile Communications Standards

Future standards also are likely to be a tale of two worlds. While US strategy around 5G has been slow to gel into short-, medium-, and long-term strategies, one area where there appears to be significant agreement in some limited, particularly anti-China, quarters is expanding the US government role in standards setting. The aim appears to be to counter what is considered the malign influence of the Chinese government and Chinese companies on the standards development process under the ITU and 3GPP.

The language on standards in several documents suggests that the thrust of US policy will be toward eventually establishing a new process for "appropriate" and "responsible" standards that appears likely to preclude the participation of companies from "adversary" nations or "nations of concern." Relevant documents include the Secure 5G and Beyond Act;[72] the new White House 5G Strategy published in early April 2020;[73] the Utilizing Strategic Allied (USA) Telecommunications Act, proposed in January by a bipartisan group of congresspersons;[74] the Cyber Solarium Commission Report published in March;[75] and other legislation and government documents.

The rising tide of overall US–China technology conflict and the bifurcation of the two countries' telecommunications sectors seems likely to expand into a broader tussle over the future of the internet itself.

This approach to standards will be long term and will require buy-in from key governments, particularly countries like Japan and South Korea, that also harbor considerable concerns about China's ICT sector in general and Huawei and ZTE in particular. Any effort to force such a major change in the way modern mobile communications standards have been set would require the expenditure of substantial political capital and a deep understanding of how the industry has evolved from the 2G to the 5G generation. This includes critical areas such as handling standard essential patents that are a key part of why companies participate in the standards-setting process. It remains uncertain whether the US government has a clear strategy on the standards issue, and whether the mobile industry and key groups like GSMA would react to any attempt to bifurcate the standards development process, given its complexity and its current well-established processes.

[71] Discussions with industry, October 2020.

[72] Secure 5G and Beyond Act of 2020.

[73] White House, *National Security Strategy*.

[74] Future Networks Team, *Internet 2030*.

[75] US Cyberspace Solarium Commission, *Report*.

Next-Generation Internet Architecture

The rising tide of overall US–China technology conflict and the bifurcation of the two countries' telecommunications sectors seems likely to expand into a broader tussle over the future of the internet itself.

While media reports frame the issue as Huawei and other codevelopers pushing for an alternative internet architecture and standards that could favor Beijing's vision of data sovereignty and information control, the so-called New Internet Protocol (IP) proposal is based on a forward-looking white paper sponsored by Huawei, not a standards proposal. The white paper, *Internet 2030: Towards a New Internet for the Year 2030 and Beyond*,[76] argues that the current internet architecture, including the underlying telecommunications infrastructure as well as Internet Transport Control Protocol/Internet Protocol (TCP/IP) and latency issues, may not be optimal for new types of applications like holographic communications and augmented reality/virtual reality. Internet governance observers view the paper as a call for study of future architectures that would take decades to be adopted within the current structure.[77] Milton Mueller, founder of the Internet Governance Project, argues that a fear of China's technology rise and the current regime in Beijing are driving Western concerns about initiatives such as New IP and wonders why it is "dangerous for Chinese companies to entertain bold new ideas about the next steps in the evolution of data communications."

The white paper and its Chinese backers spotlight the ambitions that companies like Huawei in particular and China in general have for shaping the next-generation telecommunications and internet architecture. Beijing and Chinese organizations have been pushing a competing vision for internet architecture developed by Robert Kahn, who coinvented the TCP/IP protocol with Vint Cerf. Kahn's Digital Object Architecture (DOA)[78]—a general architecture for a distributed information storage, location, and retrieval system running over the internet—has been taken up by Chinese players and championed as a viable alternative for ensuring the security of the internet with the huge explosion of connected devices as part of the IoT. Chinese officials and companies have used the ITU Telecommunications Standards Sector (ITU-T) Study Group 20[79] (focused on IoT and smart cities) and ITU-T Study Group 17 (focused on security)[80] as the main points of influence. While this effort has failed to gain traction within the existing internet governance system, Chinese companies such as Huawei and the major carriers have devoted considerable effort to researching new approaches to telecommunications architectures in the age of IoT that could serve as the basis for an alternative framework in the coming decade.

New Technology Platforms Designed to Push Beijing's Concept of Digital and Data Sovereignty

Finally, a number of broader technology trends highlight how the issue of telecommunications networks is a subset of a more expansive set of decoupling possibilities between the two countries, extending into areas such as financial services and cross-border payments and data systems.

Over the next ten years, the possibility of China and like-minded allies pursuing an alternative technology stack—including but going well beyond telecommunications infrastructure—appears increasingly likely, particularly in the wake of the coronavirus pandemic. Programs such as China's Belt and Road Initiative and its digital counterpart, the Digital Silk Road, are critical to

[76] Future Networks Team, *Internet 2030*.

[77] Mueller, "About That Chinese 'Reinvention' of the Internet."

[78] Buell, "What Is the Digital Object Architecture (DOA)?"

[79] ITU, "ITU-T in Brief."

[80] See, e.g., Lyons and Kahn, "Blocks as Digital Entities."

this trend.[81] While assessing what these initiatives actually constitute has been challenging, Beijing's vision is coming into focus. One certainty is that, across emerging markets as well as Asian- and European-developed economies, Beijing wants Chinese companies to be involved at all levels of digital infrastructure construction: fiber optic and mobile equipment infrastructure, telecommunications carrier services, and over-the-top providers of applications services.

Indeed, Beijing's support for accelerating Digital Silk Road–branded projects could contribute to and accelerate the bifurcation of technology stacks globally. In the wake of the pandemic, Belt and Road countries, for example, will be looking to boost the capacity of their digital infrastructures. "Team China's" tech conglomerates will enjoy significant state support to meet this demand as state organs seek to kick-start economic growth and bolster geopolitical influence. A significantly worsening US–China relationship and growing technology competition appear likely to compel China to abandon cooperation with Western entities and, instead, to pursue a separate technology stack, replete with its own standards-setting process. The increasing lack of trust among China, the United States, and European governments is being exacerbated by a push in the United States to stress China's handling of the COVID-19 outbreak and overall responsibility for the crisis as the basis for further economic and technology decoupling from Beijing.

Many Chinese tech companies still view the Belt and Road and Digital Silk Road initiatives as means of securing short-term boosts to profits. Yet Chinese officials increasingly view the Digital Silk Road in particular as providing a ready channel for testing out the deployment of technologies and systems as part of a technology stack that hews closer to Beijing's concept of data and digital sovereignty.[82]

Already, concern about the dominance of large Western tech platforms has been the theme of many of the discussions and presentations at the annual World Internet Conference in Wuzhen,[83] where Belt and Road countries are well represented and US and EU government presence is minimal. The conference has also featured increasing participation from the ITU, where Beijing enjoys strong influence.

Financial services and payments are another key example of how Beijing seeks to shape the technology stack and supported systems. In April 2020,[84] Beijing launched the Blockchain Services Network (BSN),[85] an ambitious effort to provide a low-cost technology platform for developing blockchain-based applications. The six-month pilot—which officials wrapped in Belt and Road rhetoric—took place in Singapore as well as China. Separately, in December 2019 at the Hainan Free Trade Zone & Global Digital Economic Forum,[86] Chinese government representatives touted the development of blockchain in mainland China to counterparts in Russia, Kazakhstan, Indonesia, and Bahrain. The forum included the launch of a BSN developer competition organized by Huobi China, a leading blockchain and cryptocurrency company, telecom giant China Mobile, and China UnionPay. A senior State Information Center official touted BSN as a key part of China's national information infrastructure that could be deployed globally at low cost. Rhetoric around both BSN and China's central bank digital currency plans suggests that China aspires to lead the development of a global, non-US-influenced payment system, though there are any number of major political, economic, and technological hurdles currently standing in its way. Huawei has also developed blockchain as a service (BaaS) for its cloud offerings and is a member of

[81] Triolo and Greene, "Will China Control the Global Internet?"

[82] Triolo and Greene, "Will China Control the Global Internet?"

[83] See the conference website, http://www.wuzhenwic.org/.

[84] Stockton, "China Launches National Blockchain Network."

[85] Xinhua, "China's Blockchain-Based Service Network."

[86] Ghosh, "China Reinforces Blockchain Connection."

Navigating the complex US–China relationship within the substantially changed telecommunications world that US policymakers confront presents a huge challenge to existing US institutions. What is at stake is nothing less than the state of the global telecommunications landscape and the internet itself in 2030.

and contributor to the Linux Foundation's Hyperledger Block Consortium.[87] Hyperledger is also a key piece of BSN. Blockchain was also included in Beijing's rollout of the new infrastructure initiative in May 2020.[88]

No US company remotely compares to Huawei's sweeping technological reach. Huawei is increasingly a major player in proposing next-generation internet architectures, developing an AI stack and making it open source, collaborating on new blockchain initiatives, and engaging in key consumer and industrial applications, from augmented and virtual reality to autonomous vehicles, smart cities, and smart factories. European telecom vendors remain highly capable in mobile infrastructure but have nowhere near the technology ambitions or reach of Huawei.

In sum, the issue of the connectivity and dependence between the US and China telecommunications sectors has morphed far beyond that of the 1980s and 1990s era focused on voice calls between large central office switches into a global competition about next-generation architectures and governance systems for cyberspace as a whole. This process has gone from US technology dominance to something far more complex and competitive, and the telecommunications sectors of the two countries in 2030 will look back on 2020 as this paper has looked back on the 1990s: as a simpler era about to be displaced by a much more complex one, with a very different relationship between competing nations.

Maxims for the US Government Approach

Navigating the complex US–China relationship within the substantially changed telecommunications world that US policymakers confront presents a huge challenge to existing US institutions. What is at stake is nothing less than the state of the global telecommunications landscape and the internet itself in 2030. American policymakers must look to a ten-year horizon within which 5G networks will be deployed and the following generation will be researched and developed. They must in this context devise a strategy that recognizes that some level of significant decoupling, deleveraging, and China–America bifurcation seems inevitable. Yet, they must also acknowledge that there are some levels of technology interconnection that may be inevitable for US companies to successfully compete in global markets for business and influence. They must start from the premise that there are currently no US competitors to global telecommunications network systems integrators, but also note that US global leadership, particularly in data network infrastructure, internet services, and emerging technology, is at stake in the technology race with China. The American response must engage a mix of public and private collaborations committed to maintaining a multi-stakeholder governance model for an interoperable internet, and take into consideration the second- and third-order impacts of policies and regulations that could have unintentionally damaging and disruptive effects on US competitiveness and connectivity to the rest of the world. The United States should seek nuanced policy approaches that differentiate how

[87] Zhao, "Huawei Unveils Hyperledger-Powered Blockchain Service Platform."

[88] Triolo and Sherlock, "'New Infrastructure.'"

5G networks are handled domestically and internationally, and it should consider how US policies impact the evolution of a global internet infrastructure that is dependent on factors outside of direct US control. For example, if the United States does not actively encourage more investments in undersea cable infrastructure, this could result in computing capabilities moving offshore—which would threaten the central role the United States has occupied in the internet ecosystem for decades. Rather than taking a piecemeal, reactive approach that creates uncertainty for domestic industry, the United States should develop a coherent strategy centered on gaining acceptance from allies and, critically, the private sector that is capable of both addressing specific security threats and enables US companies to maintain global leadership.

The process should foster a competitive playing field and avoid the dominance of one company or technology system. One possible approach would combine a new plurilateral and multilateral approach to network security, reflecting modern security approaches, with an effort to foster diversity in the vendor space while seeking to keep the massive China market open to existing and future Western vendors to ensure they have sufficient prospects for growth. The latter is clearly a tall order in the existing geopolitical setting, but no less crucial given the size of the Chinese market. These challenges center on several key nodes. The United States could also provide economic incentives for US and other trusted companies to build submarine cables and develop strategic partnerships with countries like India and Indonesia to develop non-China-dependent routes across the Pacific.

A new approach that builds on the UK model and extends it more broadly, first to US allies and then more broadly to EU member states and Asian democracies, would begin building a future security architecture for next-generation networks, 5G and beyond.

Supporting Multilateral and Plurilateral Efforts to Bolster 5G Supply Chain Security

Whatever the outcome of the US campaign to convince allies and other countries to abandon Huawei, security concerns around 5G networks are here to stay. Even a Chinese-free US and allied 5G network must include better security. In early 2020, the UK National Cybersecurity Centre (NCSC) issued a series of documents designed to ensure the security of 5G supply chains and deployments, including a framework for all new vendors entering the space. The UK government announcement[89] to Parliament that the United Kingdom would be allowing "high-risk" vendors to supply equipment to carriers for its 5G networks, without naming Huawei explicitly, marked a watershed for Europe that set the United Kingdom off in a different direction from the United States. Rather than adopting a zero-tolerance policy toward Huawei, the United Kingdom instead put forward a holistic approach to network security for advanced telecommunications networks. The announcement was accompanied by the release of very detailed analysis of the risk to telecommunications networks, plus new security requirements[90] for both carriers and vendors as well as additional restrictions around high-risk vendors, such as Huawei. As previously noted, under a new political climate vis-à-vis China, in the summer of 2020 the UK government backpedaled on allowing new use of Huawei equipment and set a timeline for carriers to phase out Huawei equipment from

[89] See UK Government, "Baroness Morgan's Written Ministerial Statement."

[90] See NCSC, *Summary*.

their networks.[91] The primary factor here was the success of the United States' change to the foreign direct product rule directed at Huawei, which cast major doubt on the firm's ability to supply UK carriers. The NCSC also noted that if as a result Huawei had to turn to alternative vendors for hardware, it would be difficult to verify the security of new equipment.[92]

In addition to the tough new security standards around all aspects of 5G, the NCSC-released documents sketched out a UK government strategy aimed at driving diversification of vendors in 5G, particularly in the RAN. The UK government will work with new vendors in this space to ensure that they are able to comply with the new security framework when they offer new products or services. One initial focus will be to push for interoperability of RAN interfaces to ensure that carriers can use equipment developed by new market entrants. This will be a lengthy process, with UK officials talking of a five-year timeline for developing a more competitive RAN market.

US agencies have deep technical know-how and could develop and implement a strategy similar to the UK approach. However, they have not yet done so. ***A new approach that builds on the UK model and extends it more broadly, first to US allies and then more broadly to EU member states and Asian democracies, would begin building a future security architecture for next-generation networks, 5G and beyond. Within this broader framework, it should be possible for Chinese vendors to convince regulators to drop the high-risk vendor, though they may remain barred from some parts of the network, such as mobile edge computing. This approach can also be applied to the architecture itself of next-generation networks.***

[91] See UK Government, "Huawei to Be Removed."

[92] NCSC, *Advice*.

Shoring up Existing Vendors and Bridging to the New Era of Open Standards/Interface Approaches Such as O-RAN

While, as of August 2020, there does not appear to be an appetite within the US government to fund investments in either Ericsson or Nokia, US officials are likely to back private equity efforts to shore up the firms via strategic investments. In addition, US government policies going forward will likely benefit these firms as the US military pursues its own 5G network ambitions and the FCC pushes rural carriers to rip Huawei and ZTE gear from their networks and replace it over the next two years.[93] US policy is already attuned to the industry direction, where carriers prefer open standards and interfaces enabling them to choose from many vendors, specifically, around the concept of O-RAN,[94] without being locked into one or several large integrated vendors. However, policymakers need to find ways to foster vendor diversity over the next two to three years and then expand and solidify that diverse vendor marketplace over the long term.[95]

[93] Donahue suggests several options to support Ericsson, Nokia, and Samsung, such as stock investments, tax policies, debt guarantees, loans, and procurements. Another option he proposes is the US government working with private sector actors to acquire a controlling interest on one of the European firms, possibly using authorities under the Defense Production Act Title III or via congressional authorization. As of September 2020, these options are being considered but are less likely to go forward, in favor of a strategic private equity investment. See Donahue, "Worst Possible Day."

[94] O-RAN is just one of several approaches to opening up the telecom equipment vendor sector to allow for more modular approaches and supply chain diversity. O-RAN is relatively narrow with a focus on open-source software running on commodity hardware. Others argue commodity hardware cannot reach sufficient performance/reliability. Also, O-RAN does not solve the need for integration. An alternative approach would involve tight integration of modular hardware and software. Other approaches are emerging within industry.

[95] This is essentially Donahue's third option, "creating a US-based consortium," but it is most likely that this will be a

This requires creation of new governmental structures to manage the complex interactions between industry and governments, both in the United States and in other countries with similar security and diversity concerns. However, the danger is that this approach, coming at a time of heightened bilateral tensions between the United States and China, will help drive further bifurcation of the advanced telecommunications network space. In April 2020, US carriers led the formation of the Open RAN Policy Coalition (ORPC),[96] with over forty members, including leading technology companies from the United States, Japan, and Europe. None of the members are from China, India, or emerging market countries. Some observers believed that O-RAN had been "politically hijacked" in the US effort to cripple Huawei. The existing O-RAN Alliance includes key Chinese telecommunications companies as vendors, and this sets up the potential for O-RAN to also develop along separate lines. A bill before the US Congress at the time of this writing, the Utilizing Strategic Allied (USA) Telecommunications Act,[97] is designed to encourage competition via accelerating the O-RAN model.

The US government will have to consider how to most beneficially support a range of other open-source and virtualization efforts in the telecommunications arena as the industry moves to open standards and interfaces in anticipation of a new standards-setting effort on 6G mobile. In addition to O-RAN for the RAN, for example, there are other efforts to make parts of the core open source—for example, Open Platform for Network Function Virtualization (OPNFV);[98] the Open Network Foundation (ONF),[99] which is intended to promote the use of software-defined networking via open standards development; and the Linux Foundation's Open Network Automation Platform (ONAP),[100] which does the same for the orchestration and management portions of next-generation networks.

Similarly, the US government will need to determine how best to support other standards efforts, including initiatives undertaken by the European Telecommunications Standards Institute (ETSI) focused on software-defined networking and virtualization,[101] IEEE's Wi-Fi 6 efforts,[102] the Internet Engineering Task Force (IETF), and the IEEE Future Networks Initiative's effort for 5G and Beyond.[103] In addition, the US National Science Foundation is funding open-source test beds such as Platforms for Advanced Wireless Research (PAWR).[104] As noted above, any effort to try to leapfrog to 6G outside of or in a complementary manner to 3GPP and ITU efforts will require a deeper understanding of open-source initiatives and collaboration with European partners and others in Asia, particularly Japan and South Korea. This leapfrog approach would require that the US government forge technology alliances that are enduring, coupled with market forces, flexible, and technology agnostic. This will likely require new policy and technology organizations to be established within key government departments to ensure the requisite expertise can be brought to bear.

A US military program launched by the Defense Advanced Research Projects Agency (DARPA) is attempting to bridge open-source initiatives with security concerns around 5G. The Open,

consortium that includes players from Japan, South Korea, and Europe, and not just US firms. See Donahue, "Worst Possible Day."

96 See Fletcher, "AT&T, Verizon Part of New 31-Member Open RAN Policy Coalition."

97 See "A Bill to Use Proceeds from Spectrum Auctions."

98 See the OPNFV website, https://www.opnfv.org/.

99 See the ONF website, https://www.opennetworking.org/.

100 See the ONAP website, https://www.onap.org/.

101 See, e.g., ETSI, "Network Functions Virtualisation (NFV)."

102 See IEEE, "IEEE Future Directions."

103 See IEEE, "IEEE Future Networks."

104 See the PAWR website, https://advancedwireless.org/.

Programmable, Secure 5G program (OPS-5G) is expected to launch in October 2020.[105] Its designers claim that "OPS-5G changes are focused on increasing trust at a set of soft points that include unmanaged, unattended, long-lived, and possibly long-forgotten IoT devices. Additionally, OPS-5G addresses unintended and unwanted interactions between network slices and threats from the vast increases in network scale." It remains unclear how this effort would be plugged into existing private sector initiatives around O-RAN and security architecture, and how all this would mesh with existing 5G standards around security still being developed by 3GPP. This highlights the challenges of working within existing bodies and processes or developing new ones and achieving sufficient industry buy-in. Discussions around the US military pursuing its own 5G network development run into a similar dynamic, where it is unclear which companies would build a separate military network at cost and scale.

A key question will be whether the United States can foster a diversified vendor market across the United States, Japan, South Korea, and Europe, without the vendors having access to China's vast market.

A New Industrial Policy

Finally, all of the above approaches could most effectively be wrapped into a longer-term approach that addresses all aspects of the role of governments in an era of rapidly developing telecommunications technology. A central goal should be to maintain global interoperability and avoid damaging bifurcation of the global industry. Within this context, the US government must both adapt to and attempt to shape all of the following: (1) the deployment of next-generation wireless and fixed networks; (2) moves toward modular, interoperable open standards and interfaces for hardware and software; and (3) the need to level the playing field for companies in the massive Chinese market. ***A key question will be whether the United States can foster a diversified vendor market across the United States, Japan, South Korea, and Europe, without the vendors having access to China's vast market.*** This is likely to require shoring up European vendors, fostering diversity, and using multilateral means (in conjunction with major market players such as Europe and Japan) to push China to open its market so that prospective vendors can access a market that would provide economies of scale and future potential growth.[106]

Only a long-term strategy that includes trade and investment and a united US and European approach could succeed in opening the Chinese telecom market for Western equipment and leveling the playing field. But US efforts to ban Huawei and ZTE are at odds with such an approach, and Beijing would be unlikely to agree to allow Western vendors to win tenders within the current political environment.[107] Other approaches such as fostering the establishment of an international organization to establish standards around security and establishing a level playing field with the ICT sector are destined to run into political opposition

[105] See "Open Programmable Secure 5G (OPS-5G)."

[106] See Waring, "Nokia Misses Massive China Mobile 5G Tender." In 2014, after threatening to launch an investigation, the EU came to an agreement with China to address EU concerns about Huawei subsidies such as export credits. The EU also pushed for greater access for Ericsson and Nokia to the Chinese market, but progress on both of these areas has been limited, despite talk of revisiting the issue last year. Nokia, for example, was shut out of a major China Mobile tender in April 2020, likely over Chinese concerns about the company's finances and technology, while Ericsson landed around 12 percent of the contracts, and all the rest went to ZTE and Huawei.

[107] See Triolo and Allison, "Will the Battle over Huawei Kill Globalization?"

but also represent a potentially attractive alternative to change the rules of the game.[108]

Alternative approaches include Donahue's proposal,[109] which would entail the United States single-handedly upending the existing global system, including the vital standards-setting process, the overarching push for interoperability, the highly interconnected nature of global carrier networks, and a market-based division of labor that includes access to all markets. This would be a hugely expensive undertaking, and probably a bridge too far, particularly in the wake of the global COVID-19 pandemic.

The challenges of this approach were highlighted by an early 2020 call from the US Department of State to a major US carrier, after Secretary of State Pompeo's speech warning of the dangers of Huawei. A senior State Department official wanted to know whether it was possible for the carrier to arrange overseas roaming on its network such that US government officials' and US citizens' voice and data traffic would not traverse Huawei equipment. The carrier politely explained that there is no way for the firm's network to know the vendor of the equipment that is carrying traffic at any given moment, and that traffic would probably traverse many vendors' hardware and software at the same time depending on the application or call. The only way to feasibly do this would be to cut off all roaming agreements for all carriers known to be using Huawei gear. That would mean, of course, China; virtually all of Europe and Africa, except Rwanda; parts of Latin America, the Middle East, Asia, and Russia; plus Canada and Mexico. This of course struck the carrier as an approach that would be broadly destructive for international commerce and for the firm, which operates a highly globally integrated network.[110] This effort is now nonetheless part of the so-called 5G Clean Path initiative launched in late April 2020.[111] Global interoperability could become a casualty of this approach, particularly looking ahead to broad 5G stand-alone deployments and eventually the dawn of the 6G era.

The telecommunications sectors of the United States and China, once closely intertwined, appear destined for further separation absent a major change in bilateral relations, substantial increase in trust between the two governments, and the political will on both sides to reengage in trade and other bilateral discussions to address the major technology and market access challenges the two sides face. The impact of unrestrained decoupling and deleveraging in other critical tech sectors, such as semiconductors, will leave US companies in a difficult position. At the moment, it is clear that the accelerating engines of technology development and business imperatives are continuing to run in a direction—toward globalization and interoperability—that is opposite of where the engines of government are driving. The resulting collisions will be traumatic.[112]

[108] Kupchan and Triolo, "Distrust But Verify"

[109] Donahue warns that the difficulties of developing a US- or US/allies-dominated ICT supply chain that would allow the building of a completely China-free set of global commercial networks are immense and can likely only be funded with full Department of Defense buy-in, and through major mobilization of the US government in conjunction with the private sector. See Donahue, "Worst Possible Day."

[110] Author discussions with US carriers.

[111] See Department of State, "Secretary Michael R. Pompeo."

[112] See, e.g., Muggah and Rohozinski, "What's at Stake?"

Bibliography

AFD China. "Huawei Files 25% of the World's 4G Patents." [Referencing China IP News.] AFD China, 2014. https://www.afdip.com/index.php?ac=article&at=read&did=2356.

Ahrens, Nathaniel. *Case Study: Huawei. China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan*. Washington, DC: Center for Strategic and International Studies, 2013. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

Alper, Alexandra, Toby Sterling, and Stephen Nellis. "Trump Administration Pressed Dutch Hard to Cancel China Chip-Equipment Sale: Sources." Reuters, January 6, 2020. https://www.reuters.com/article/us-asml-holding-usa-china-insight/trump-administration-pressed-dutch-hard-to-cancel-china-chip-equipment-sale-sources-idUSKBN1Z50HN.

Anderson, Howard. "10 Reasons Why Motorola Failed." Network World, April 9, 2008. https://www.networkworld.com/article/2277903/10-reasons-why-motorola-failed.html.

"Attorney General William Barr's Keynote Address: China Initiative Conference." Transcript. Center for Strategic and International Studies. February 6, 2020. https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference.

"A Bill to Use Proceeds from Spectrum Auctions," S. 3189, 116th. Cong. (2020). https://www.congress.gov/bill/116th-congress/senate-bill/3189.

BIS (Department of Commerce Bureau of Industry and Security). "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List." 15 C.F.R. 744. *Federal Register* 84, no. 162 (August 21, 2019): 43493. https://www.federalregister.gov/documents/2019/08/21/2019-17921/addition-of-certain-entities-to-the-entity-list-and-revision-of-entries-on-the-entity-list.

———. "Addition of Entities to the Entity List." 15 C.F.R. 744. *Federal Register* 84, no. 98 (May 21, 2019): 22961. https://www.bis.doc.gov/index.php/documents/regulations-docs/2394-huawei-and-affiliates-entity-list-rule/file.

———. "Additions to the Entity List." 15 C.F.R. 744. *Federal Register* 81, no. 45 (March 8, 2016): 12004. https://www.govinfo.gov/content/pkg/FR-2016-03-08/pdf/2016-05104.pdf.

———. "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List." 15 C.F.R. 744. *Federal Register* 85, no. 97 (May 19, 2020): 29849 https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

———. "Order Terminating Denial Order Issued on April 15, 2018, against Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd." *Federal Register* 83, no. 141 (July 23, 2018): 34825. https://www.bis.doc.gov/index.php/documents/pdfs/2246-zte-order-terminating-denial-order.

Blanchard, Ben. "Taiwan Minister Says TSMC Has Offset Lost Huawei Orders." Reuters, June 22, 2020. https://www.reuters.com/article/us-taiwan-economy/taiwan-minister-says-tsmc-has-offset-lost-huawei-orders-idUSKBN23T1E3.

Buell, Mark. "What Is the Digital Object Architecture (DOA)? Read Our New Information Paper." Internet Society (blog), October 26, 2016. https://www.internetsociety.org/blog/2016/10/what-is-the-digital-object-architecture-doa-read-our-new-information-paper/.

"China Announces Measures to Boost IC Industry." *China Daily*, Updated June 25, 2014. http://usa.chinadaily.com.cn/business/2014-06/25/content_17613997.htm.

Demchak, Chris, and Yuval Shavitt. "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking." *Military Cyber Affairs* 3, no. 1, article 7 (2018): 1–9. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca.

Department of Commerce. "Secretary Ross Announces Activation of ZTE Denial Order in Response to Repeated False Statements to the U.S. Government." Press release, April 16, 2018. https://www.commerce.gov/news/press-releases/2018/04/secretary-ross-announces-activation-zte-denial-order-response-repeated.

———. "Securing the Information and Communications Technology and Services Supply Chain." 15 C.F.R. 7. *Federal Register* 84, no. 229 (November 27, 2019): 65316. https://www.govinfo.gov/content/pkg/FR-2019-11-27/pdf/2019-25554.pdf.

Department of Defense. General Services Administration. National Aeronautics and Space Administration. "Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment." *Federal Register* 85, no. 135 (July 14, 2020): 42665. https://www.govinfo.gov/content/pkg/FR-2020-07-14/pdf/2020-15293.pdf.

———. "Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (PUBLIC LAW 105–261)." https://media.defense.gov/2020/Aug/28/2002486689/-1/-1/1/LINK_1_1237_TRANCHE-23_QUALIFYING_ENTITIES.PDF.

Department of Justice. "Executive Branch Agencies Recommend the FCC Revoke and Terminate China Telecom's Authorizations to Provide International Telecommunications Services in the United States." News release, April 9, 2020. https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations.

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

Department of State. "The Clean Network." https://www.state.gov/the-clean-network/.

———. "Secretary Michael R. Pompeo at a Press Availability." April 29, 2020. https://www.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/.

Dickson, Annabelle, and Laurens Cerulus. "Boris Johnson Allows Huawei to Build Parts of UK 5G Network." *Politico*, January 28, 2020. https://www.politico.eu/article/boris-johnson-allows-huawei-to-build-parts-of-uk-5g-network/.

Donahue, Thomas. "The Worst Possible Day: U.S. Telecommunications and Huawei." *PRISM* 8, no. 3 (January 9, 2020): 15–35. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053215/the-worst-possible-day-us-telecommunications-and-huawei/.

ETSI. "Network Functions Virtualisation (NFV)." https://www.etsi.org/technologies/nfv.

European Commission. "Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures." January 29, 2020. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

"Expressing the Sense of the House of Representatives That All Stakeholders in the Deployment of 5G Communications Infrastructure Should Carefully Consider Adherence to the Recommendations of 'The Prague Proposals.'" H.R. 575, 116th Cong. (2019). https://www.congress.gov/bill/116th-congress/house-resolution/575/text.

FCC (Federal Communications Commission). "FCC Denies China Mobile USA Application to Provide Telecommunications Services." News release, May 9, 2019. https://www.fcc.gov/document/fcc-denies-china-mobile-telecom-services-application.

———. "Forum on 5G Open Radio Access Networks." https://www.fcc.gov/news-events/events/forum-5g-virtual-radio-access-networks.

———. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*. FCC 20-133. Washington, DC: Federal Communications Commission, 2020. https://www.fcc.gov/document/fcc-improves-transparency-and-timeliness-foreign-ownership-review.

———. "Protecting against National Security Threats to the Communications Supply Chain through FCC Programs; Huawei Designation; ZTE Designation." 47 C.F.R. 54. *Federal Register* 85, no. 2 (January 3, 2020): 230. https://www.federalregister.gov/documents/2020/01/03/2019-27610/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs.

———. *Protecting against National Security Threats to the Communications Supply Chain through FCC Programs*. FCC 19-121. Washington, DC: Federal Communications Commission, 2019. https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

FCC.report. "GU Holdings Inc." Accessed May 6, 2020. https://fcc.report/IBFS/Company/GU-Holdings-Inc.

Fletcher, Bevin. "AT&T, Verizon Part of New 31-Member Open RAN Policy Coalition." FierceWireless, May 5, 2020. https://www.fiercewireless.com/regulatory/at-t-verizon-among-new-31-member-open-ran-policy-coalition.

Freifeld, Karen, and Sijia Jiang. "China's ZTE Pleads Guilty, Settles U.S. Sanctions Case for Nearly $900 Million." Reuters, March 7, 2017. https://www.reuters.com/article/us-usa-china-zte/chinas-zte-pleads-guilty-settles-u-s-sanctions-case-for-nearly-900-million-idUSKBN16E1X1.

Fuller, Douglas B. *Cutting off Our Nose to Spite Our Face: US Policy toward Huawei and China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools.* National Security Report NSAD-R-2-059. Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2020.

Fuller, Doug, and Paul Triolo. "The Ripple Effects of a Complete Ban on Huawei Access to U.S. Tech Will Be Huge." *SupChina*, May 21, 2019. https://supchina.com/2019/05/21/the-ripple-effects-of-a-complete-ban-on-huawei-access-to-u-s-tech-will-be-huge/.

Future Networks Team. *Internet 2030: Towards a New Internet for the Year 2030 and Beyond*. Huawei Technologies. Accessed May 6, 2020. https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Documents/Internet_2030%20.pdf.

Ghosh, Aarav. "China Reinforces Blockchain Connection with BRI Countries." *Blockchain News*, December 5, 2019. https://www.namecoinnews.com/china-reinforces-blockchain-connection-with-bri-countries/.

Hardesty, Linda. "What Is eCPRI, and Why Is It Important for 5G and Open vRAN?" *Fierce Wireless*. October 15, 2019. https://www.fiercewireless.com/tech/what-ecpri-and-why-it-important-for-5g-and-open-vran.

Harris, Mark. "Google and Facebook Turn Their Backs on Undersea Cable to China. TechCrunch." February 6, 2020. https://techcrunch.com/2020/02/06/google-and-facebook-turn-their-backs-on-undersea-cable-to-china/.

Healthman, Amelia. "Is Huawei Going to Be Removed from the UK's 5G Network? What We Know So Far . . ." *Evening Standard*, July 6, 2020. http://a.msn.com/01/en-gb/BB16o6fW?ocid=se.

IEEE. "IEEE Future Directions." https://cmte.ieee.org/futuredirections/tag/wifi-6/.

———. "IEEE Future Networks." https: //futurenetworks.ieee.org/.

IGI Consulting. *China Telecom 2000: Vol. 3 Switching Market and Opportunities in China*. Winchester, MA: IGI Consulting, 1997.

ITU (International Telecommunication Union). "ITU-T in Brief." Accessed May 6, 2020. https://www.itu.int/en/ITU-T/about/Pages/default.aspx.

Kennedy, Scott. "Made in China 2025." *Critical Questions* (Center for Strategic and International Studies), June 1, 2015. https://www.csis.org/analysis/made-china-2025.

Kleinhans, Jan-Peter. *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung. February 2019. https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf.

Kupchan, Cliff, and Paul Triolo. "Distrust But Verify: How the U.S. and China Can Work Together on Advanced Technology." *SupChina*, November 26, 2019. https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/.

Lazonick, William, and Edward March. "The Rise and Demise of Lucent Technologies." Originally presented to the conference on Innovation and Competition in the Global Communications Technology Industry, INSEAD, August 23–24, 2007. http://www.theairnet.org/files/research/lazonick/Lazonick%20and%20March%20Lucent%20COMPLETE%2020110324.pdf.

Lei, Leping. "China's Optical-Network Evolution." *OEMagazine*, May 2002. https://spie.org/news/chinas-optical-network-evolution?SSO=1.

Li, Yao. "New Infrastructure, What Is It?" [In Chinese.] *Xinhuanet*, April 26, 2020. http://www.xinhuanet.com/politics/2020-04/26/c_1125908061.htm.

Liu, Coco, Lauly Li, and Cheng Ting-fang. "China Bets on $2tn High-Tech Infrastructure Plan to Spark Economy." *Nikkei Asian Review*, June 1, 2020. https://asia.nikkei.com/Business/China-tech/China-bets-on-2tn-high-tech-infrastructure-plan-to-spark-economy.

Lyons, Patrice A., and Robert E. Kahn. "Blocks as Digital Entities: A Standards Perspective." *Information Services & Use* 38, no. 3 (2018): 173–185. https://doi.org/10.3233/ISU-180021.

Mueller, Milton. "About That Chinese 'Reinvention' of the Internet . . ." Internet Governance Project. March 30, 2020. https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/.

Muggah, Robert, and Rafal Rohozinski. "What's at Stake in the U.S.-China Rivalry? The Very Future of the Internet." *Globe and Mail*, August 13, 2020. https://www.theglobeandmail.com/opinion/article-whats-at-stake-in-the-us-china-rivalry-the-very-future-of-the/.

NCSC (National Cybersecurity Centre). *NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks*. London: NCSC, January 28. 2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

———. *Summary of NCSC's Security Analysis for the UK Telecoms Sector*. London: NCSC, January 28. 2020. https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector.

NDRC (National Development and Reform Commission). "Press Conference to Introduce Macroeconomic Operations." [In Chinese.] April 20, 2020. https://www.ndrc.gov.cn/xwdt/xwfb/202004/t20200420_1226031.html.

"Open Programmable Secure 5G (OPS-5G)." DARPA Broad Agency Announcement. HR001120S0026. January 30, 2020. https://beta.sam.gov/opp/6ee795ad86a044d1a64f441ef713a476/view?keywords=OPS-5G&sort=-relevance&index=&is_active=true&page=1.

Osawa, Juro. "AT&T Deal Collapse Forces Huawei to Rethink Global Plans." *The Information*, January 9, 2018. https://www.theinformation.com/articles/at-t-deal-collapse-forces-huawei-to-rethink-global-plans.

Pai, Ajit. "Save the Date." February 6, 2020. https://www.fcc.gov/news-events/blog/2020/02/06/save-date.

Rappeport, Alan. "Trump Contradicts Advisers on China Technology Fears." *New York Times*, February 18, 2020. https://www.nytimes.com/2020/02/18/us/politics/trump-contradicts-advisers-china-technology.html.

Rogers, Mike, and C. A. Dutch Ruppersberger. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Washington, DC: Permanent Select Committee on Intelligence, US House of Representatives, 2012. https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

Salinas, Sara. "Six Top US Intelligence Chiefs Caution against Buying Huawei Phones." CNBC, February 13, 2018 (updated February 15, 2018). https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

Secure 5G and Beyond Act of 2020. Pub. L. No. 116-129, 134 Stat. 223. 2020. https://www.congress.gov/bill/116th-congress/senate-bill/893/text.

Senate Democrats. "Schumer, Cotton Request FCC Conduct Review of Prior FCC-Granted Licenses Authorizing Two Chinese Telecomm Companies – Owned and Controlled by the Chinese Government – to Operate in the U.S.; Senators' Letter Follows FCC's Recent Rejection of China Mobile USA's Application for Same Authorization on National Security Grounds." September 16, 2019. https://www.democrats.senate.gov/newsroom/press-releases/schumer-cotton-request-fcc-conduct-review-of-prior-fcc-granted-licenses-authorizing-two-chinese-telecomm-companies_owned-and-controlled-by-the-chinese-government--to-operate-in-the-us-senators-letter-follows-fccs-recent-rejection-of-china-mobile-usas-application-for-same-authorization-on-national-security-grounds.

Stockton, Nick. "China Launches National Blockchain Network in 100 Cities." *IEEE Spectrum*, March 20, 2020. https://spectrum.ieee.org/computing/software/china-launches-national-blockchain-network-100-cities.

Strumpf, Dan. "Huawei Founder Ren Zhengfei Takes off the Gloves in Fight against U.S." *Wall Street Journal*, June 6, 2020. https://www.wsj.com/articles/huawei-founder-ren-zhengfei-takes-off-the-gloves-in-fight-against-u-s-11591416028.

Stubbs, Jack, and Kate Holton. "UK Tells Telcos to Stockpile Huawei Gear in Face of U.S. Sanctions: Letter." Reuters, June 19, 2020. https://www.reuters.com/article/us-britain-huawei/uk-tells-telcos-to-stockpile-huawei-gear-in-face-of-u-s-sanctions-letter-idUSKBN23Q33R.

Sturgeon, Jamie. "Where Nortel Went Wrong." *Financial Post*, January 14, 2012. https://business.financialpost.com/technology/where-nortel-went-wrong.

Suzuki, Wataru. "Jack Ma Calls for 'Inclusive Chips' Amid US Ban on ZTE." *Nikkei Asian Review*, April 25, 2018. https://asia.nikkei.com/Economy/Trade-war/Jack-Ma-calls-for-inclusive-chips-amid-US-ban-on-ZTE.

Tabuchi, Hiroko. "T-Mobile Accuses Huawei of Theft from Laboratory." *New York Times*, September 4, 2014. https://www.nytimes.com/2014/09/06/business/t-mobile-accuses-huawei-of-theft-from-laboratory.html.

Taylor, Rob, and Sara Germano. "At Gathering of Spy Chiefs, U.S., Allies Agreed to Contain Huawei." *Wall Street Journal*, December 14, 2018. https://www.wsj.com/articles/at-gathering-of-spy-chiefs-u-s-allies-agreed-to-contain-huawei-11544825652.

Tian, Tao, and Wu Chunbo. *The Huawei Story*. Los Angeles: SAGE, 2015.

Triolo, Paul. "China's 5G Strategy: Be First out of the Gate and Ready to Innovate." In *China's Uneven High-Tech Drive, Implications for the United States*, edited by Scott Kennedy, 21–28. China Innovation Policy Series. Washington, DC: Center for Strategic and International Studies, February 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200302_Kennedy_ChinaUnevenDrive_v3.pdf?33r3oE.zYL35PXvcofD5frIVeK1lzS9G.

Triolo, Paul, and Allison Sherlock. "'New Infrastructure'—China's Race for 5G and Networked Everything Has a New Catchphrase." *SupChina*, July 1, 2020. https://supchina.com/2020/07/01/new-infrastructure-chinas-race-for-5g-and-networked-everything-has-a-new-catchphrase/.

Triolo, Paul, and Kevin Allison. "The Geopolitics of 5G." *Eurasia Live*, November 15, 2019. https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g.

———. "The Geopolitics of Semiconductors." Eurasia Live, September 2020. https://www.eurasiagroup.net/live-post/geopolitics-semiconductors.

———. "Will the Battle over Huawei Kill Globalization?" *SupChina*, February 21, 2020. https://supchina.com/2020/02/21/will-the-battle-over-huawei-kill-globalization/.

Triolo, Paul, and Robert Greene. "Will China Control the Global Internet Via Its Digital Silk Road?" *SupChina*, May 8, 2020. https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/.

Triolo, Paul, Rogier Creemers, and John Lee. "Beijing Authorities Push Rapid 5G Deployment Despite COVID-19 Headwinds (Translation)." *DigiChina* (blog), April 21, 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/beijing-authorities-push-rapid-5g-deployment-despite-covid-19-headwinds-translation/.

"Trump Signs Bill Banning ZTE, Huawei Business with US Government." *Telecompaper*, August 14, 2018. https://www.telecompaper.com/news/trump-signs-bill-banning-zte-huawei-business-with-us-government--1256671.

US Cyberspace Solarium Commission. *Cyberspace Solarium Commission Report*. Washington, DC: US Cyberspace Solarium Commission, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

UK Government. "Baroness Morgan's Written Ministerial Statement to the House of Lords on UK Telecommunications." January 28, 2020. https://www.gov.uk/government/news/baroness-morgans-written-ministerial-statement-to-the-house-of-lords-on-uk-telecommunications.

———. "Huawei to Be Removed from UK 5G Networks by 2027." Press release from Department for Digital, Culture, Media & Sport; National Cyber Security Centre; and the Rt. Hon. Oliver Dowden CBE MP, July 14, 2020. https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

Waring, Joseph. "Nokia Misses Massive China Mobile 5G Tender." Mobile World Live, April 1, 2020. https://www.mobileworldlive.com/featured-content/top-three/nokia-misses-massive-china-mobile-5g-tender/.

Webster, Graham, Rogier Creemers, Paul Triolo, and Elsa Kania. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)." *Cybersecurity Initiative*, New America (blog), August 1, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

White House. "Executive Order on Addressing the Threat Posed by TikTok." August 6, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

———. "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector." April 4, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-establishing-committee-assessment-foreign-participation-united-states-telecommunications-services-sector/.

———. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

———. *National Security Strategy of the United States of America*. Washington DC: White House, December 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

———. *National Strategy to Secure 5G*. Washington, DC: White House, March 2020. https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Xinhua. "Commercial Use of China's Blockchain-Based Service Network Kicks Off." *China Daily*, April 27, 2020. https://www.chinadaily.com.cn/a/202004/27/WS5ea629ada310a8b241151ce5.html.

Yan, Xu, and Douglas Pitt. *Chinese Telecommunications Policy*. Norwood, MA: Artech House, Inc., 2002.

Zhao, Wolfie. "Huawei Unveils Hyperledger-Powered Blockchain Service Platform." CoinDesk, April 18, 2018. https://www.coindesk.com/huawei-unveils-hyperledger-based-blockchain-service-platform.

About the Author

Paul Triolo leads the geo-technology practice at Eurasia Group, focusing on global technology policy issues, cybersecurity, internet governance, ICT regulatory issues, and emerging areas such as 5G deployment. As an advisor for the Paulson Institute, he works with the MacroPolo team on China technology issues. He is also a China Digital Economy Fellow (nonresident) at New America, a regular contributor to the *DigiChina* blog, and a columnist with *SupChina*. He is quoted frequently in the media on global tech issues and US–China trade and technology competition. He served in senior positions within the US government for more than twenty-five years, focusing primarily on China's rise as a science and technology and cyber power. Paul holds a bachelor's degree in electrical engineering from Penn State University and has work experience in Silicon Valley.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY