CAROLYN BARTHOLOMEW

CHINA AND 5G

Beijing's techno-nationalist approach to digital innovation puts the United States at a disadvantage, with serious ramifications for economic, military, and political security. Now is the time for a strategic response.

The Chinese Communist Party is determined to dominate the global digital marketplace. Chinese companies with virtually unlimited access to capital for the development of the next generation of connectivity are going head-to-head with US companies. Beyond economic competition, Beijing's techno-authoritarianism travels too, and Beijing is working to export to sympathetic regimes the same combination of equipment and ideology it uses for monitoring and controlling its citizens at home.

Conflicts between China and other nations, including the United States, have been brewing for decades, centering around China's unfair trade practices, subsidies, market barriers, and intellectual property theft. As high technology becomes increasingly important to the global economy, concern about the Chinese government's practices in the world of technology also grows.

The global race to 5G, the fifth generation of cellular network technology, is one of the most visible of the technology flashpoints in the US-China relationship. 5G is the backbone for a wide range of new technological advances, including Smart Cities and the Internet of Things. China is racing to be first with a whole-of-government approach encompassing resources and bureaucratic coordination not imaginable in the United States, which relies on individual companies in the private sector to build and operate 5G infrastructure. China's ambitions extend beyond being first to deploy 5G nationwide or dominate global market share. To facilitate its goals, the Chinese government is carefully calibrating Chinese companies' participation in international standards-setting bodies, aiming to ensure that global standards are compatible with Chinese technology for generations to come.

China's comprehensive approach to advancing 5G, with the weight of the Chinese government and its funding behind it, has both economic and national

security consequences for the United States. China's digital initiatives give China a greater foothold to expand export markets for its technology, develop global standards that favor Chinese products and services, export its authoritarian values, control information, and expand surveillance as it supplies digital infrastructure to consumers and governments throughout the world.

Belt and Road, global stage

The Chinese government's strategy for achieving global technological dominance manifests throughout President Xi Jinping's signature foreign policy, the Belt and Road Initiative (BRI). BRI is an externally oriented development program designed to increase Chinese presence and investments in countries around the world, expand markets for Chinese products, and help China's slowing economy. It is also solidifying China's global footprint and increasing its diplomatic and strategic power. BRI, which formally launched in 2013, is actually not a new concept. It is rather a culmination and rebranding of previous policies and projects aimed at creating a Chinese sphere of geopolitical and economic influence that usurps that of the United States and displaces Western liberal values. Chinese leaders call it the "project of the century" and have written it into the nation's constitution. As China opened up to the world and implemented market-opening economic reforms in the 1980s and 1990s, China's then-paramount leader, Deng Xiaoping, counseled an approach to "hide your capabilities and bide your time." In this view, the outside world did not need to see how China was getting stronger until its leaders were ready to exercise the country's strength. With BRI, China's leadership has signaled an end to the Deng era. BRI underscores China's move onto the global stage and goes hand-in-hand with newfound diplomatic assertiveness and aggressive regional military buildup.

Broadly, BRI's land-based "belt" crosses from China to Central and South Asia, to the Middle East, and then to Europe. The sea-based "road" connects China with South Asia, the Middle East, East Africa, and Europe via sea-lanes that traverse the South China Sea, Indian Ocean, Red Sea, Suez Canal, and Eastern Mediterranean. But BRI's ambitions are not confined to just two geographic paths. Although plans for additional areas are less developed, China's vision includes Latin America, the Caribbean, the Arctic, and even outer space.

Two decades ago, China's entry into the World Trade Organization was promoted as key to spurring both economic and political liberalization. At the time it was also believed that liberal democratic governance was a precondition for economic success and sustainable technological advancement. Instead, China continued to pursue state-directed industrial policy, steal intellectual property, and maintain barriers to market access. One-party rule and the suppression of dissent remained staples of authoritarian governance. And though the sustainability of its debt-driven economic growth is certainly questionable, China has shown it can move from mere copying and assembly to innovation of advanced technology, even if it relies largely on theft of trade secrets and subsidies to its national champions to do so. Beijing wants to move from "made in China" to "made by China," and then to "invented by China."

Though the most visible manifestations of BRI are economic, it has clear strategic intent, aiming to increase China's influence over global politics and governance. Chinese leaders want to use BRI to revise the global political and economic order to align with Chinese interests. In a speech marking BRI's fifth anniversary in August 2018, President Xi emphasized that the initiative "serves as a solution for China to participate in global opening up and cooperation, improve global economic governance, promote common development and prosperity, and build a community of common human destiny." The phrase "common human destiny" is repeated throughout Chinese Communist Party speeches on BRI and makes clear the all-encompassing nature of Xi's goals.

Digital Silk Road, surveillance state

A central component of the BRI is the Digital Silk Road: China's plan for integrating the digital sectors of telecommunications (including the major companies ZTE, China Mobile, and Huawei), the Internet of Things, and e-commerce (Alibaba and JD.com) to create regional connectivity. The plan envisions a China-centric technological order, founded on Chinese exports of digital infrastructure such as cross-border optical cables and other communications networks, while setting the stage for the Chinese government amassing large datasets and manipulating political perceptions around the world. According to China's vice minister of industry and information technology, Chen Zhaoxiong, the Digital Silk Road will help "construct a community of common destiny in cyberspace," a phrase mirroring language China uses to describe its preferred vision for a global order aligned to Beijing's liking.

Where Chinese 5G equipment and connected products are used anywhere in the world, they could gain access to the private data of billions of people, enabling the Chinese government to collect private information about individuals' medical histories, spending habits, political views, personal details expressed on social media, physical location, financial situation, and more. Access to such information could be used in any

number of ways, including gaining a commercial or technical advantage in data-driven markets, targeting key individuals for recruitment by intelligence operations, or compromising political figures.

China is already employing an Orwellian application of technology to repress an entire population, as seen in the chilling actions of the Chinese government against the Uyghurs, a minority Muslim group, in Xinjiang province. Estimates of the number of Muslims in China being held in concentration camps run as high as two million people. Cultural and religious sites, such as mosques and cemeteries, are being demolished, and Uyghur women are being raped both inside and outside the camps. Beijing's repression in Xinjiang is increasingly enabled by a broad array of technology, including surveillance cameras, artificial intelligence, biometrics (such as voice samples and DNA), and facial recognition profiling. The nongovernmental organization Human Rights Watch has documented extensive use of technology to track and control the Uyghurs. It has reported that the Chinese government is installing QR codes on Uyghur homes in order to get instant access to the personal details of the people who live there. Leaving one's home by the back door instead of the front is deemed suspicious activity.

More broadly, through the Chinese government's system of "social credit scores," enabled by advanced communication technologies, the government is working to stamp out dissent and criticism of government officials and actions, and to promote conformity and loyalty to Chinese Communist Party ideology. By gathering information about individuals such as where they are traveling and with whom they are communicating, for example, the Chinese government is refining its ability to implement social controls. Already, some people in China are finding themselves unable to purchase airplane tickets, gain employment, or obtain housing based on their social credit scores.

A Chinese app known in English as "Study the Great Nation" and likened to Mao's "Little Red Book," released early in 2019, is already being used by one hundred million people. The app is designed to inculcate in people the views of China's leader, indoctrinating them with "Xi Jinping thought" and enforcing loyalty to the Chinese Communist Party. Chinese people are encouraged to download the app and use its exercises, earning points by reading articles, commenting positively on them, and taking quizzes about China and its leader. In some workplaces, use of the app is tied to wages, and the app is mandatory for Party officials and civil servants. It also provides a potential "backdoor" for the Party to log users' locations, calls, and contact lists, according to a report published by the German cybersecurity company Cure53. The app was developed by the Party's Propaganda Department with help from the Chinese company Alibaba. Code found in the app provides "superuser" access to smartphones, enabling the modification of files and installation of keystroke logging software. Users must agree to allow access to personal data, cameras, microphones, call logs, and locations in order to run the app.

The Chinese government's techno-nationalist policy has a goal of reducing the country's dependence on foreign—principally US—technology and then achieving technological superiority. It embraces technology as a central tool of illiberal governance, enhancing the effectiveness of surveillance, censorship, propaganda, and suppression of dissent, and also aims outward, seeking to export these technologies and the authoritarian model they enable. At the May 2017 Belt and Road Forum President Xi said, "We should advance the development of big data, cloud computing, and smart cities," all technologies advanced by 5G. The Digital Silk Road raises serious concerns about both information security and the expansion of the surveillance state beyond China's borders.

Controlling the playing field

Telecommunications are a central part of China's Belt and Road Initiative, raising alarm about both information security globally and the expansion of the Chinese surveillance state. Chinese telecommunications companies are expanding their efforts to build infrastructure, provide network services, and sell communications equipment in BRI countries. And, together with the equipment, countries are buying its standards. Through the combination of setting the standards and building the infrastructure, China controls the equipment, the technical assistance, and the ability to shape developing technology.

China is promoting the implementation of its national standards for 5G in countries along the Belt and Road. The Chinese companies Huawei, China Mobile, and ZTE are closely involved in developing 5G technology and have increased their participation in international standard-setting bodies for 5G. According to research by the Australian Strategic Policy Institute, as of April 2019, Chinese companies were involved in 52 5G initiatives in 34 countries.

Chinese control of underlying technical "laws" and architectural frameworks gives Chinese products, already developed to those standards, a competitive edge, puts Chinese companies in the prime position to provide technical assistance, and allows new technologies produced in China to be designed to meet those standards. The United States has long

benefited from its ability to set standards in a broad range of technical areas, including cell towers, mobile device communications, data centers, and smart utility networks. Now, BRI is intended to advance the adoption of Chinese technology standards in these and other areas such as high-speed rail, telecommunications, and energy. If these efforts are successful, they will create long-term reliance on Chinese intellectual property and technology, while disadvantaging US and other non-Chinese companies throughout the world.

In purely economic terms, the Chinese government's whole-of-government push to win the race for 5G is showing results. According to a report released by the multinational professional services firm Deloitte in August 2018, since 2015 China had built 350,000 new 5G towers, compared with 30,000 constructed by the United States. Factoring in differences in permitting costs and total market size, Deloitte projected that the United States had underspent China on 5G by about $24 billion over a three-year period. The four largest US mobile network operators would have needed to increase capital expenditures (including costs of 4G network maintenance, improvements, and new construction) by 16% over those three years to have kept up with China's pace of 5G deployment.

Although the United States will likely retain the lead in implementing some of the most complicated 5G technologies, China is well poised to pull ahead in general commercial rollout as well as become a global magnet for engineering talent. The sheer scale of China's 5G program and the government support provide significant cost advantages, as do well-established local supply chains and lower permitting costs. The Deloitte study estimates that "equipment necessary to add a telecommunications carrier in China is about 65% the cost of adding one in the United States." China's Ministry of Industry and Information Technology issued commercial 5G licenses to the country's three major state-owned telecom operators in June 2019. In November, all three launched commercial 5G networks, marking an accelerated deployment from China's original plans to launch in 2020. China Mobile, the country's largest network, is now live in 50 cities, with the other two networks planning to reach as many cities by the end of 2019. Measuring by number of 5G base stations, China is neck-and-neck with South Korea for the world's largest 5G network. Unsurprisingly, Huawei, which has close government ties and is China's leading telecommunications equipment provider, won half the contracts for 5G network equipment from China Mobile.

By comparison, US networks trail in breadth of coverage and speed. AT&T's 5G network is live, but only for commercial customers in parts of 21 US cities, as of November 2019. Verizon is close behind, with service offered in roughly 20 cities and plans to launch in 10 more by the end of 2019. T-Mobile has launched the United States' first nationwide network as of early December 2019, but this network relies on upgraded 4G equipment and is only slightly faster than the carrier's current 4G LTE network.

The Chinese government provides its state-owned telecommunication companies with an array of advantages as they move forward on domestic 5G implementation. For example, whereas US carriers bid $2.7 billion at auctions for 5G spectrum, the Chinese government provides virtually free bandwidth. The telecommunications operator Huawei does not disclose how much support it receives from the Chinese government. According to a Harvard Business School working paper, for a typical Chinese company in a technology-intensive sector, 22% of expenditures on research and development consist of government subsidies. Huawei, as a flagship Chinese company, likely receives more. And direct subsidies are not the only benefit tilting the playing field in Huawei's favor. It receives favorable financing deals backed by Chinese state-owned policy banks that can provide huge loans and guaranteed share of domestic contracts, not to mention reduced R&D costs through theft of intellectual property.

China controls the equipment, the technical assistance, and the ability to shape developing technology.

US companies are thus forced to compete on an uneven playing field, where Chinese companies can easily be the lowest bidder, often coming in with bids up to 30% lower than non-Chinese companies. In one case, Huawei underbid by 60% the Swedish company Ericsson in supplying the Dutch carrier KPN for 5G equipment, according to the *Washington Post*. Dutch authorities decided to use Huawei for less vulnerable segments of the network and stick to safer suppliers for the network's core. However, developing countries often cannot afford to take similar precautions, particularly because Chinese policy banks provide generous lending terms to countries that install Chinese telecommunications equipment.

Backdoors and hijacked data

The expansion of Huawei creates a number of concerns, not least of which are the vulnerabilities in its equipment that make it open to attack by hackers, the potential

collection of sensitive data through backdoors, and the company's legal obligation to deliver information to the Chinese government if asked. A report released in June 2019 by Finite State, a Columbus, Ohio-based cybersecurity firm, describes how Huawei telecommunications gear is far more likely than other companies' equipment to have flaws that can be leveraged by hackers for malicious use. Exploitation of known vulnerabilities, such as backdoors, could enable Huawei, or government or private hackers, to access a broad range of data. Such exploitation could allow unauthorized, malicious, and disruptive access to US critical infrastructure.

Data hijacking—the redirection of internet traffic and exfiltration of data—by Chinese telecom equipment is well documented. A handful of networks form the global backbone of the internet, and data generally get transmitted across the shortest route to their destination IP address. The routing process is determined behind the scenes through Border Gateway Protocol (BGP) tables, which show the closest network for data to flow through. In redirecting, the BGP is hijacked by a network that claims it is the closest network even if it is not. Hijack attacks are often difficult to detect, especially if they simply change the route, capture the data, then deliver it to its intended recipient. (It is also possible to intercept data and never forward it on). But in some cases, the geographical internet traffic routes—and the time the data spends in transmission—are far too disjointed to be accidental.

China is well poised to pull ahead in general commercial rollout as well as become a global magnet for engineering talent.

In 2016 and 2017, internet traffic was redirected from North America into China a number of times, as documented in a 2018 article by Chris Demchak of the US Naval War College and Yuval Shavitt of Tel Aviv University, published in *Military Cyber Affairs*. Redirected data to China disappeared into a black box, then came back out the other side and proceeded to its destination.

In October 2016, a major connection point in Los Angeles (where a long-distance telecommunications carrier connects to a local network and moves the local traffic to its destination), owned by a China Telecom subsidiary, was used to re-route bank data to China that was destined for Italy. In this case, the attackers attempted to reroute the traffic back to Italy, but failed. In another incident of data hijacking described by Doug Madory, director of an Oracle internet analysis unit, China Telecom "engaged in Internet traffic 'misdirection,'" impacting a large US infrastructure company.

As a large Chinese company, Huawei is required by law to have a Chinese Communist Party Committee, which influences corporate governance in parallel with the board of directors. Its role is to enforce the strategic and ideological goals of the Party. Huawei also benefits from subsidies and other advantages the Chinese state confers to national champions, including guaranteed domestic market share and market entry barriers for foreign competitors. Though Huawei claims that it would not turn over information to the Chinese government if it was asked to do so, Chinese law requires companies in China to help national authorities gather intelligence. For a telecom operator, the information could include anything transmitted over a Huawei network. In late July 2019, Czech Radio broke a story that cited former Huawei managers in the Czech Republic and Czech intelligence sources asserting that Huawei employees were required to collect sensitive and personal data on government officials and businesspeople. They claimed that the material, which was sometimes shared with officials at the Chinese Embassy, was entered into a central database that could be accessed by Huawei's headquarters in China.

The Henry Jackson Society in London recently analyzed a trove of twenty-five thousand resumes of Huawei employees and found that many mid-level technical personnel had strong backgrounds in work associated with intelligence gathering and military activities. Specifically, these employees had at least one of the following characteristics: "worked as agents within China's Ministry of State Security, worked on joint projects with the Chinese People's Liberation Army, were educated at China's leading military academy, and/or had been employed with a military unit linked to a cyber attack on US corporations." Countries purchasing 5G equipment from Chinese telecom operators do so at their peril.

Exporting techno-authoritarianism

Out of national security concerns, some countries, starting with Australia, have banned Huawei from their 5G network. The United States participates in an important, on-going surveillance and intelligence sharing arrangement, the Five Eyes (FVEY), with Australia, the United Kingdom, Canada, and New Zealand. If any of these countries chooses to allow Huawei into its 5G network, there are serious concerns that this will compromise the group's ability to share information securely.

Chinese-built 5G networks are spreading across Africa

and Latin America. Huawei has reportedly built about 70% of Africa's 4G networks and has signed a contract for South Africa's first commercial 5G network. It should be expected that Huawei's work in 5G across Africa will grow. The China-Africa Research Initiative at the Johns Hopkins University School of Advanced International Studies identified 47 different Huawei projects across Africa that were benefiting from subsidized loans. Of those, 45 were financed by the Export-Import Bank of China. Far beyond providing export credit to companies in the way the United States' EXIM Bank does, this goliath state financing vehicle extends credit to developing countries and Chinese companies in those countries, often to fund Chinese infrastructure construction. China's bank provides loans to favored sectors or causes that are often not commercially viable but represent a policy, security, or diplomatic priority to the Chinese government. As of 2018, it had $491 billion in outstanding loans—nearly 30 times that of the US EXIM Bank.

5G, with its faster download speeds and enhanced capacity, can be used for good and for ill. There are very real concerns that 5G networks could be used to sow confusion, seed misinformation, and disrupt normal activities in the event of a conflict. Even in liberal democracies, 5G networks may be used to collect information to try to silence dissent and undermine opposition. The export of Chinese equipment brings with it particular concerns about the export of Chinese techno-authoritarianism and the surveillance state.

To appreciate what's at stake, one need only look at Ecuador's smart policing system—built by Chinese companies, partly staffed by Chinese technicians, and financed by Chinese state loans. As of 2018, the nationwide network included 4,300 cameras and was being tested tests for the use of large-scale facial recognition. The system also includes the capability to track the location of mobile devices. During his visit to Ecuador in 2016, Xi Jinping visited the headquarters of the smart policing center, highlighting the role of Chinese surveillance equipment. Though Ecuador was a pioneer for China's export of wholesale surveillance systems, other South American countries have followed suit, and China is planning destinations for these technologies beyond that continent. In 2018, Xi Jinping called for further Chinese exports of "social stability" techniques to Middle Eastern countries.

The entire contents of the African Union's servers was being sent to servers in Shanghai.

In 2017, the computer system of the headquarters of the African Union—an assembly of 55 member states on the continent of Africa—in Addis Ababa was discovered by information technology technicians to be sending out large amounts of data at 2:00 a.m. nightly. The French newspaper *Le Monde* reported in 2018 that the data, said to have been the entire contents of the African Union's servers, was being sent to servers in Shanghai. The African Union headquarters had been designed and built by the Chinese and computer systems had been delivered turn-key—with backdoors in the system. The servers are believed to have been made by Huawei.

A Chinese state-owned company specializing in big data and artificial intelligence can mine the equivalent of five trillion words in 65 different languages every day from sources such as social and traditional media for use by China's national security apparatus, according to a report by the Australian Strategic Policy Institute. The information gathered could be used for a multitude of purposes, including tracking criticism of Chinese government actions, identifying sources of dissent, and targeting populations or individuals for cultivation as "friends" of China.

All is not lost ... yet

There are steps the US government can and should take now, including assessing supply chain risk, ensuring that the nation quickly and securely deploys a 5G network, and enhancing the review of exports and investments to protect the country's national security interests. The United States remains a leader in researching and producing cutting-edge dual-use technologies as well as some of the essential components in China's telecommunications expansion. In the wrong hands, both the technologies and the components could undermine United States' interests. Chinese firms may seek to acquire this intellectual property and know-how, as well as vital data on US citizens, through acquisitions of US companies.

US companies and consumers are very clearly at risk, as is the US military. Advanced technology is central to the ability of the nation's modern military to operate. As the Department of Defense considers how best to harness the immense bandwidth and potential inherent in commercial 5G systems, any possible risks associated with the use of Chinese equipment must get serious consideration. In an April 3, 2019, statement, six retired US senior military leaders expressed concern about a Chinese-developed 5G network, including its ability to provide near-persistent data transfer back to China. They pointed out that China's 2017 National Intelligence Law legally requires that "any organization or citizen shall

support, assist, and cooperate with" the Chinese security services. Using Chinese-developed networks to transfer military data is inherently risky and could endanger US military operations in locations around the world.

Acting out of both national and economic security concerns, the Trump administration has taken partial steps to limit or ban Huawei's purchase of US parts and components. In May 2019, Huawei was placed on the Entities List, administered by the Department of Commerce's Bureau of Industry and Security, which identifies companies and other organizations believed to be involved (or to pose a significant risk of becoming involved) in activities contrary to US national security or foreign policy interests. The administration's ban has been delayed three times with 90-day temporary licenses from the Department of Commerce, and companies have continued selling to Huawei through the waivers. In June 2019, President Trump announced at the G20 meeting that he was lifting some of the restrictions on Huawei. He said he would allow US companies to resume sales of their high-technology equipment to Huawei as long as the sales did not involve goods related to national security. According to media reports, Beijing demanded the removal of the US ban on the sale of US technology to Huawei as a precondition for reaching a trade deal.

Using Chinese-developed networks to transfer military data is inherently risky and could endanger US military operations.

The Department of Commerce has granted some waivers for US companies to sell Huawei products. At the time of writing it is not clear what criteria the department is using to make this determination, how many have been granted, and what the timeline is for future waivers.

China's techno-nationalist ambitions are still dependent on US technology, and experts disagree on whether the administration's actions will stymie Huawei's ability to deliver 5G. Some have estimated that Huawei had a large enough stockpile of parts and licensing agreements to get it through the end of 2019. Some companies have found ways to sell into China without labeling goods as originating from the United States. Moreover, stockpiles of networking gear may be sufficient to give Huawei enough time to find alternatives to US components, including homegrown substitutes.

The president's June announcement was not well received in Congress, where some senators have been adamant that Huawei is a national security threat and not a bargaining chip in trade negotiations. The 2019 National Defense Authorization Act (NDAA) prohibited purchases by federal government agencies of telecommunications equipment or services from China, including those produced by Huawei and ZTE, and of surveillance and telecommunications equipment produced by the Chinese companies Hytera, Hikvision, and Dahua. The administration released a preliminary version of an interim rule implementing this provision, and the rule went into effect on August 13. The House and Senate have recently agreed on language for NDAA 2020 that requires Huawei to remain on the entity list until other regulations are put in place to safeguard telecommunications infrastructure, and requires the Department of Commerce to issue a report on licenses granted for export to Huawei.

In an additional attempt to limit Chinese products from US telecommunications infrastructure, the Federal Communications Commission in November 2019 voted unanimously to deny subsidies from the $8.5 billion annual Universal Service Fund to companies purchasing Huawei and ZTE equipment, and proposed that the subsidy recipients be required to replace existing Huawei equipment in order to receive additional subsidies.

These efforts at oversight by the administration and the Congress are crucial. But more action is needed.

The US-China Economic and Security Review Commission, a bipartisan, congressionally chartered commission that I chaired in 2019, looked closely at 5G and the Internet of Things in its 2018 annual report and recommended that:

- Congress direct the National Telecommunications and Information Administration and Federal Communications Commission to (1) identify steps to ensure the rapid and secure deployment of a 5G network, with a particular focus on the threat posed by equipment and services designed or manufactured in China, and (2) determine whether any new statutory authorities are required to ensure the security of domestic 5G networks.
- Congress require the Office of Management and Budget's Federal Chief Information Security Officer Council to prepare an annual report to Congress to ensure that supply chain vulnerabilities from China are adequately addressed, particularly for Internet of Things-enabled technologies.

On a five-year and longer time horizon, the United States needs to think about how to ensure access to critical infrastructure, such as base stations and data centers, that is not produced in the United States, if

alternative, trusted suppliers Ericsson, Nokia, and Samsung do not continue to produce leading-edge technology. The nation must ramp up efforts in four areas.

1. Work with allies to develop new sources of critical technology. Outspending the Chinese government is not an option. Rather, the United States must collaborate with its allies and partners who share concerns to invest in the development of new sources of critical technology, from innovation through production. The Chinese government is transparent about the sectors of its economy it plans on building and about its use of a whole-of-government approach to achieve its goals. The United States needs its own whole-of-government approach, partnered with the private sector, to address the challenges. This approach must include participation by the Department of Defense, the Defense Advanced Research Projects Agency, the Defense Intelligence Unit, the intelligence community, the InQTel venture capital group, the Department of Commerce, the Federal Communications Commission, the National Institute of Standards and Technology, and the National Science Foundation, among others.

2. Formulate forward-looking industrial policy. It is past time for the US government to get over the allergic reaction to "industrial policy." With limited resources, decisions will need to be made about where to focus, and government must become more tolerant of risk—some innovation succeeds, some does not. Government investment in foundational research is essential to remaining competitive.

3. Support domestic companies whose products will be essential to the future of 5G. US companies critical to the development of 5G must remain economically vibrant; this will include Qualcomm, which leads in chips for 5G devices; Intel, which provides chips used in 5G network equipment; Cisco and Dell, which provide routers and switches used in network equipment; and HP, a leader in chips used in connected devices within the Internet of Things. In the face of China's pursuit of technological self-sufficiency, US firms face the loss of an important market, and, with that market, revenue vital for funding future R&D. The US government should work with these companies to identify and implement programs and policies that will best assist them in meeting the China challenge.

4. Play a leadership role in international standards-setting. Given the Chinese government's active pursuit of leadership in organizations that set standards, it is critically important for the United States to increase its engagement and participate vigorously in international organizations that set

Some senators have been adamant that Huawei is a national security threat and not a bargaining chip in trade negotiations.

standards and govern the internet. Chinese company representatives hold chair and vice-chair positions on 10 of the 56 decision-making panels at the 3GPP, the main 5G standards organization. The Chinese national Huolin Zhao was reelected Secretary General for the International Telecommunications Union in 2018 for a four-year term beginning in 2019. In November 2019, China nominated a candidate to lead the United Nations World International Property Organization, which sets the rules for international patents, trademarks, and copyrights. The United States must ratchet up its participation and leadership in the 3GPP, the International Telecommunications Union, the International Standards Organization, the International Electrotechnical Commission, the Internet Engineering Task Force, and the Institute of Electrical and Electronics Engineers Standards Association.

The security of individuals, companies, and governments across the globe relies on international collaboration in the setting of 5G standards and requires a vibrant private sector across countries and continents to supply secure physical infrastructure and software. Time remains for the United States, together with its allies, to lead this effort to create large 5G networks with the necessary cybersecurity, but the door is slowly closing.

Carolyn Bartholomew *was the chair of the congressionally chartered US-China Economic and Security Review Commission in 2019 and now serves as its 2020 vice chair.*

Recommended reading

Deloitte, "5G: The chance to lead for a decade" (2018).

Chris C. Demchak 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 (2018).

Finite State, "Supply Chain Assessment: Huawei Technologies Co., Ltd." (June 2019).

US-China Economic and Security Review Commission, *2018 Report to Congress* (Washington, DC: US Government Printing Office, 2018).

Lily Fang, Chaopeng Wu, Josh Lerner, and Qi Zhang, "Corruption, Government Subsidies, and Innovation: Evidence from China," Harvard Business School, working paper 19-031 (2018).