Securing Our 5G Future:

The Competitive Challenge and Considerations for U.S. Policy

November 2019

Elsa B. Kania

Bold. Innovative. Bipartisan.

1152 15th Street NW
Suite 950
Washington, DC 20005

CNAS.ORG / @CNASDC
T: 202.457.9400
F: 202.457.9401

ACKNOWLEDGMENTS

Thank you so much to Paul Scharre, Martijn Rasser, and Loren DeJonge Schulman for their very helpful comments and suggestions on the draft. I have greatly appreciated the insights of attendees of workshops convened through the "Securing Our 5G Future" project at the Center for a New American Security (CNAS) during the spring and summer of 2019. I am also grateful to all of the industry and government stakeholders who have provided input and feedback in the course of the writing and research. Thanks very much to Ainikki Riikonen and Megan Lamberth for their support and assistance with the project and in the process of finalizing this report. Any remaining shortcomings are the responsibility of the author alone.

ABOUT THE AUTHOR

Elsa B. Kania is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security. Her research focuses on Chinese military innovation and technological development. At CNAS, she contributes to the Artificial Intelligence and Global Security Initiative and the "Securing Our 5G Future" program. Ms. Kania was a 2018 Fulbright Specialist and is a Non-Resident Fellow with the Australian Strategic Policy Institute's International Cyber Policy Centre. She has been invited to testify before the House Permanent Select Committee on Intelligence, the U.S.-China Economic and Security Review Commission, and the National Commission on Service. Ms. Kania is a Ph.D. student in Harvard University's Department of Government, and she is a graduate of Harvard College.

ABOUT THIS REPORT

This report is produced as part of the CNAS project "Securing Our 5G Future," which explores the opportunities and challenges of 5G in a world of highly globalized and competitive innovation. This project is made possible because of support from AT&T, Qualcomm, and Samsung, who helped sponsor a series of workshops in the spring and summer of 2019 that contributed to informing this report.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Today's advances in fifth-generation telecommunications (5G) promise a transformational technology that is critical to enabling the next industrial revolution. 5G will provide massive benefits for future economic development and national competitiveness, including certain military applications. 5G is far more than simply a faster iteration of 4G. The benefits include its high speed, low latency, and high throughput, which enable data flows at vastly greater speed and volume than today's 4G networks. Future smart cities will rely on 5G, autonomous vehicles will depend on this increased connectivity, future manufacturing will leverage 5G to enable improved automation, and even agriculture could benefit from these advances. The advent of 5G could contribute trillions to the world economy over the next couple of decades, setting the stage for new advances in productivity and innovation.

The United States risks losing a critical competitive advantage if it fails to capitalize upon the opportunity and manage the challenges of 5G. Today, China seems poised to become a global leader and first mover in 5G. The United States may be situated in a position of relative disadvantage. The U.S. government has yet to commit to any funding or national initiatives in 5G that are close to comparable in scope and scale to those of China, which is dedicating hundreds of billions to 5G development and deployment. There are also reasons for serious concern about the long-term viability and diversity of global supply chains in this industry. Huawei, a Chinese company with global ambitions, seems to be on course to become dominant in 5G, establishing new pilots and partnerships worldwide.

The stakes are high because 5G will be a vital component of future critical infrastructure, presenting new risks and novel threats of disruption or exploitation. The current degree of consolidation in the industry exacerbates the risks of market failure. It is particularly concerning because Huawei's products and services have been assessed to be highly insecure, yet remain attractive to certain countries that fear falling behind in 5G and because of Huawei's ability to undercut competitors on price. However, the notion of a "race for 5G" is problematic and can be misleading. To ensure security will be more important than speed in establishing a durable foundation for 5G's future.

Although there are encouraging indications the U.S. government is starting to concentrate more on 5G, the policies to date have not yet proved commensurate with what is at stake. The Trump administration must also reframe and reorient its approach to competition in 5G, because the notion of "America first in the race to 5G" is not a winning strategy, nor should the aim of the United States be to deploy 5G as quickly as possible. U.S. policy should focus on promoting the security, collaboration, and healthy competition that are so vital to the future of 5G, in close collaboration with allies and partners.

Such a strategy should recognize that the U.S. government can and must play a critical role in promoting innovation through investing in 5G as a new foundation for American competitiveness in the fourth industrial revolution. Moreover, speed must not come at the expense of security, and future 5G networks should be secure by design from the start. An American 5G strategy should encompass five main lines of effort.

1. Prioritize and invest in 5G as a foundation for American competitiveness.

- Recognize the strategic significance of 5G and prioritize policy responses aimed at reinvigorating American technological leadership.
- Undertake government investment and incentivize private-sector investment in large-scale construction of 21st-century digital infrastructure, and explore a variety of options for collaboration between industry leaders and government to promote 5G development.
- Prioritize and accelerate existing initiatives to remove obstacles to commercial innovation, particularly sharing and, where necessary, reallocation of spectrum.

2. Ensure that future 5G networks will be secure by design from the start.

- Formalize a rigorous process for screening of vendors and carriers for U.S. 5G networks, and continue to promote collaboration between industry and government stakeholders on options for risk mitigation and security.
- Explore new approaches to establishing and maintaining greater visibility and situational awareness over U.S. 5G supply chains and the security practices of vendors and carriers.
- Develop a comprehensive framework for the assessment, mitigation, and management of the full range of systemic risks of future 5G networks.
- Recognize the vital importance of technical standards in shaping future technological developments, and incentivize improvements in security by prioritizing it as a requirement.
- Enhance the security of 5G networks and systems that involve high-risk or untrusted hardware and devices.

3. Contest leadership and technological innovation in and beyond 5G.

- Explore options to disrupt the status quo and innovate new approaches to 5G and beyond, including the use of greater network virtualization.
- Intensify support for research for new and innovative techniques to make more spectrum available, including through spectrum sharing.
- Urgently pursue efforts to build up and expand a healthy supply chain and industrial ecosystem in 5G.
- Promote the development of robust commercial ecosystems to enable new start-ups to leverage the full benefits of 5G.

4. Pursue deeper coordination and collaborative innovation with allies and partners.

- Prioritize cooperation with allies and partners to promote secure and collaborative alternatives for 5G development.
- Ensure that U.S. policies intended to constrain or challenge the global expansion and influence of Chinese technology companies are carefully balanced, messaged, and coordinated domestically among relevant stakeholders and internationally with allies and partners.
- Collaborate through NATO and with allies in the Indo-Pacific region to develop a secure and integrated communications architecture to facilitate information sharing and coordination.

- Collaborate with partners and allies on investments in the global development of digital infrastructure.

5. Prepare to leverage the positive and mitigate the negative externalities of 5G for national security.

- Prepare for the systemic risks of scenarios in which China continues to succeed in becoming a major player in global 5G networks.
- Evaluate the threats of disruption of critical infrastructure, as well as espionage and exploitation, involving and targeting 5G.
- Evaluate and experiment with the potential of 5G for defense and military applications.

5G has emerged as a key front in U.S.-China rivalry. Although the advent of 5G could greatly benefit the global economy and produce positive-sum outcomes, and its realization will require international cooperation and coordination to sustain global interoperability, it is undeniable the stakes are high. The outcome of this competition could shift the global center of gravity for growth and innovation. As a rising power, China has prioritized efforts to challenge American leadership in innovation. If successful in realizing its 5G ambitions, China could be poised to reshape the international technological ecosystem and capture major strategic dividends that will enhance its global power and influence. To compete, the U.S. government can and must contribute to catalyzing American innovation.

I. THE PROMISE OF 5G

Today's advances in fifth-generation telecommunications (5G) promise a transformational technology critical to enabling the next industrial revolution. This new generation of mobile communications constitutes a vital platform and digital backbone for massive increases in connectivity that will have far-reaching implications.[1] 5G is far more than simply a faster iteration of 4G; it represents a paradigm change.[2] The benefits of 5G include its very high speed, low latency, and high throughput. While the jump from 3G to 4G enabled the current mobile economy, the leap from 4G to 5G will open up entirely new economic opportunities and applications. 5G will enable data flows at vastly greater speed and volume than today's 4G networks, perhaps 100 or more times faster.[3] Future smart cities will rely on 5G, autonomous vehicles will depend on this increased connectivity, future manufacturing will leverage 5G for improved automation, and even agriculture could benefit from these advances.[4] The development and deployment of 5G are rapidly progressing, with a growing number of 5G pilots worldwide, including 92 pilots expected to launch in the United States by the end of 2019.[5] 5G technologies are on track for widespread commercialization in the 2020s and could generate great value across multiple industries.[6] American policymakers must recognize the imperative of leading in and embracing the potential of 5G to ensure future American competitiveness.

5G has emerged as a new frontier for U.S.-China rivalry. Today, China seems poised to become a global leader in 5G deployment and could succeed in seizing a key first-mover advantage in this industry.[7] The United States may be situated in a position of relative disadvantage, by some assessments.[8] However, the state of play in 5G is highly complex, and assessments of who is leading can vary,[9] depending upon the metrics considered.[10] The Trump administration has claimed, "America is now leading the global race to deploy secure and reliable 5G."[11] Typically, national competitiveness in 5G can be evaluated based on a number of factors, including the availability of spectrum, robustness of the overall industry players, investments in the construction of the requisite infrastructure for 5G, and commercial deployments of 5G networks.[12] U.S. carriers are moving more quickly to deploy "nonstandalone" 5G networks that build upon existing 4G infrastructure.[13] There has also been recent progress in making greater amounts of spectrum available in the United States, primarily in the high-band, namely mmWave, range.[14] By contrast, China has invested more heavily in the fiber and physical infrastructure required for standalone 5G, which could require intense capital expenditures. Chinese companies are primarily pursuing options for 5G involving midband spectrum, which might prove more promising for large-scale realization of 5G.[15] In 5G, the first movers and early adopters may benefit from being able to promote an industrial and commercial ecosystem designed to build upon their 5G networks.[16]

The question of who develops and controls the core technologies that are foundational for 5G has great significance for its future trajectory. Today, 5G remains at a fairly nascent stage in its development.[17] 5G is continuing to progress through groundbreaking research and inventions that resolve complex scientific issues involving speed, capacity, security, and reliability. The technical standards that will enable interoperability and facilitate the widespread commercialization of these technologies are still taking shape through the global standards-setting process known as the 3rd Generation Partnership Project (3GPP), a consortium of telecom associations and other organizations.[18] When it comes to the foundation of critical technology standards through which 5G is being defined, only a small subset of companies can be considered among the leading contributors to these standards based on the capabilities of their technologies, which involve technical documents

that establish new technology requirements and design solutions to meet those requirements. 5G standards establish the blueprint of this future communications infrastructure. Currently, in this process, key leaders include U.S.-based Qualcomm; China's champion, Huawei;[19] Nokia, headquartered in Finland; Ericsson, a Swedish company; and Samsung, a South Korean conglomerate, which are the major contributors to patents and standards. However, few American companies rank at present among the primary players in the construction of certain requisite equipment for 5G, particularly radio access networks.[20] The current degree of consolidation exacerbates the risks of market failure.[21] There are reasons for serious concern about the long-term viability and diversity of supply chains in this industry.

5G has the potential to provide benefits for future economic development. The advent of 5G may contribute trillions to the world economy over the next several decades,[22] setting the stage for new advances in productivity and innovation.[23] The hitherto unparalleled connectivity that 5G will provide is integral to realizing the full potential of the "internet of things" (IoT) and artificial intelligence (AI) technologies in the real world. 5G can enable new industries and contribute to a dynamic digital economy.[24] Moreover, 5G networks also possess promising military applications.[25] Such increases in speed and connectivity could facilitate data fusion and improved situational awareness to enhance command and control,[26] providing significant operational advantages on the future battlefield.[27] Given the importance of 5G for national competitiveness, it is hardly surprising that 5G is often characterized as a "race," even an "arms race," between China and the United States. However, 5G is more of a marathon, rather than a sprint, insofar as its operationalization will play out over at least a decade to come. In the process, security will be more important than speed in establishing a durable foundation for 5G's future. While the development and deployment of 5G are endeavors that involve intense rivalries among countries and companies, the realization of 5G equally requires cooperation and interoperability. U.S. strategy should concentrate on promoting the security, collaboration, and healthy competition that are so vital to the future of 5G.

II. THE CHINA CHALLENGE IN 5G

The Chinese government has been actively mobilizing to contest global leadership in 5G, while rapidly progressing in the nationwide deployment of this foundational technology. While the U.S. government has only recently started to concentrate on 5G,[28] the origins of China's efforts can be traced to as early as 2007, when the State Council approved a "major special project" on next-generation telecommunications,[29] pursuant to the National Medium- and Long-Term Science and Technology Plan Outline (2006-2020).[30] The United States had been relatively dominant in 4G, and China initially lagged behind and struggled more in 3G and 4G. Chinese leaders have been determined to leapfrog ahead in 5G through pursuing, and since arguably achieving, a first-mover advantage.[31] Concurrently, the Chinese government has undertaken significant investments in building up a more robust digital infrastructure of fiber optic networks that are important to facilitate the large-scale deployment of 5G.[32] China's science and technology plans and research initiatives, from the 863 Plan to "Internet Plus" and the National Strategic Emerging Industries Development Plan,[33] have supported advances in 4G and 5G. In China today, robust activities in research, development, and commercialization extend across universities, companies, and even a number of defense industry conglomerates.[34] Meanwhile, the IMT-2020 promotion group, established by the Chinese government in 2013, has coordinated efforts among state agencies and industry stakeholders to support research and development, as well as testing and standards, for

5G.[35] The Chinese government has also undertaken a proactive and coordinated approach to spectrum management and reallocation, involving military and industry stakeholders, to prepare for widespread 5G deployment through licensing and deconfliction of the requisite spectrum.[36] There are not only no comparable efforts in the United States but also no existing mechanisms to replicate and implement such a strategy.

China's efforts in 5G are estimated to amount to hundreds of billions of dollars across a combination of government funding and commercial investments.[37] Since 2015, China has outspent the United States by over $24 billion overall, according to one estimate.[38] This massive mobilization of resources has enabled rapid construction of the requisite infrastructure for standalone 5G, such as base stations, in which China Tower has proved to be a key player.[39] For 2019, China is planning to accelerate efforts in 5G and to dedicate 57 percent (or about $146 billion) of $256 billion planned spending on technology to 5G.[40] China is also launching a number of pilot projects to explore its potential across various industries, such as smart transport, industrial internet, and health care. As of 2019, 5G is already entering widespread precommercial deployment in a number of cities, including Beijing and Shanghai. For instance, the city of Shenzhen, which is home to Huawei, has become a major center for 5G development, intending to fully deploy 5G by late 2019.[41] By 2020, full commercial deployment is on track to launch. [42] Seemingly in response to U.S. pressures on Huawei and seeking to bolster its progress in 5G, the Chinese government has accelerated its timetable for issuing official licenses to China Mobile, China Unicom, and China Telecom, as well as China Broadcasting Network Corp., for mid-band spectrum.[43] Moreover, the Chinese government has provided carriers with low-cost spectrum and cheap land to facilitate deployment.[44]

The Chinese government and leading Chinese enterprises are actively promoting commercial deployment and experimentation with new applications of 5G. By 2025, an estimated 430 million people in China will have access to 5G, accounting for one-third of the world's total 5G users.[45] China is also developing early applications of AI and 5G applications in health care. In March 2019, the People's Liberation Army (PLA) General Hospital, in collaboration with China Mobile and Huawei, engaged in the world's first remote brain surgery using 5G.[46] The precise, real-time control that 5G provides can facilitate telemedicine at greater distances, which enables world-class surgeons to reach patients in rural or remote regions that lack the requisite medical services.[47] The Chinese government is also concentrating on applications of AI in industrial internet, including for advanced manufacturing.[48]

China's attempts to advance 5G still confront certain challenges, notably the discrepancy between the high expectations for 5G relative to the current maturity of the technology. For instance, despite the tremendous enthusiasm for its potential, 5G requires significant investments in the near term, but the future business models that will enable 5G to become profitable for operators remain unclear. For the 2020 to 2030 time frame, expenditures of Chinese network operators on 5G could reach $411 billion, according to an authoritative estimate from China's Ministry of Industry and Information Technology.[49] China's 5G era may be well underway, but the long-term trajectory of this state-driven approach to 5G remains to be seen. These sizable investments may be inefficient but could prove effective in driving development and establishing market predominance nonetheless.[50] The United States has yet to commit to any funding or national initiatives in 5G that are close to comparable in scope and scale.[51]

For China, Huawei is a national champion that has been at the heart of the 5G agenda from the start. Although it claims to be a private company, an assertion that has been challenged because its structure of ownership is opaque and contested,[52] Huawei has a history of strong state support and apparent linkages to the Chinese military and intelligence that start with its founder and persist to the present.[53] Since 2009, Huawei has invested massively in research and development of next-generation telecommunications.[54] The company plans to sustain and increase its investments in 5G with an annual R&D budget that may exceed $15 billion and could reach $20 billion in the years to come.[55] Huawei seems and claims to be on course to become dominant in 5G, establishing new pilots and partnerships around the world, from Asia to Africa and across much of Europe.[56] The company is building upon its established presence in 4G networks, which already amounts to nearly a third of the global telecommunications market.[57] Huawei is one of the few players for now that can provide mature, cost-effective equipment and systems integration for 5G, such as radio access networks and base stations. Huawei has shipped over 150,000 5G base stations worldwide as of June 2019.[58] Despite persistent security concerns, Huawei has continued to expand its reach, currently boasting a total of 50 commercial 5G contracts that span at least 30 countries, particularly a significant proportion in Europe.[59] Huawei has also signed a deal to develop 5G in Russia as of June 2019.[60] In addition, Huawei commands the greatest number of patents in 5G,[61] which amount to 1,529 in total as of late 2018, with the closest contender, Nokia, holding 1,397 patents.[62] However, estimates vary.[63] Of course, although these numbers are significant indicators of Huawei's prominence in 5G, pure patent counts should not be interpreted as an indication that Huawei is the clear leader, despite the company's claims to the contrary.[64] In this regard, although Huawei should be recognized as a formidable contender, its apparent leadership is hardly unassailable.

China may possess certain systemic advantages in 5G development and particularly deployment. The Chinese government has facilitated active and highly coordinated engagement in the establishment of global 5G standards, particularly through the IMT-2020 promotion group.[65] Huawei has clearly exerted a strong influence in the adoption of standards for 5G,[66] including those that benefit its own technologies. For example, Huawei particularly advocated for the adoption of Polar Code, a technique for the channel coding that is necessary to ensure accuracy, efficiency, and redundancy for data in digital communications.[67] Huawei has made 11,423 contributions to 5G standards,[68] while its wholly owned subsidiary HiSilicon has added 7,248 contributions, according to estimates from December 2018.[69] This compares with 10,351 from Ericsson, 6,878 from Nokia, and 4,493 contributions from Qualcomm.[70] It is important to remember that quantity is not always synonymous with quality or relative impact.[71] However, these numbers are certainly indicative of very forceful Chinese participation in the process, which has involved high-level representation from Chinese companies, their involvement in positions of leadership, and apparent coordination in promoting certain options.[72] By some accounts, Huawei is seen as a constructive contributor in a process that has been fairly collaborative.[73] Yet there have also been persistent concerns that Huawei has been attempting to "flood" the process,[74] including by taking on a high share of positions in decision-making on 3GPP panels, to establish unique sway.[75]

The Chinese government recognizes technical standards as a matter of strategic importance and has prioritized the promotion of Chinese intellectual property (IP) in the 3GPP 5G standards. This strong emphasis on shaping standards could facilitate successful deployment and commercialization of 5G technologies by Chinese companies that then might be poised to capture a sizable share of the profits and revenues in this critical industry. Moreover, progress in standardization is important to

facilitate interoperability, including the full leveraging of the potential of 5G to create related products and services. Meanwhile, there are efforts underway to formulate a new initiative, "China Standards 2035" (中国标准2035),[76] which could formally launch in 2020 and is intended to contribute to China's emergence as a "standards superpower" (标准强国).[77] This focus on standardization, from high-speed rail to artificial intelligence, is intended to increase the overall quality of China's economic development while facilitating the "going out" of Chinese companies and technologies.[78] An oft-quoted saying emphasizes, "First-class companies make standards, second-class companies do services, and third-class companies make products."[79] This contestation of standards continues China's quest to improve its "discourse power" (话语权) to exercise a "right to speak" and global influence commensurate with its growing economic and technological capabilities.[80] In particular, promotion of the "Digital Silk Road" could place Chinese companies, standards, and infrastructure at the center of the international information technology ecosystem, while perhaps serving as a vector for Beijing's global influence.[81]

Chinese advances in 5G also contribute to military innovation. The PLA aims to leverage emerging technologies to achieve an advantage in future military competition. In his capacity as commander-in-chief Xi Jinping, has called upon the PLA to become a "world-class" military (世界一流军队) by midcentury.[82] 5G will be vital to the process of military "intelligentization" (智能化), which involves the realization of AI in support of a range of applications and capabilities.[83] 5G could be critical to information support,[84] creating improvements in data sharing, new mechanisms for command and control, and enhanced system construction to fulfill future operational requirements,[85] such as the military internet of things.[86] 5G is anticipated to enable machine-to-machine communication among sensors, drones,[87] or even swarms on the battlefield, as well as improvements in human-machine interaction.[88] The potential for rapid integration of information and improved communications could provide key advantages for situational awareness. As China looks to construct a more integrated information and communications architecture across space- and ground-based systems, 5G could be incorporated.[89] For instance, there are plans to integrate 5G with BeiDou, China's dual-purpose competitor to GPS, to improve position, navigation, and timing capabilities.[90] Beyond the battlefield, deployment of 5G could facilitate China's model of national defense mobilization, providing for more "intelligent" approaches to coordinate resources and logistical support to fulfill the demands of wartime contingencies.[91] For instance, when Jilin Province carried out a drill for national defense mobilization, 5G was used to support emergency communications.[92] Already, some units in Chinese military and paramilitary forces have started to employ 5G for pilot programs, such as border security.[93]

China's development of 5G will be shaped by the implementation of a national strategy of military-civil fusion (军民融合).[94] There are certain synergies between military and commercial technologies, including advanced electronics in which elements of the Chinese defense industry, such as the China Electronics Technology Group Corp. (CETC), have particular proficiency.[95] Even some military academic institutions, such as the PLA Strategic Support Force's Information Engineering University, have noteworthy proficiency in relevant technological components, especially chips and advanced antennas.[96] The Information Engineering University, which contributes to the Chinese military's education and capabilities for information operations, is engaged in research on 5G network security, seemingly in collaboration with Huawei.[97] Increasingly, a growing number of companies, including Shenzhen Kingsignal (金信诺),[98] are pursuing opportunities for expansion into the military 5G market, including working on military projects.[99] In November 2018, a number of

industry players established the 5G Technology Military-Civil Fusion Applications Industry Alliance (5G技术军民融合应用产业联盟), including ZTE, China Unicom, and the China Aerospace Science and Industry Corp. (CASIC), a major defense conglomerate.[100] This new partnership aims to foster collaboration and integration in military and civilian development of 5G.[101] Some Chinese telecom companies are already supporting 5G pilot projects that appear to be intended for dual-use or military employment.[102]

III. 5G RISKS AND SECURITY CONCERNS

The U.S. government has actively sounded the alarm over the risks that Huawei may present, urging allies and partners to impose a ban against it in order to mitigate the threats of disruption or espionage through 5G networks.[103] Huawei has faced pushback and scrutiny, and a growing number of countries have considered—or undertaken in the case of Japan, Australia, and the United States, among others—a ban or *de facto* exclusion of Huawei on the basis of varying rationales and mechanisms, which have predated U.S. action in some cases.[104] There are also valid concerns that the outright exclusion of Huawei may slow and increase the costs of 5G deployment.[105] What has often been characterized as an American "campaign" targeting Huawei risks backfiring if continued on its current trajectory, in which U.S. rationales have been perceived as shifting and inconsistent.[106] However, a growing number of concerning incidents involving Huawei, including indicators of the insecurity of its equipment, accusations regarding its theft of intellectual property, and its involvement in providing surveillance capabilities to governments, continue to be exposed.[107]

China's quest for 5G dominance has played out within a complex technological and geopolitical landscape.[108] Indeed, different countries have their own security concerns and considerations, but not all share American assessments of the severity of these risks. Insofar as American policymakers see China as a great power rival and strategic competitor, allowing Chinese companies to play a key role in American critical infrastructure, or that of U.S. allies and partners, presents grave threats that are untenable and unacceptable for the United States, not only espionage but also outright subversion of this critical infrastructure.[109] Yet Huawei has continued to expand its global presence, and the U.S. government has yet to present a viable and attractive alternative to working with Huawei. Many countries may have sunk costs and be "locked in" already to this choice based on earlier decisions, which raises concerns about not only security but also fair competition.[110] However, it is encouraging to see emerging consensus among like-minded countries about potential principles and shared approaches to 5G security, particularly through the progress of a recent conference on 5G security in Prague.[111]

The age of 5G will present new risks and novel threats of disruption or exploitation. 5G involves far more than just new and faster wireless networks; it will be a vital component of future critical infrastructure. Consequently, the cybersecurity of 5G networks could prove uniquely challenging, considering the high levels of complexity and much greater potential for damage in the case of an attack. Not only the confidentiality of data on 5G networks but also questions of integrity and assurance will become urgent challenges. Whereas most cyberattacks to date have involved only data theft, an attack against future 5G networks could cause massive damage that might threaten public safety and critical industries in future smart cities.[112] The often subpar security of IoT devices, of which there are an estimated 20 billion globally and growing, also presents serious reasons for concern. A high proportion of devices on the U.S. market have been made in China by companies

with very poor track records on security.[113] While vulnerabilities have been and remain a major concern in the telecom industry for 3G and 4G, the stakes will be even higher for securing 5G networks at all stages of their life cycles.[114] In some cases, supply chains could be weaponized deliberately by adversaries that may prefer to "win without fighting."[115] The exclusion of high-risk vendors is an important measure to mitigate risk but does not constitute a complete solution.

5G must be designed and implemented with a holistic approach to security in mind from the start. The development of secure networks must entail more than simply excluding high-risk vendors, requiring rigorous, ongoing testing and screening. Indeed, careful scrutiny should be extended to all aspects of the production, construction, and management of these networks, involving screening of the security of all vendors and carriers. If an end-to-end approach to security is effectively implemented, 5G could prove more secure than our existing networks and critical infrastructure, but the consequences of insecurity would be far graver. In public debates on 5G security, the call and search for a "smoking gun" has been problematic. This framing of the issue has often distracted policymakers from thinking about the greater challenge of mitigating vulnerabilities that tend to be pervasive. Bugs can be just as problematic as backdoors. It is inherently challenging to differentiate an accidental vulnerability from one that is deliberately introduced. The primary difference is intent, which cannot be discerned from code alone. It is encouraging that the 3GPP's SA3 working group is focusing on security, seeking to ensure that such security concerns will shape the development of standards.[116] However, industry and government are just starting to grapple with the full range of issues in play.

Given the gravity of these security challenges, the apparent centrality of Chinese companies in the global development of 5G has raised intense concerns. There is a very real risk that vulnerabilities in networks, whether the result of poor security practices or deliberate introduction of backdoors, could be weaponized for leverage or coercive purposes, particularly in a crisis or conflict scenario. Considering China's history of IP theft and cyberespionage, there is also a real risk such networks could be exploited for purposes of espionage.[117] As a Chinese company, Huawei also would be subject to a number of legal demands, regulatory requirements, and mechanisms of coercion that are often ambiguous and expansive.[118] Regardless of whether Huawei's leadership may wish to disregard an order from the Chinese government, China lacks an independent judiciary system for company leaders to plead their case against the government, as Apple did in the United States when it fought an FBI order to unlock an iPhone. Huawei's claims that it would "say no" to the Chinese government are not credible without indications of the company's actual ability to do so.

Even if Huawei is given the full benefit of the doubt, despite its history and apparent involvement with the Chinese military and intelligence organizations, Huawei's products and services have been assessed to be highly insecure, with a much greater prevalence of vulnerabilities relative to their primary competitors.[119] Moreover, there are reasons to question whether knowledge of any bugs in its equipment could be shared more readily with China's Ministry of State Security (MSS). This risk may be heightened given the influence of MSS in China's vulnerabilities database, not to mention Huawei's historical and continued linkages to the Chinese People's Liberation Army, including military intelligence.[120] For the United States, these risks and security concerns are inextricable from today's geopolitical exigencies, insofar as the U.S.-China rivalry encompasses scenarios for which there is a nonzero probability of conflict, including over Taiwan. Consistently, Chinese military writings have highlighted the potential for cyberattacks on critical infrastructure as a prelude to

outright warfare.[121] The presence of equipment from high-risk vendors, such as Huawei, even in rural telecoms is concerning, considering that some of these networks are near military bases, which raises risks of espionage or exploitation.

5G security presents a global challenge that will demand creative and cooperative solutions. Huawei will likely remain a major player in 5G in a number of countries, including some U.S. allies and partners, that believe the benefits of partnering with it outweigh the risks. Although a criteria-based calculation of risk provides compelling arguments for exclusion of such highly risky players, many nations could still continue current collaborations with Huawei in ways that exacerbate global risks to this emergent ecosystem. Even if the United States were to succeed in fully securing its own 5G networks, U.S. data and entities may remain reliant, including for military and commercial activities, upon overseas digital infrastructure that could prove highly vulnerable. The presence of Huawei's equipment in the critical infrastructure of U.S. allies and partners, whose support or location as a staging ground the U.S. military might require to fulfill its treaty obligations in the event of a crisis or conflict, also creates new risks, to an extent that could undermine U.S. capabilities for command and control and power projection. As Dan Coats, had warned during his time as director of national intelligence (DNI), "U.S. data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service."[122]

Consequently, it is in the U.S. interest to develop and promote collaborative approaches to 5G security with allied and partner nations. Certainly, robust testing and rigorous oversight, such as the Huawei Cyber Security Evaluation Center that was established in the United Kingdom and comparable mechanisms created in Berlin and Brussels, constitute one alternative for risk mitigation. However, no such screening can provide a complete or perfect solution, particularly considering the inherent complexity of 5G.[123] Moreover, no amount of testing can enable full confidence, particularly when Huawei's involvement in the operation and maintenance of 5G networks would provide routine access that could be exploited. Huawei's apparent failure so far to meet these security standards and reports of the extent and severity of vulnerabilities in its equipment have not engendered confidence. There are reasons for skepticism that these paradigms will merit emulation.[124] Given the stakes, security cannot—and must not—be an afterthought in the process, nor a consideration to be sacrificed for the sake of cost or speed. Those countries that choose less secure options or prioritize ease and rapidity of deployment may encounter higher risks and greater costs in the future.

IV. CURRENT AMERICAN POLICY INITIATIVES IN 5G

Although there are encouraging indications the U.S. government is starting to concentrate more on 5G, policy responses have not yet been fully realized or proven commensurate with the opportunity and challenge. During the Obama administration, there were early efforts to apply lessons learned from U.S. success in 4G to progress in 5G. As early as 2010, the Federal Communications Commission (FCC) had issued a memo calling for freeing up 500 megahertz of spectrum for commercial employment,[125] which was followed by a 2013 memorandum to advance spectrum policy.[126] In July 2016, the Obama administration also launched the Advanced Wireless Research Initiative through the National Science Foundation (NSF), which had provided $400 million in funding for four 5G testbeds and research.[127] These policies have been since overridden by new measures introduced during the Trump administration. Concerningly, near the start of the Trump

administration, the FCC also repealed a requirement that the FCC had introduced during the Obama administration,[128] which had stipulated that 5G be secure.[129]

The Trump administration has started to concentrate on issues of 5G in response to its potential economic dividends and intense concerns about the competitive challenge from China. Initially, policy debates centered upon a plan for the nationalization of 5G networks, which has been consistently condemned and yet still recurred.[130] However, U.S. policy has started to progress toward more practical measures. In October 2018, the White House convened a 5G summit that called for a National Spectrum Strategy, which will concentrate on improving allocation of spectrum.[131] The National Telecommunications and Information Administration (NTIA) is working with a task force and seeking comments on the development of this agenda.[132] The FCC is also implementing its "5G Fast Plan," which is focusing on spectrum issues, updating policies on infrastructure, and modernizing regulations.[133] To date, most of the spectrum that has been auctioned has involved bands in the mmWave range,[134] whereas the spectrum that is most conducive to large-scale 5G deployment is midband spectrum, which has been less available so far.[135] There are also reasons to be encouraged about the progress of commercial deployments of 5G by U.S. companies.[136] However, certain options currently being marketed as 5G are not much faster or more capable than existing 4G LTE alternatives.[137]

5G has become a new driver of concern and competition in U.S.-China relations that has motivated ever more forceful responses in U.S. policymaking. In May 2019, the Trump administration issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain.[138] This measure may provide sweeping authorities to exclude technologies and transactions linked to "foreign adversaries." Although details of its implementation remain to be determined, it is likely that a number of Chinese companies, presumably Huawei among them, will be constrained by this measure. This latest policy comes in addition to the prior exclusion of ZTE and Huawei from government contracting, disincentives for U.S. carriers to work with them, and recently the exclusion of China Mobile from offering services in the U.S. market.[139] Significantly, the Commerce Department placed Huawei on its Entity List because of violations of U.S. sanctions on Iran,[140] barring U.S. companies from working with Huawei or its subsidiaries.[141]

It remains unclear how this measure will be implemented and to what extent U.S. companies will be partially or entirely restricted from exporting their products to Huawei over the long term. Despite its attempts to develop indigenous alternatives, Huawei remains highly dependent upon a number of U.S. and global suppliers, including Xilinx, Qualcomm, and Synopsys.[142] Although HiSilicon has achieved some initial successes in its own semiconductors, referred to as "spare tires" for the company,[143] China's difficulty in the manufacture of semiconductors remains a significant weakness,[144] often manifesting in the theft and targeting of foreign IP in this sector.[145] If the ban on sales to Huawei were to be fully enforced, the company would confront a deeply painful pathway ahead. However, Huawei's capabilities—and the Chinese government's determination to support this "national champion"—should not be underestimated.[146] Moreover, the uncertainty about the implementation of this measure, including because of the partial reprieve initially provided, not to mention the attempts of companies to circumvent these restrictions, indicates that Huawei may yet fight through.[147] At the same time, this measure risks causing collateral damage for a number of U.S. companies that have relied on sales to the China market for a noteworthy proportion of their revenues. It will be important to evaluate options to mitigate the potential impact of these negative

externalities, but the Trump administration has yet to address this issue. Ultimately, the net effect of this measure may be to accelerate Huawei's drive to achieve independence from American technologies.

Beyond these measures, the United States has yet to pursue more proactive policies to promote long-term leadership in 5G. There has not been extensive U.S. government investment in 5G technologies to date. Only limited research and development is occurring in American companies and universities, at least relative to the intensity and magnitude of efforts within China's technology ecosystem. The United States had led in 4G and LTE, yet a number of adverse trends in the telecom industry have weakened key players in the United States and Europe.[148] As a result of factors including deregulation and increased consolidation, unhealthy and uncompetitive dynamics have damaged the overall vitality of the industry, which some analyses have critiqued as tending toward oligopoly.[149] These trends have been exacerbated by Chinese industrial policies that have enabled Huawei to undercut its competitors in price. In the course of its rise, Huawei has received state subsidies that are estimated to amount to billions, including a $10 billion line of credit from the China Development Bank that was tripled to $30 billion in 2009 to enable its global expansion.[150] At present, few U.S. or European companies appear to be well-positioned to compete directly with Huawei in terms of providing scalable and cost-effective alternatives for certain of the key equipment, particularly in the radio access network.

However, there are also reasons to hope policy action and effective coordination could contribute to more favorable outcomes. The capability to shape and promote the development of these foundational technologies has paramount importance to the future of 5G. To date, American companies have primarily concentrated on nonstandalone 5G, which builds upon existing 4G infrastructure and may prove more viable commercially in the near term.[151] On the other hand, Chinese companies are actively pursuing standalone 5G, which could prove more transformative in the long term.[152] Given the cost and complexity of 5G technologies, their large-scale construction tends to require substantial investments beyond what may be incentivized by market forces alone, particularly for standalone networks.

V. POLICY RECOMMENDATIONS AND CONSIDERATIONS

The United States must prioritize and pursue a national strategy for 5G. To compete in 5G, the U.S. government must reframe and reconceptualize its approach. The notion of "America first in the race to 5G" will not work and is not a winning strategy,[153] nor should the aim of the United States be to deploy 5G "as soon as possible."[154] Instead, American strategy must promote a healthy, secure future in this fifth and future generations of telecommunications through competition and innovation in collaboration with allies and partners. The U.S. government can and must play a critical role in catalyzing innovation by investing in 5G as a new foundation for American competitiveness in the fourth industrial revolution. The United States must move quickly and be prepared to make significant adjustments, including on the allocation of spectrum. Yet speed must not come at the expense of security. U.S. policies must concentrate on ensuring that future 5G networks will be secure by design from the start. This proposed strategy involves five lines of effort.

1. Prioritize and invest in 5G as a foundation for American competitiveness.

Recognize the strategic significance of 5G, and prioritize policy responses that actively invest in reinvigorating American technological leadership. The White House should establish an interagency "Task Force on 5G Strategy" to concentrate on 5G security, deployment, and competitiveness. 5G should be elevated as a key priority that will require high-level attention and robust efforts and investments to augment existing initiatives. The United States must learn from its own history of constructive government involvement in funding and supporting research and development.[155] The U.S. government must not merely play defense in reacting to China's initiatives and advances in 5G, but rather must start proactively investing in American innovation.

Invest in large-scale construction of 21st-century digital infrastructure and explore options for collaboration between industry leaders and government to promote 5G development. Although commercial innovations have been and will remain a critical driver of 5G development, the U.S. government should take a more active role. The U.S. digital infrastructure required for 5G deployment is inadequate relative to the demands of 21st-century connectivity.[156]

- The U.S. government should explore options to assist the construction of 5G networks in major urban and rural centers. In the process, the United States can leverage new models of partnership and collaboration, such as funding and empowering state and local governments, while seeking to incentivize private-sector investment.[157]
    - The White House should organize an initiative through which cities and companies could develop joint proposals and receive funding to launch 5G pilots and projects with a combination of private and government investment.[158]
    - At the same time, closing the digital divide through investing in expanding connectivity to rural areas should remain a priority to enable equality of opportunity.[159]
- The U.S. government also should stimulate secure 5G deployment through procurement, including for military bases and training facilities. This initiative can build upon initial testing.[160]

Prioritize and accelerate existing initiatives to remove obstacles to commercial innovation, particularly sharing and, where necessary, reallocation of spectrum. 5G requires multiple elements of the spectrum, including not only mmWave but also options for midband (i.e., "sub-6") spectrum, which is important for deployment at scale.[161] Currently, the crowded character of U.S. spectrum, including usage by satellite companies and the military of this midband spectrum, presents significant impediments to 5G deployment and commercialization in the United States. A future U.S. spectrum strategy must be prepared to take urgent action to address this deficiency. Building upon recent sales of mmWave spectrum, the U.S. government should pursue options for sharing and freeing up additional spectrum resources as quickly as feasible.

- Current initiatives such as the FCC's 5G Fast Plan should be prioritized, sustained, and accelerated where appropriate,[162] particularly to address the relative disparity in the availability of sub-6 spectrum.[163]
- The U.S. government should prepare to actively engage in the International Telecommunication Union's (ITU) World Radiocommunication Conference (WRC-19)

in October 2019 on the basis of U.S. concerns and priorities about global issues of spectrum policy and its regulation.[164]

2. Ensure that future 5G networks will be secure by design from the start.

Formalize a rigorous process for screening of vendors and carriers for U.S. 5G critical infrastructure, and continue to promote collaboration between industry and government stakeholders on options for risk mitigation. U.S. policy can establish a stronger precedent for 5G security through a framework with clear criteria based on consensus and coordination with allies and partners. To date, the U.S. Department of Homeland Security (DHS) has initiated an Internet and Communications Technology Supply Chain Task Force that is starting this process of creating such criteria for assessment of risk, in collaboration with partners in industry.[165] The apparent emergence of initial consensus on these issues among the 32 countries that participated in the recent Prague 5G Security Conference also presents a promising initiative with momentum that should be sustained going forward.[166]

- The threat criteria to evaluate the risks associated with various vendors and carriers on the basis of objective standards and considerations should involve: the legal regimes within which companies operate, including rule of law and protections against arbitrary exercise of state power; their practices of corporate governance, including any linkages to foreign governments or military organizations; their ability to meet certain standards of security in technical evaluations; their transparency regarding responses to requests received from government organizations; their history of security practices, including any instances of flaws or vulnerabilities; their track record of adherence to IP protection, including any incidents of corruption or commercial espionage; and rigorous screening of the overall security of their supply chains, among others, leveraging automated techniques where feasible.[167] The vendors and carriers that are unable to meet certain standards could be partly or wholly excluded from U.S. 5G networks.

Explore new approaches to establishing and maintaining greater visibility and situational awareness of U.S. 5G supply chains and the security practices of vendors and carriers. The U.S. government should encourage the establishment of a mechanism to facilitate the sharing of information and intelligence on 5G security that might leverage public-private partnerships, among relevant industry and government stakeholders.[168] Such a center or "fusion point" might facilitate the sharing and integration of information and intelligence among critical players in the United States and with allies and partners to overcome existing market failures and regulatory obstacles.

Develop a comprehensive framework for the assessment, mitigation, and management of the full range of systemic risks to future 5G networks. The U.S. government should build upon ongoing initiatives in the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to concentrate on formulating standards and promoting best practices and methods for security evaluation.[169] Future progress can also leverage the FCC's initial formulation of best practices for 5G security via the FCC Communications Security Reliability and Interoperability Council (CSRIC), while reintroducing security as a requirement for U.S. 5G networks.[170]

- For high-risk vendors that already integrated into the U.S. supply chain and telecom ecosystem, CISA should undertake a systematic assessment of current levels of risk and potential countermeasures for a progressive transition to vendors with better security,

including compensation when necessary for replacement of high-risk or insecure equipment by smaller carriers.[171]

Recognize the vital importance of technical standards in shaping future technological developments, and incentivize improvements in security by prioritizing it as a requirement. China has emerged as a serious contender in this abstruse and technical, yet highly consequential, aspect of technological development, sometimes seemingly exploiting the standard-setting process. U.S. leadership in 5G will greatly depend upon promoting the development of foundational technologies taking shape through 3GPP.[172]

- The U.S. government should promote best practices in standardization on the basis of voluntary and consensus-based processes of governance that center upon the merit of technologies.[173]
    - The National Institute of Standards and Technology (NIST) should explore opportunities to contribute to convening and coordinating standards activities, including on security. For instance, NIST could expand the mandate and activities of its existing alliance for 5G networks to explore new options and directions.[174]
- The requirements of cybersecurity and methods to mitigate the risks of disruption must remain a core consideration, including the continued promotion of security standards for internet of things devices.[175]

Explore innovative solutions to enhance the security of 5G networks and systems that involve high-risk or untrusted hardware and devices. The United States should actively explore viable options for risk mitigation and management on future high-risk 5G networks, including the potential for default or standardized implementation of end-to-end encryption and greater network slicing, isolation, or segmentation.[176]

- The U.S. government should support research and projects that promote and demonstrate such techniques as secure network slicing. The employment of automated techniques to screen for vulnerabilities in supply chains also appears to be promising. In particular, solutions that leverage machine learning for intrusion detection on future 5G networks should be further explored and leveraged.[177]

3. **Contest leadership and technological innovation in and beyond 5G.**

Explore options to disrupt the status quo and innovate new approaches to 5G and for next-generation advancements. Today, 5G is still taking shape, pursuant to ongoing research and standards development.[178] Consequently, the United States should increase funding for research in next-generation telecommunications for the long term.

- This support for basic and applied research could extend to the establishment of new "centers of excellence" for advanced telecommunications at selected universities, augmenting current initiatives and partnerships undertaken under the auspices of NIST, such as its Alliance for 5G Networks.[179]
- The U.S. government should provide tax credits for the companies that are investing in 5G research and development.
- The U.S. government should expand and increase funding to the NSF's Advanced Wireless Research Initiative,[180] building upon the current project on Platforms for

Advanced Wireless Research (PAWR),[181] and ongoing research funded through the Office of Naval Research (ONR), among other institutions.[182]

- The U.S. government should organize a "5G Futures Challenge" via the Defense Advanced Research Projects Agency (DARPA) to incentivize innovative alternatives that may be less dependent on hardware in which Chinese companies have established advantage.
    - For instance, network virtualization for 5G appears promising.[183] This technique could possess advantages of lower costs and faster time to market, as well as potential military applications.[184]
- The Office of Science and Technology Policy should commission an independent assessment of all past and current research programs that the U.S. government and military research enterprises have funded in this field to identify key gaps and improve situational awareness of current strengths and weaknesses, in order to evaluate future priorities and research directions.

Sustain and intensify support for research on new and innovative techniques to make available more spectrum, including via spectrum sharing. Since the availability and challenges of reallocating spectrum remains a critical bottleneck to 5G development, the U.S. government should redouble current initiatives to develop new options for spectrum sharing, including through new approaches to coordinate and deconflict among military and commercial enterprises.

- NSF should consider launching a new program to fund academic research on spectrum sharing over the next five years. The model of NTIA's Spectrum Sharing Innovation Test-Bed should also be expanded to new localities and with new academic partners.[185]
- DARPA's Spectrum Collaboration Challenge has presented successful examples of new approaches to improve spectrum sharing,[186] leveraging automation and artificial intelligence to improve adaptability. Future initiatives should continue to build upon its initial successes.[187]

Promote the development of robust 5G industry and commercial ecosystems. NSF and FCC should jointly support "5G Incubators" for exploration of and experimentation with promising applications of 5G in academic research and by start-ups.

- FCC could partner with accelerators to provide local 5G platforms that start-ups could leverage to develop initial commercial applications, perhaps supported by a combination of federal and venture capital funding.
- The Department of Homeland Security's Office of Innovation and Collaboration, perhaps along with other government initiatives for venture capital, could direct investment to teams and start-ups with proposals for 5G security solutions and applications.[188]

Urgently pursue efforts to build up and expand a healthy supply chain and industrial ecosystem in 5G. At present, there are no American companies in 5G that can compete directly with Huawei in the radio access network. There are a small number of viable alternatives among current companies. The U.S. government should explore opportunities to diversify and rebalance its existing dependencies in

supply chains and vendors. It is important to mitigate dangerous dependencies or the vulnerability that any single player or source of equipment could be compromised by a potential adversary.

- The U.S. government must also promote and incentivize the development of greater capability for manufacturing of the specialized equipment required, considering the use of existing authorities, such as the Defense Production Act, where applicable.
- The U.S. government should actively support the Open Radio Access Networking Alliance (ORAN), facilitating transitions toward Software Defined Networks (SDN) and Network Function Virtualization (NFV) that support greater variety or diversification of the supply chain.[189]

4. Pursue closer coordination and collaborative innovation with allies and partners.

Prioritize cooperation with allies and partners to promote secure, collaborative alternatives for 5G development. In a world of globalized innovation, the development and deployment of 5G must involve and will require international cooperation. The United States should promote closer collaboration on security and development among partner nations and trusted companies. In addition, the U.S. government could expand collaborations with allies and partners on mechanisms for the review of investments and research partnerships, as well as the introduction of export controls where appropriate for advanced telecommunications and related technologies.[190]

Ensure U.S. policies to constrain or challenge the global expansion and influence of Chinese technology companies are carefully balanced, messaged, and coordinated domestically among agencies and internationally with allies and partners. U.S. attempts to highlight the risks presented by the global activities of Chinese technology companies must remain balanced and bolstered by the available evidence to achieve greater traction and legitimacy. If American security concerns are perceived as excessive or motivated by protectionism, then U.S. efforts to highlight real and serious issues may lose ground to Huawei's counternarratives and Chinese government propaganda.[191]

- To the extent possible, the U.S. intelligence community should share with allies or declassify and publicly release further evidence for these concerns regarding Huawei. American messaging can also leverage and highlight the full range of materials in the open source that reveal incidents of concern, including Huawei's linkage to a data breach at the African Union headquarters.[192]
- The Five Eyes intelligence-sharing partnership, in conjunction with like-minded nations that share similar concerns, should explore institutionalizing initiatives to facilitate rapid sharing of information and threat intelligence on risks involving the telecom industry.

Collaborate through NATO and with allies in the Indo-Pacific to develop a secure, integrated communications architecture to facilitate information sharing and coordination. For the United States, critical competitive advantage in any future conflict scenario requires capability to fight alongside allies and partners. However, divergences or asymmetries in trajectories for defense technological innovation could create new complications for future alliance interoperability, whether for communications in crisis scenarios or power projection during wartime contingencies.

- The U.S. military should explore options for collaboration with NATO partners on the development of dedicated 5G networks for secure communication, potentially under the aegis of the "Connected Forces Initiative."[193]

- The U.S. military should evaluate options to integrate 5G into the existing information and communications infrastructure for alliance coordination mechanisms with Japan and South Korea.[194]

Coordinate investments in the global development of digital infrastructure for next-generation connectivity. U.S. attempts to dissuade nations that are considering working with Huawei are impeded by the fact there are no viable or positive alternatives. The United States, along with allies and partners, should explore opportunities to partner on investments in telecommunications infrastructure to provide a viable alternative in price and accessibility to nations seeking options to build up their digital infrastructure, leveraging existing initiatives such as the BUILD Act.[195]

5. Prepare to leverage positive and mitigate the negative externalities of 5G for national security.

Prepare for systemic risks of likely scenarios in which China continues to succeed in becoming a major player in global 5G networks. Based on current trends, 5G networks that involve Chinese vendors and equipment will likely remain on track to become a major element of the global information technology ecosystem. The U.S. military and government must prepare to operate across and around networks that may be highly insecure, recognizing the risks inherent in such complex systems. Such adaptation will require rigorous evaluation of risks and exploration of options for the security and reliability of U.S. data passing through networks involving highly risky vendors and/or carriers.

- The U.S. government should explore alternative architectures to enable secure communications and intelligence sharing with allies and partners around the world despite riskier conditions, perhaps including improved standards for security, enhanced encryption, and increased network segmentation.
- The U.S. military must start to evaluate the full range of challenges of operating and projecting power in a demanding environment lacking access to telecommunications infrastructure. At worst, the U.S. military could be seriously hindered by such disruption in ways that could impede or undermine defense mobilization and operations.[196]

Evaluate the risks of disruption of critical infrastructure, as well as espionage and exploitation, involving and targeting 5G. In the near future, 5G technologies could not only exacerbate the risks of espionage but may also become the target of industrial espionage. In recent history, China's attempts to catch up with the United States technologically have often involved the theft and absorption of foreign technologies.[197] Huawei's initial success is alleged to have been enabled by an aggressive campaign of cyberespionage that targeted and undertook IP theft against the Canadian company Nortel, which contributed to its bankruptcy.[198] Although China's own indigenous capabilities in innovation have since increased considerably, continued initiatives to access international resources for innovation remain a priority and active line of effort. For instance, Huawei has actively funded research across a number of American and international universities, which has started to provoke some concerns about how such academic partnerships might be exploited to access innovative advances.[199]

- Given this track record and reasons for future concern, the DNI should commission a comprehensive assessment from a counterintelligence perspective of the range of risks to American and allied telecom companies and universities.

Evaluate and experiment with the potential of 5G for defense and military applications. The speed and connectivity that 5G enables will be vital to future battle networks. For instance, the Chinese military and defense industry have been actively exploring 5G, including through some initial pilot programs. The introduction of 5G for training purposes may support new techniques in live, virtual, and constructive (LVC) training that could be critical to preparing for future high-end conflicts.[200]

- The U.S. military should establish a target and time frame to introduce 5G pilots on bases and training facilities with the aim of integrating this next-generation connectivity into future command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) architectures and current training environments.
  - The National Training Center, as well as Army Futures Command and similar service-specific initiatives, such as AFWERX and the NavalX Agility Office, could organize war games, simulations, and exercises to test new concepts of operations and capabilities that could be enabled by 5G.[201]
- U.S. military research enterprises should consider scaling up current support for research related to 5G, exploring opportunities to expand collaboration with academic and industry stakeholders.
  - The Defense Innovation Unit and Strategic Capabilities Office should prioritize or introduce projects evaluating near-term and long-term options that might leverage commercial advancements in these technologies. Of course, the introduction of a new, untested, and perhaps vulnerable technology for military command and control also could create new risks, such that effort should proceed with great attention to concerns about assurance.

VI. CONCLUSIONS AND IMPLICATIONS

5G has emerged as a key front in U.S.-China rivalry. Although the advent of 5G could greatly benefit the global economy and produce positive-sum outcomes—and its realization will require international cooperation and coordination to sustain global interoperability—it is also undeniable that the stakes are high. The outcome of this competition could shift the global center of gravity for growth and innovation. As a rising power, China has employed a strategy that has prioritized efforts to challenge American leadership in innovation. If successful in realizing its 5G ambitions, China could be poised to reshape the international technological ecosystem. China has recognized this technological transformation as a historic opportunity to "surpass at a turning point" (弯道超车), through investing heavily in a new domain of technology in which the United States does not possess and may not be able to achieve decisive leadership.[202] 5G is so critical because it will prove a vital platform to realize the full potential of a range of frontier technologies, particularly artificial intelligence and all its multifaceted applications, which will converge and intersect in ways that may prove exciting and sometimes unexpected.

As the United States looks to embrace this fourth industrial revolution, the American approach must concentrate on proactively investing in and promoting future American competitiveness. It is critical to progress beyond the defensive or reactive responses to Chinese initiatives that have dominated recent U.S. policy conversations. Instead, U.S. policies and strategy for innovation must center on the basic and fundamental prerequisites that have contributed to America's history of success in science and technology. At first glance, the capacity for coordination and national mobilization that

are characteristic of an authoritarian approach to technological development may appear appealing and unachievable in the U.S. political economy. However, some of the most successful elements of China's present policies reflect adoption of approaches that are informed by a close study of and learning from the history of American innovation.[203] The combination of state-driven priorities and market-oriented competition have contributed to China's successes, despite obvious inefficiencies, but the apparent incursion of the Party-state upon the tech sector that is occurring under Xi Jinping as General Secretary of the Chinese Communist Party risks undermining future innovation.

Ultimately, the United States ought not to envy or seek to emulate China's model but should recognize that certain approaches to technology strategies can be effective if implemented in a manner that concentrates on catalyzing healthy competition. The U.S. government should contribute toward the future vitality and dynamism of American innovation through sustaining and increasing investment in basic research. Clearly, talent is also at the core of this technological competition. It will be critical to continue to expand opportunities for science, technology, engineering, and mathematics (STEM) education, while also recognizing the importance of immigration as a source of comparative advantage. Concurrently, significant investments in digital infrastructure will be vital for America's capability to leverage the full dividend of this fourth industrial revolution. The best responses to the challenge of competition with China must start at home. The United States should embrace this competition as an impetus for its own revitalization.

ENDNOTES

[1] For useful context on these technologies and the key policy considerations in play, see Jill C. Gallagher and Michael E. DeVine, "Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress," R45485 (Congressional Research Service, January 30, 2019), https://fas.org/sgp/crs/misc/R45485.pdf.

[2] For Huawei's conceptualization of this network architecture, see "5G Network Architecture: A High-Level Perspective," https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf.

[3] Although estimates vary, 5G is anticipated to reach and perhaps exceed speeds of 1,000 megabits per second.

[4] For examples, see Nell Lewis, Max Burnell, and Angelica Pursley, "How 5G will change the future of farming," CNN Business, April 1, 2019, https://www.cnn.com/2019/04/01/business/5g-farming/index.html.

[5] For a recent assessment, see "The Global Race to 5G Spring 2019 Update" (CTIA, April 2, 2019), https://www.ctia.org/news/the-global-race-to-5g-spring-2019-update.

[6] For one estimate of these time frames, see "Road to 5G: Introduction and Migration" (GSMA, April 2018), https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf.

[7] For one evaluation of China's prospects in 5G, see "China is poised to win the 5G race" (EY, 2018), https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf.

[8] For a recent assessment that provides a compelling accounting of such reasons for concern, see Milo Medin and Gilman Louie, "The 5G Ecosystem: Risks & Opportunities for DoD" (Defense Innovation Board, April 3, 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[9] For a positive perspective on China's prospects in 5G, see "China is poised to win the 5G race."

[10] For an assessment that provides a more optimistic perspective on the status of U.S. efforts in 5G, see "The Global Race to 5G Spring 2019 Update."

[11] The White House, "President Donald J. Trump Is Taking Action to Ensure that America Wins the Race to 5G," April 12, 2019, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-taking-action-ensure-america-wins-race-5g.

[12] These factors are adapted generally from a number of reports and relevant assessments.

[13] For one discussion of the potential trajectory of 5G in the United States, see "The 5G era in the US," (GSMA, 2018), https://www.gsmaintelligence.com/research/?file=4cbbdb475f24b3c5f5a93a2796a4aa28&download.

[14] Monica Alleven, "It's a wrap: FCC concludes first set of high-band auctions, raising $2.7B," FierceWireless.com, May 28, 2019, https://www.fiercewireless.com/wireless/it-s-a-wrap-fcc-concludes-first-set-high-band-auctions-raising-2-7b.

[15] "5G in China: Outlook and regional comparisons," (GSMA and CAICT, 2017), https://www.gsmaintelligence.com/research/?file=67a750f6114580b86045a6a0f9587ea0&download.

[16] For further details and this argument regarding network effects, see Dan Littmann et al., "5G: The chance to lead for a decade" (Deloitte, 2018) https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf.

[17] For a good basic primer on 5G technology, see Amy Nordrum, Kristen Clark, and IEEE Spectrum Staff, "Everything You Need to Know About 5G," January 27, 2017, https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g.

[18] "3GPP system standards heading into the 5G era," https://www.3gpp.org/news-events/3gpp-news/1614-sa_5g.

[19] For an earlier case study on some of the factors that have contributed to Huawei's success, see Nathaniel Ahrens, "CASE STUDY: Huawei," in "China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan" (Center for Strategic and International Studies, February 2013), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130215_competitiveness_Huawei_casestudy_Web.pdf.

[20] Brian Fung, "How China's Huawei took the lead over U.S. companies in 5G technology," *The Washington Post*, April 10, 2019, https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/?stream=top&utm_campaign=newsletter_axioschina&utm_medium=email&utm_source=newsletter&utm_term=.c627237c14d9.

[21] For on account of this dynamic, see Adam Janofsky, "U.K. Cybersecurity Official Says 5G Market Is 'Fundamentally Broken,'" *The Wall Street Journal*, June 6, 2019, https://www.wsj.com/articles/u-k-cybersecurity-official-says-5g-market-is-fundamentally-broken-11559839990.

[22] "The Mobile Economy 2019" (GSMA, 2019), https://www.gsma.com/r/mobileeconomy.

[23] For one of the most frequently referenced assessments of this economic impact, see Karen Campbell et al., "The 5G economy: How 5G technology will contribute to the global economy" (IHS Markit, January 2017), https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf.

[24] This white paper authored by an influential Chinese think tank highlights the economic and societal implications of 5G: "White Paper on the Economic and Societal Influence of 5G" [5G 经济社会影响白皮书] (Chinese Academy of Information and Communications Technology [中国信息通信研究院], June 2017), https://web.archive.org/web/20190330034647/http://www.caict.ac.cn/kxyj/qwfb/bps/201804/P020170711295172767080.pdf.

[25] For an initial discussion of the U.S. and Chinese militaries' interest in 5G, see Elsa B. Kania, "Why China's Military Wants to Beat the US to a Next-Gen Cell Network," DefenseOne.com, January 8, 2019, https://www.defenseone.com/ideas/2019/01/why-chinas-military-wants-beat-us-next-gen-cell-network/154009. For discussion of the potential of 5G in defense, see Medin and Louie, "The 5G Ecosystem: Risks & Opportunities for DoD."

[26] These advances will be critical to the realization of the internet of things (IoT) on the battlefield and deployment of artificial intelligence "at the edge." See, for instance, "Internet of Battlefield Things (IOBT)," February 7, 2017, https://www.arl.army.mil/www/default.cfm?page=3050.

[27] For initial discussion of Pentagon concerns regarding 5G, see C. Todd Lopez, "Pentagon Official: U.S., Partners Must Lead in 5G Technology Development," Defense.gov, March 26, 2019, https://dod.defense.gov/News/Article/Article/1796437/pentagon-official-us-partners-must-lead-in-5g-technology-development.

[28] It is worth noting that although 5G has only recently emerged as the subject of active policy debate, there were significant and ongoing initiatives launched in 2016 during the Obama administration. See The White House, "Fact Sheet: Administration Announces an Advanced Wireless Research Initiative, Building on President's Legacy of Forward-Leaning Broadband Policy," July 15, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/15/fact-sheet-administration-announces-advanced-wireless-research.

[29] For details on this initiative, see a recent update about it: ""New Generation Broadband Wireless Mobile Communication Network" National Science and Technology Major Special Project Press Conference" ["新一代宽带无线移动通信网"国家科技重大专项新闻发布会], Ministry of Science and Technology, January 6, 2017, http://www.nmp.gov.cn/tpxw/201701/t20170110_4869.htm.

[30] For the initial plan: "National Medium and Long Term Science and Technology Plan" (2006-2020) [国家中长期科学和技术发展规划纲要], Ministry of Science and Technology, February 9, 2006, http://www.most.gov.cn/mostinfo/xinxifenlei/gjkjgh/200811/t20081129_65774_9.htm.

[31] For context on the relative failure of China's efforts to promote its own preferred standards in 3G, see "China's 3G Technology Gamble: Who Has the Last Laugh?," Knowledge.Wharton.UPenn.edu, July 6, 2011, https://knowledge.wharton.upenn.edu/article/chinas-3g-technology-gamble-who-has-the-last-laugh.

[32] "Guideline to improve Internet speed, lower prices," State Council of the People's Republic of China, May 20, 2015, http://english.gov.cn/policies/latest_releases/2015/05/20/content_281475111283130.htm. See also "China to spend $182 billion to boost Internet by end of 2017," Reuters, May 20, 2015, https://www.reuters.com/article/us-china-internet-idUSKBN0O50JH20150520.

[33] "State Council Notice on the Issuance of the "Thirteenth Five-Year" National Strategic Emerging Industries Development Plan" [国务院关于印发"十三五"国家战略性新兴产业发展规划的通知], November 29, 2016, https://web.archive.org/web/20190408045526/http://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm.

[34] "MoST: 863 Plan Supported 5G Development, Investing 300 Million Yuan" [科技部：863计划支持5G发展投入逾3亿元], China Education and Research Network, November 11, 2014, http://www.edu.cn/zi_xun_1170/20141111/t20141111_1200437.shtml.

[35] For more on IMT-2020's recent activities, see its website: http://www.imt-2020.org.cn/zh/news.

[36] "Zhang Feng attended the radio management key work promotion symposium to emphasize the acceleration of the 5G system, etc. key frequency planning and licensing progress" [张峰出席无线电管理重点工作推进座谈会强调加快5G系统等重点频率规划和许可进度], *People's Post and Telecommunication Report* [人民邮电报], August 27, 2018, http://www.cnii.com.cn/hygl/2018-08/27/content_2097314.html.

[37] It is difficult to come up with a reasonable estimation of total spending or the extent to which announced investments will materialize and, if so, how efficiently. However, this range is a reasonable approximation for government programs that have provided funding and industry investments, as well as related spending on relevant equipment and digital infrastructure, such as fiber.

[38] Arjun Kharpal, "China has outspent the US by $24 billion in 5G technology since 2015, study shows," CNBC.com, August 7, 2018, https://www.cnbc.com/2018/08/07/china-outspent-us-by-24-billion-in-5g-technology-since-2015.html. See this report from Deloitte, which leverages its analysis and company financials to come up with this estimate: Littmann et al., "5G: The chance to lead for a decade."

[39] Laura He, "China Tower plans to speed up 5G network construction without increasing spending," *South China Morning Post*, July 24, 2018, https://www.scmp.com/business/companies/article/2156702/china-tower-plans-speed-5g-network-construction-without.

[40] Meng Jing, "China to push 5G commercialisation even as Huawei faces US-led resistance in West," *South China Morning Post*, March 25, 2019, https://www.scmp.com/tech/big-tech/article/3003104/china-push-5g-commercialisation-even-huawei-faces-us-led-resistance.

[41] "Shenzhen could see 5G in second half," *Asia Times*, April 16, 2019, https://www.asiatimes.com/2019/04/article/shenzhen-set-to-debut-5g-commercial-apps.

[42] "Shenzhen could see 5G in second half." See also Zhang Dan, "Central Beijing to get 5G in 2019 as network construction will cover strategic areas," *Global Times*, March 3, 2019, http://www.globaltimes.cn/content/1140765.shtml.

[43] The temporary licenses for 5G were issued in January 2019, and the estimate at that point was that official licenses would be issued in late 2019 and 2020. However, the Chinese government ended up issuing these official licenses as of June 2019. Ma Si, "Temporary licenses for 5G get govt nod," *China Daily*, January 1, 2019, http://www.chinadaily.com.cn/a/201901/11/WS5c37eb3ba3106c65c34e3d35.html; and Josh Horwitz and Sijia Jiang, "China issues 5G licenses in timely boost for Huawei," Reuters, June 5, 2019, https://www.reuters.com/article/us-china-telecom-5g/china-issues-5g-licenses-in-timely-boost-for-huawei-idUSKCN1T707T.

[44] Stu Woo, "In the Race to Dominate 5G, China Sprints Ahead," *The Wall Street Journal*, September 7, 2019, https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888.

[45] "China Mobile Internet Development Report: China's 430 million people will use 5G in 2025" [中国移动互联网发展报告：2025年中国4.3亿人将用上5G], *Beijing Nightly* [北京晚报], June 25, 2019, http://it.people.com.cn/n1/2019/0626/c1009-31195396.html.

[46] "First remote surgery in China conducted using 5G technology," *Global Times*, March 17, 2019, http://www.globaltimes.cn/content/1142340.shtml.

[47] For instance, in June 2019, Beijing Jishuitan Hospital completed the world's first 5G remote operations using robotic systems for orthopedic surgery. "The first multi-center 5G teleoperation was completed" [首例多中心5G远程手术完成], *Beijing Daily*, June 28, 2019, http://www.xinhuanet.com/info/2019-06/28/c_138180254.htm.

[48] "China should accelerate the pace of 5G commercial use with the industrial Internet as a breakthrough" [中国应以工业互联网为突破口加快5G商用步伐], China News Network [中国新闻网], June 25, 2019, https://web.archive.org/save/http://it.people.com.cn/n1/2019/0626/c1009-31195331.html.

[49] Bien Perez, "Why China is set to spend US$411 billion on 5G mobile networks," *South China Morning Post*, June 19, 2017, https://www.scmp.com/tech/china-tech/article/2098948/china-plans-28-trillion-yuan-capital-expenditure-create-worlds. For the original sourcing, see "White Paper on the Economic and Societal Influence of 5G" [5G 经济社会影响白皮书].

[50] Li Mengyan [李孟研] and Wang Renfei [王任飞], "The curtain is open, the 5G era is really coming" [大幕开启, 5G时代真的要来了], China Military Network, January 18, 2019, http://www.81.cn/jfjbmap/content/2019-01/18/content_225613.htm.

[51] For instance, the Rural Digital Opportunity Fund that was recently announced does constitute a noteworthy undertaking but consists primarily of funding that was repurposed from the Universal Service Fund. For reporting on the topic, see Brian Fung, "5G is about to get a big boost from Trump and the FCC," *The Washington Post,* April 12,

2019, https://www.washingtonpost.com/technology/2019/04/12/g-is-about-get-big-boost-trump-fcc/?utm_term=.79b5447a385f.

[52] For recent research on this issue, see Christopher Balding and Donald C. Clarke, "Who Owns Huawei?," May 8, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

[53] For the investigation that prominently highlighted these concerns, including the respective connections of Huawei's founder and former chairwoman to the Chinese military and Ministry of State Security, see "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[54] As of 2017, Huawei noted in its annual report that it had spent over $60.4 billion on research and development over the past decade. "Huawei's 2017 Annual Report: Solid Performance and Lasting Value for Customers," March 30, 2018, https://www.huawei.com/us/press-events/news/2018/3/huawei-2017-annual-report. To some extent, this spending has been enabled by funding from China's military and intelligent organizations: Andrew Liptak, "The CIA says that China's security agencies provided funds for Huawei: report," TheVerge.com, April 20, 2019, https://www.theverge.com/2019/4/20/18508915/cia-huawei-china-security-agencies-funds-report.

[55] Sijia Jiang, "China's Huawei to raise annual R&D budget to at least $15 billion," Reuters, July 26, 2018, https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169.

[56] For context, see Keith Johnson and Elias Groll, "The Improbable Rise of Huawei," *Foreign Policy* (April 3, 2019), https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china.

[57] Dell'Oro Group, "Key Takeaways – Worldwide Telecom Equipment Market 2018," March 4, 2019, http://www.delloro.com/delloro-group/telecom-equipment-market-2018.

[58] "Huawei ships over 150,000 5G base stations worldwide," Xinhua, June 27, 2019, http://en.people.cn/n3/2019/0627/c90000-9591819.html.

[59] Sherisse Pham, "Huawei is still signing up 5G customers despite US pressure," CNN, June 26, 2019, https://www.cnn.com/2019/06/26/tech/huawei-ken-hu-mwc/index.html; and Julia Horowitz, "European companies want to do business with Huawei. That just got harder," CNN, April 30, 2019, https://edition.cnn.com/2019/04/30/business/huawei-vodafone-europe/index.html.

[60] Andrew Kramer, "Huawei, Shunned by U.S. Government, Is Welcomed in Russia," *The New York Times*, June 6, 2019, https://www.nytimes.com/2019/06/06/business/huawei-russia-5g.html.

[61] "Who is leading the 5G patent race?," IPlytics, December 12, 2018, https://www.iam-media.com/who-leading-5g-patent-race.

[62] Chen Qingqing, "Huawei leads in patent applications as R&D investment edge helps withstand US crackdown," *Global Times*, March 19, 2019, http://www.globaltimes.cn/content/1142707.shtml.

[63] According to another calculation from late 2018, Huawei has 933 standard-essential patents and ZTE has 796, both ranking behind Samsung, which has 1,166, and ahead of Ericsson with 794 and Qualcomm with 730: "Who is leading the 5G patent race?," IPlytics.

[64] Ma Si, "Restriction will hurt US, Huawei says," *China Daily*, May 16, 2019, http://www.chinadaily.com.cn/a/201905/16/WS5cdcc5daa3104842260bbfa7.html. While also an imperfect measure, citation-weighted patent counts are typically recognized as a more reliable proxy for the value of patent portfolios.

[65] For more on IMT-2020's recent activities, see its website: http://www.imt-2020.org.cn/zh/news.

[66] As of mid-2018, representatives from Chinese companies held 10 of the 57 chairman and vice chairman positions on 3GPP panels. Newley Purnell and Stu Woo, "China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns," *The Wall Street Journal*, March 30, 2018, https://www.wsj.com/articles/washington-woes-aside-huawei-is-determined-to-lead-the-way-on-5g-1522402201.

[67] For some of the controversy around the adoption of Polar Code, see Frank Hersey, "Lenovo founder in public backlash for 'unpatriotic 5G standards vote,'" TechNode.com, May 16, 2018, https://technode.com/2018/05/16/lenovo-huawei-5g.

[68] "Who is leading the 5G patent race?" IPlytics.

[69] Sarah Feldman, "Huawei Is Leading the Race to Develop 5G," Statista.com, May 22, 2019, https://www.statista.com/chart/17536/mobile-network-standards.
[70] "Huawei Is Leading the Race to Develop 5G."
[71] Todd Shields and Alyza Sebenius, "Huawei's Clout Is So Strong It's Helping Shape Global 5G Rules," Bloomberg, February 1, 2019, https://www.bloomberg.com/news/articles/2019-02-01/huawei-s-clout-is-so-strong-it-s-helping-shape-global-5g-rules. For a discussion of some of the drawbacks of counting contributions in the 3GPP process, see "Top 5 drawbacks of "contribution counting" in 3GPP. (Don't count on it!)," OnQ Blog on Qualcomm.com, https://www.qualcomm.com/news/onq/2017/08/02/top-5-drawbacks-contribution-counting-3gpp-dont-count-it. Indeed, these counts of contribution can be misleading as a metric and should not be evaluated as an indication of relative technological leadership across companies. This count includes all kinds of contributions, including editorial comments and incremental revisions, all of which receive an equal weight without differentiation of quality or impact.
[72] The Chinese government has learned from the failure of prior efforts to push for the adoption of an indigenous standard known as TD-SCDMA for 3G and then TD-LTE for 4G.
[73] Monica Alleven, "Huawei maintains seat at standards table despite geopolitical woes," FierceWireless.com, February 28, 2019, https://www.fiercewireless.com/wireless/huawei-maintains-seat-at-standards-table-despite-geopolitical-woes.
[74] "Warner, Rubio Ask Intelligence Community for Public Report Detailing Chinese Participation in 5G Standard-Setting," U.S. Senator Mark R. Warner, press release, March 1, 2019, https://www.warner.senate.gov/public/index.cfm/2019/3/warner-rubio-ask-intelligence-community-for-public-report-detailing-chinese-participation-in-5g-standard-setting.
[75] For one discussion of this topic, see Parv Sharma, "5G Ecosystem: Huawei's Growing Role in 5G Technology Standardization," Counterpoint Research, August 20, 2018, https://www.counterpointresearch.com/huaweis-role-5g-standardization.
[76] For initial discussion of the initiative, see "National Standards Commission: Currently Developing "China Standards 2035"" [国家标准委：正制定《中国标准2035》], China News Network, January 10, 2018, http://www.xinhuanet.com/fortune/2018-01/10/c_129787658.htm.
[77] "National Standards Commission: Currently Developing "China Standards 2035."" See also how this emphasis on standardization is being applied to the implementation of military-civil fusion: "Standardizing Military-Civil Fusion "Qingdao Consensus" Released" [标准化军民融合"青岛共识"发布], *Sc&T Daily*, December 20, 2018, https://web.archive.org/save/https://finance.sina.com.cn/roll/2018-12-20/doc-ihqhqcir8616896.shtml
[78] "Standards boost the high-quality development of China's economy" [标准助推中国经济高质量发展], *Workers Daily* [工人日报], June 13, 2019, http://finance.people.com.cn/n1/2019/0613/c1004-31134458.html.
[79] "一流企业做标准，二流企业做服务，三流企业做产品," and see, for instance, "5G Patent Competition Escalates; Chinese Companies Compete to Increase Investments" [5G专利竞争升级 中国企业竞相加大投入], Shanghai Securities News [上海证券报], December 19, 2017, http://webcache.googleusercontent.com/search?q=cache:jsaVSWvmj4EJ:news.xinhuanet.com/2017-12/19/c_1122132724.htm+&cd=10&hl=en&ct=clnk&gl=us.
[80] For context on the concept of discourse power, see this initial analysis: Elsa B. Kania, "The Right to Speak: Discourse and Chinese Power," Party Watch, November 27, 2018, https://www.ccpwatch.org/single-post/2018/11/27/The-Right-to-Speak-Discourse-and-Chinese-Power.
[81] See the author's prior writings on the subject for a more detailed discussion, including: Elsa B. Kania, "China's play for global 5G dominance—standards and the 'Digital Silk Road,'" The Strategist, June 27, 2018, https://www.aspistrategist.org.au/chinas-play-for-global-5g-dominance-standards-and-the-digital-silk-road.
[82] See a number of articles in *PLA Daily* and a number of PLA publications that have discussed this issue, including "The 5G era is coming! Military communications can reach nearly unobstructed standards" [5G时代来临！军队通讯可达到近乎无阻碍的标准], China Military Network, March 27, 2017, http://www.81.cn/jwgz/2017-03/27/content_7539515.htm.
[83] For a more detailed assessment of China's approach to artificial intelligence in warfare, see Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power" (Center for a New American Security, November 2017), https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.
[84] For earlier discussion in Chinese military media, see "5G Era: Military Intelligentization Will Refresh the Form of the Battlefield" [5G时代：军事智能化将刷新战场形态], China National Defense Report [中国国防报], March 27, 2017,

https://web.archive.org/web/20190414200822/http://www.mod.gov.cn/mobilization/2017-03/27/content_4776647_2.htm.

[85] Zhang Qingliang [张清亮] and Zhang Guoning [张国宁], "5G Promotes the Acceleration of Military Intelligentization" [5G推动智能化作战提速], China National Defense Report [中国国防报], March 12, 2019, http://www.81.cn/gfbmap/content/2019-03/12/content_229076.htm.

[86] Hao Yaohong [郝耀鸿], "5G, One Step Closer to the Military Internet of Things" [5G, 离军事物联网更近一步], *Confidential Work*《保密工作》, July 2017, http://www.cnki.com.cn/Article/CJFDTotal-BMGZ201707033.htm. Hao Yaohong is an expert on military communications with the PLA Special Operations Academy (特种作战学院).

[87] "5G UAV Application White Paper" [5G无人机应用白皮书], IMT-2020 Promotion Group [IMT-2020(5G)推进组], August 2018, http://www.caict.ac.cn/kxyj/qwfb/bps/201809/t20180928_186178.htm.

[88] Wang Peng [王鹏] "The Military Applications of 5G Communications Technology" [5G通信技术的军事应用], *China Youth Report* [中国青年报], January 17, 2019, http://www.xinhuanet.com/mil/2019-01/17/c_1210040454.htm. The author of this piece is affiliated with the PLA Air Force Engineering University (空军工程大学).

[89] For an example of research from a research institute of the China Electronics Technology Group Corp. (CETC) on this concept, see Xu Quansheng [徐全盛], Zou Qinyi [邹勤宜], and Ge Linqiang [葛林强], "Research on Tactical Communication with Air-Ground Integration Based on 5G" 基于5G的天空地一体化战术通信研究], Communication Technologies《通信技术》, February 2016, http://www.cnki.com.cn/Article/CJFDTotal-TXJS201602017.htm.

[90] "Director Chen Mingbo went to Qianxun SI to investigate the development of "Beidou +5G" military-civil fusion applications" [陈鸣波主任今赴千寻位置调研"北斗+5G"军民融合应用发展情况], June 14, 2018, http://www.sheitc.gov.cn/zxxx/678101.htm.

[91] "How does national defense mobilization embrace the 5G era?" [国防动员如何拥抱5G时代], China Military Network, June 27, 2018, http://www.81.cn/gfbmap/content/2018-06/27/content_209482.htm.

[92] "When communication is paralyzed, can the PLA resume command using 5G?" [通讯陷入瘫痪，解放军能不能用5G恢复指挥？], CCTV, June 17, 2019, http://military.cctv.com/2019/06/17/ARTIQE70Hgi9NzGxbt1OrXIh190617.shtml.

[93] Minnie Chan, "China to use 5G technology to tackle flow of refugees, smuggled goods over North Korean border," *South China Morning Post*, April 8, 2019, https://www.scmp.com/news/china/diplomacy/article/3005285/china-use-5g-technology-tackle-flow-refugees-smuggled-goods.

[94] This term (军民融合) can also be translated as "civil-military integration." In practice, this strategy extends not only to technological development but also to talent cultivation and national defense mobilization, among other initiatives.

[95] For instance, a division of CETC held a training program on 5G for military-civil fusion in collaboration with Xidian University: "CETC Northwest Group Co., Ltd. Organized "5G Key Technologies and Military-Civilian Fusion Applications" Training" [中电科西北集团有限公司举办"5G关键技术及军民融合应用"培训], Sohu, March 24, 2019, https://web.archive.org/save/https://www.sohu.com/a/303429803_808513.

[96] This research on a chipset for visible light communication that could contribute to future 5G architectures was undertaken by the PLA Strategic Support Force's Information Engineering University in collaboration with other units from academia and industry: "The world's first commercial-grade ultra-wideband visible light communication specialized chipset was successfully researched and developed" [全球首款商品级超宽带可见光通信专用芯片组研发成功], China Military Online, August 25, 2018, http://www.81.cn/jfjbmap/content/2018-08/25/content_214300.htm.

[97] The sources describing this project are available upon request.

[98] "The domain of military-civilian fusion has added a lot of strength, Shanghai Haoxun sprints to an IPO" 军民融合领域再添猛将，上海瀚讯冲刺IPO], March 15, 2019, http://www.3snews.net/domestic/244000055546.html. For an English-language description of the company, see "Shanghai Haoxun Technologies Inc.," SIMIC Holdings, http://www.simicholdings.com/changeLang?url=http://www.simicholdings.com/industry/industryFours/2b40e8df1c824aa1b94c39db1c372980?v=4. KingSignal also has a presence in the U.S. market. "Telco Source Connect Opens Kitting and Fulfillment Center in Dallas to House High-Performance Connectivity Products from Kingsignal," February 29, 2019, https://markets.businessinsider.com/news/stocks/telco-source-connect-opens-kitting-and-fulfillment-center-in-dallas-to-house-high-performance-connectivity-products-from-kingsignal-1027946009.

[99] "Kingsignal brings a signal interconnection system and underwater integrated system to debut at the 12th China Air Show" [金信诺携信号互联系统及水下综合系统亮相第十二届中国航展], Sohu, November 7, 2018, http://webcache.googleusercontent.com/search?q=cache:g81f9BBT81EJ:business.sohu.com/20181107/n554644010.shtml+&cd=1&hl=en&ct=clnk&gl=us. It is also worth noting that Kingsignal has recently entered the U.S. market.

"Telco Source Connect Opens Operations Hub-Fulfillment Center in Dallas, Texas," Area Development News Desk, February 13, 2019, http://www.areadevelopment.com/newsItems/2-13-2019/telco-source-connect-fulfillment-center-dallas-texas.shtml.

[100] "5G Technology Military-Civil Fusion Applications Industry Alliance Established in Beijing" [5G技术军民融合应用产业联盟在北京成立], *Economic Network* [经济网], November 5, 2018, http://www.ceweekly.cn/2018/1105/239477.shtml; and "CASIC: Promoting the application of 5G technology in the military and civilian fields" [航天科工：推动5G技术在军民领域的应用], Economics Daily [经济日报], November 2, 2018, http://www.ce.cn/xwzx/gnsz/gdxw/201811/02/t20181102_3069I220.shtml.

[101] China has also been seeking to improve coordination between military, government, and commercial stakeholders in spectrum management. This coordination seems to occur primarily between the Ministry of Industry and Information Technology and the Central Military Commission Joint Staff Department (CMC JSD), particularly the JSD Information and Communications Bureau, or former Informatization Department. "Ten Major Events in Radio Management in 2018" [2018年无线电管理十件大事], Wireless Radio Management Bureau [无线电管理局], March 19, 2019, http://www.cctime.com/html/2019-3-19/1438378.htm. In addition, the Central Military Commission has also established the CMC Electromagnetic Spectrum Management Committee Office [中央军委电磁频谱管理委员会办公室] as of 2018.

[102] "Jiangsu Unicom and Nanjing Garrison District Accelerate the Promotion of 5G Pilot Applications in the Domain of Military-Civil Fusion" [江苏联通联合南京警备区加快推动军民融合领域5G试点应用], JSTV, February 27, 2019, http://news.jstv.com/a/20190227/1551254341392.shtml.

[103] David E. Sanger, Julian E. Barnes, Raymond Zhong, and Marc Santora, "In 5G Race with China, U.S. Pushes Allies to Fight Huawei," *The New York Times*, January 26, 2019, https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html.

[104] Simon Denyer, "Japan effectively bans China's Huawei and ZTE from government contracts, joining U.S.," *The Washington Post*, December 10, 2018, https://www.washingtonpost.com/world/asia_pacific/japan-effectively-bans-chinas-huawei-zte-from-government-contracts-joining-us/2018/12/10/748fe98a-fc69-11e8-ba87-8c7facdf6739_story.html?utm_term=.b4522d8ff42a.

[105] "Mobile network operator's body GSMA considers crisis meeting over Huawei," Reuters, February 2, 2019, https://www.reuters.com/article/us-usa-china-huawei-tech-europe-exclusiv/exclusive-mobile-network-operators-body-gsma-considers-crisis-meeting-over-huawei-idUSKCN1PR0DT.

[106] Julian E. Barnes and Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *The New York Times,* March 17, 2019, https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html.

[107] Dan Strumpf and Patricia Kowsmann, "U.S. Prosecutors Probe Huawei on New Allegations of Technology Theft," *The Wall Street Journal*, August 29, 2019, https://www.wsj.com/articles/u-s-prosecutors-probe-huawei-on-new-allegations-of-technology-theft-11567102622; and Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal,* August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[108] For a detailed discussion and assessment of these dynamics of geopolitics and "geotechnology," see Paul Triolo, Kevin Allison, and Clarise Brown, "Eurasia Group White Paper: The Geopolitics of 5G" (Eurasia Group, November 15, 2018), https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf.

[109] That is not to say that an outright banning of Huawei is the only or most desirable solution in all cases and for all countries, but clearly, allowing Huawei to have unconstrained presence in American infrastructure is highly risky at best.

[110] Specifically, AT&T's CEO has claimed, "If you have deployed Huawei as your 4G network, Huawei is not allowing interoperability to 5G — meaning if you are 4G, you are stuck with Huawei for 5G." For recent reporting on this issue and concern, see David Shepardson, "AT&T CEO says China's Huawei hinders carriers from shifting suppliers for 5G," Reuters, March 20, 2019, https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX.

[111] Kelvin Chan and Karel Janicek, "Cyber officials call for coordinated 5G security approach," The Associated Press, May 3, 2019, https://www.apnews.com/132800027bf24f95aa9f0c950f96343d.

[112] Tara Seals, "The Promise and Peril of 5G," Threatpost.com, January 9, 2019, https://threatpost.com/5g-security/140664.

[113] Dan Strumpf, Natasha Khan, and Charles Rollet, "Surveillance Cameras Made by China Are

Hanging All Over the U.S.," *The Wall Street Journal*, November 12, 2017, https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949.

[114] For an extensive discussion of these issues from an Australian perspective, see Danielle Cave et al., "Huawei and Australia's 5G Network" (Australian Strategic Policy Institute, October 2018), https://www.aspi.org.au/report/huawei-and-australias-5g-network.

[115] For an excellent assessment of policy options on this issue, see Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War" (MITRE, 2018), https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.

[116] "SA3 - Security," https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security.

[117] For an example of theft that pertains to Huawei, see "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," U.S. Department of Justice, press release, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade.

[118] For a notable consideration of the legal considerations in play, including the apparent requirements of China's National Intelligence Law and Cyber Security Law, see Donald C. Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," SSRN, March 17, 2019.

[119] The initial story in Bloomberg was somewhat problematic by some accounts, including reportedly conflating a common protocol (Telnet) with a backdoor, but the story remains that multiple vulnerabilities were discovered by Vodaphone that Huawei is reported to have been fairly slow to remedy. Jon Porter, "'Hidden backdoors' were found in Huawei equipment, reports Bloomberg," TheVerge.com, April 30, 2019, https://www.theverge.com/2019/4/30/18523701/huawei-vodafone-italy-security-backdoors-vulnerabilities-routers-core-network-wide-area-local. See this excellent analysis and recent reporting on it: Kate O'Keeffe and Dustin Volz, "Huawei Telecom Gear Much More Vulnerable to Hackers Than Rivals' Equipment, Report Says," *The Wall Street Journal*, June 25, 2019, https://www.wsj.com/articles/huawei-telecom-gear-much-more-vulnerable-to-hackers-than-rivals-equipment-report-says-11561501573; and "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd." (Finite State, June 2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

[120] See this excellent research from Recorded Future: Priscilla Moriuchi and Dr. Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," Recorded Future, March 9, 2018, https://www.recordedfuture.com/chinese-vulnerability-data-altered.

[121] See, for instance, authoritative textbooks that include direct or ambiguous discussion of the potential for attacks on critical infrastructure: Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部] ed., *The Science of Military Strategy* [战略学] (Military Science Press, 2013); and Ye Zheng [叶证], *Lectures on the Science of Information Operations [信息作战科学教程]* (Military Science Press [军事科学出版社], 2013).

[122] Daniel R. Coats, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the Intelligence Community," Statement to the Select Committee on Intelligence, U.S. Senate, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[123] "Huawei cyber security evaluation centre oversight board: annual report 2019," March 28, 2019, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

[124] "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd."; and Robert Abel, "Microsoft researchers find NSA-style backdoor in Huawei laptops," SCMagazine.com, March 29, 2019, https://www.scmagazine.com/home/security-news/vulnerabilities/microsoft-defender-advanced-threat-protection-atp-service-featured-in-windows-version-1809-discovered-an-nsa-inspired-backdoor-vulnerability-in-huawei-laptops.

[125] The White House Office of the Press Secretary, "Presidential Memorandum: Unleashing the Wireless Broadband Revolution," June 28, 2010, https://obamawhitehouse.archives.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution.

[126] Tom Power and Lawrence E. Strickling, "Administration Advances Wireless Spectrum for Economic Growth," blog on ObamaWhiteHouse.archives.gov, June 14, 2013, https://obamawhitehouse.archives.gov/blog/2013/06/14/administration-advances-wireless-spectrum-economic-growth; and The White House Office of the Press Secretary, "Presidential Memorandum -- Expanding America's Leadership in Wireless Innovation," June 14, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/14/presidential-memorandum-expanding-americas-leadership-wireless-innovatio.

[127] The White House, "Fact Sheet: Administration Announces an Advanced Wireless Research Initiative, Building on President's Legacy of Forward-Leaning Broadband Policy."
[128] Federal Communications Commission, *Fifth Generation Wireless Network and Device Security*, PS Docket No. 16-353 (February 3, 2017), https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0203/DA-17-131A1.pdf.
[129] For the initial document, see Federal Communications Commission, *Fifth Generation Wireless Network and Device Security* (December 16, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1282A1_Rcd.pdf.
[130] Kim Hart, David McCabe, and Jonathan Swan, "The "national 5G" plan that won't die," Axios.com, March 4, 2019, https://www.axios.com/the-national-5g-plan-that-wont-die-1551645945-c3d6ab60-88db-4350-aaa3-ed0788d2be7b.html; and Jonathan Swan, David McCabe, Ina Fried, and Kim Hart, "Scoop: Trump team considers nationalizing 5G network," Axios.com, January 28, 2018, https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html.
[131] The White House, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," October 25, 2018, https://web.archive.org/web/20181025174042/https://www.whitehouse.gov/presidential-actions/presidential-memorandum-developing-sustainable-spectrum-strategy-americas-future.
[132] The White House, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future."
[133] Federal Communications Commission, "The FCC's 5G FAST Plan," https://www.fcc.gov/5G.
[134] Federal Communications Commission, "FCC Takes Steps to Make Millimeter Wave Spectrum Available for 5G," https://www.fcc.gov/document/fcc-takes-steps-make-millimeter-wave-spectrum-available-5g-0.
[135] For a recent assessment, see "The Global Race to 5G Spring 2019 Update."
[136] "The Global Race to 5G Spring 2019 Update."
[137] Brian Fung, "AT&T is being criticized for upgrading its phones to 'fake' 5G. Now Sprint, T-Mobile and Verizon are piling on," *The Washington Post*, January 8, 2019, https://beta.washingtonpost.com/technology/2019/01/08/att-is-being-criticized-upgrading-its-phones-fake-g-now-t-mobile-is-piling.
[138] The White House, "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.
[139] Todd Shields, "U.S. FCC Bars China Mobile, Reviewing Other Chinese Carriers," Bloomberg, May 9, 2019, https://www.bloomberg.com/news/articles/2019-05-09/china-mobile-barred-from-the-u-s-market-over-espionage-concerns.
[140] Julia Horowitz, "Huawei pleads not guilty to charges it violated US sanctions on Iran," CNN, March 14, 2019, https://www.cnn.com/2019/03/14/business/huawei-iran-sanctions-plea/index.html.
[141] U.S. Department of Commerce's Bureau of Industry and Security, "Addition of Certain Entities to the Entity List (final rule), effective May 16, 2019," https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019.
[142] "Chart: Huawei's Dependence on U.S. Suppliers," CaixinGlobal.com, December 6, 2018, https://www.caixinglobal.com/2018-12-06/chart-huaweis-dependence-on-us-suppliers-101356383.html.
[143] Li Tao and Iris Deng, "Huawei's chip unit says it prepared years ago for doomsday scenario of US tech ban," *South China Morning Post*, May 17, 2019, https://www.scmp.com/tech/big-tech/article/3010635/huaweis-chip-unit-says-it-prepared-years-ago-doomsday-scenario-us.
[144] Raymond Zhong, "Huawei's U.S. Restrictions Expose a High-Tech Achilles' Heel for China," *The New York Times,* May 21, 2019, https://www.nytimes.com/2019/05/21/technology/huawei-china-us-trade.html.
[145] "Electrical Engineer Convicted of Conspiring to Illegally Export to China Semiconductor Chips with Missile Guidance Applications," U.S. Department of Justice, press release, July 2, 2019, https://www.justice.gov/opa/pr/electrical-engineer-convicted-conspiring-illegally-export-china-semiconductor-chips-missile.
[146] "People's Daily: Huawei is both a mirror and a benchmark" [人民日报：华为是一面镜子 也是一个标杆], *People's Daily*, May 18, 2019, https://finance.sina.com.cn/stock/usstock/c/2019-05-18/doc-ihvhiews2674771.shtml.
[147] Paul Mozur and Cecilia Kang, "U.S. Tech Companies Sidestep a Trump Ban, to Keep Selling to Huawei," *The New York Times*, June 25, 2019, https://www.nytimes.com/2019/06/25/technology/huawei-trump-ban-technology.html?module=inline.

[148] The initial initiatives launched in 2016 are to be credited for a forward-looking approach. However, the magnitude of these measures is insufficient relative to the scope and scale of the competitive challenge. The White House, "Fact Sheet: Administration Announces an Advanced Wireless Research Initiative, Building on President's Legacy of Forward-Leaning Broadband Policy."

[149] These issues are often attributed to a combination of factors that include deregulation, inadequate standardization, and fragmentation of the market with dynamics that tend toward oligopoly in some cases, along with the adverse impact of Chinese industrial policies. Robert E. Litan and Roger G. Noll, "The Uncertain Future of the Telecommunications Industry," Brookings, January 19, 2004, https://www.brookings.edu/research/the-uncertain-future-of-the-telecommunications-industry-2; Susan P. Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven, CT: Yale University Press, 2013); and Barry C. Lynn, *Cornered: The New Monopoly Capitalism and the Economics of Destruction* (Hoboken, NJ: John Wiley & Sons, 2009).

[150] Ryan Mcmorrow, "Huawei a key beneficiary of China subsidies that US wants ended," Phys.org, May 30, 2019, https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html.

[151] According to an estimate from Accenture, wireless providers could invest some $275 billion in 5G-related networks, adding $500 billion to the U.S. economy. However, it is difficult to verify that estimate based on current levels of expenditures.

[152] "5G in China: Outlook and regional comparisons."

[153] Assistant Secretary for Communications and Information David J. Redl, "Remarks of Assistant Secretary Redl at the White House 5G Summit" (White House 5G Summit, Washington, September 28, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-white-house-5g-summit.

[154] See this Tweet by @realDonaldTrump on February 21, 2019, https://twitter.com/realDonaldTrump/status/1098581869233344512?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1098581869233344512%7Ctwgr%5E393039363b74776565745f6d65646961&ref_url=https%3A%2F%2Fwww.broadcastingcable.com%2Fnews%2Ftrump-tweets-call-to-5g-arms.

[155] For a noteworthy evaluation of this dynamic, see Jonathan Gruber and Simon Johnson, *Jump-Starting America: How Breakthrough Science Can Revive Economic Growth and the American Dream* (New York: PublicAffairs, 2019).

[156] For a compelling exploration of these challenges, see Susan Crawford, *Fiber: The Coming Tech Revolution—and Why America Might Miss It* (New Haven, CT: Yale University Press, 2018).

[157] Although nationalization is not a viable approach and should not be considered, this initial proposal is notable for highlighting the importance of 5G: Swan, McCabe, Fried, and Hart, "Scoop: Trump team considers nationalizing 5G network."

[158] Potentially, such an initiative could be modeled off of the "SmartAmerica" challenge launched by White House Presidential Innovation Fellows in 2013. See https://smartamerica.org/about.

[159] See for instance recent legislation that aims to advance this objective: "US lawmakers propose $1 billion fund to replace Chinese network gear," RCR Wireless, September 26, 2019, https://www.rcrwireless.com/20190926/5g/us-lawmakers-propose-1-billion-fund-replace-huawei-gear and "SmartAmerica," https://smartamerica.org/about. Such an agenda may be analogous to the role and model of the federal government in constructing the national highway system or promoting electricity, which are two commonly suggested comparisons.

[160] For initial context on this initiative, see Dave Vergun, "DOD Develops Secure 5G Mobile Telecommunication Network Strategy," Defense.gov, May 10, 2019, https://www.defense.gov/explore/story/Article/1844423/dod-develops-secure-5g-mobile-telecommunication-network-strategy.

[161] Juho Lee, Erika Tejedor, Karri Ranta-aho, Hu Wang, Kyung-Tak Lee, Eliane Semaan, Eiman Mohyeldin, Juyeon Song, Christian Bergljung, and Sangyeob Jung, "Spectrum for 5G: Global status, challenges, and enabling technologies," *IEEE Communications Magazine,* 56 no. 3 (March 2018), 12-18.

[162] For instance, the FCC may consider devising a standard framework of regulations to propose to and incentivize localities to adopt in order to lessen the bureaucratic obstacles to 5G adoption. American policymakers may also draw lessons learned from other nations that have undertaken innovative approaches to facilitate rapid deployment of fiber and 5G networks.

[163] "The FCC's 5G FAST Plan."

[164] For context, see Michael J. Marcus, "WRC-19 Issues: A Survey," IEEE Wireless Communications, February 2017, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7864779. For an industry perspective, see "The GSMA WRC series – getting ready for WRC-19," https://www.gsma.com/spectrum/wrc-series.

[165] For context on this initiative, see U.S. Department of Homeland Security, "ICT Supply Chain Task Force Fact Sheet," https://www.dhs.gov/publication/ict-supply-chain-task-force-fact-sheet.
[166] For context, see "Prague 5G Security Conference," Government of the Czech Republic, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-173333.
[167] This listing is informed by a number of discussions and responding to questions raised in the recent meetings in Prague. For such a framework, nation of origin can contribute to such risk factors but is one among many that ought to be taken into account when evaluating security.
[168] As the U.S. government actively engages with issues of 5G security, there are likely lessons to be learned from valuable initiatives that are ongoing on supply chain security across various industries, including health care, where the risks of vulnerabilities can be very acute. For a more detailed discussion of these concerns and considerations, see Beau Woods and Andy Bochman, "Supply chain in the software era" (Atlantic Council, May 30, 2018), https://www.atlanticcouncil.org/publications/issue-briefs/supply-chain-in-the-software-era. Potentially, such a mechanism might involve a "5G Information Sharing and Analysis Center" (ISAC) under the aegis of the National Council of ISACs, or there could be lessons learned from existing organizations. For context and current models of ISACs, see "National Council of ISACs," https://www.nationalisacs.org/about-nci.
[169] This framework could build upon CISA's initial efforts to create a more systematic approach to risk mitigation. U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, "National Risk Management," https://www.dhs.gov/cisa/national-risk-management.
[170] For context, see Federal Communications Commission, "Communications Security, Reliability, and Interoperability Council VII," https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.
[171] This issue is salient for the question of Huawei equipment in rural telecoms but a more completereview should examine the totality of relevant supply chains and digital infrastructure.
[172] Americans do not appear to adequately appreciate the extent to which U.S. technological leadership, and indeed elements of the global economic order, have been shaped and enabled by standards set in the United States and by American companies.
[173] For context on NIST's current approach to 5G, see Perry F. Wilson, Kate A. Remley, William F. Young, Camillo A. Gentile, John M. Ladbury, and Dylan F. Williams, "A NIST perspective on metrology and EMC challenges for 5G and beyond," *IEEE Electromagnetic Compatibility Magazine,* 7 no. 4 (Fourth Quarter 2018), 77-85.
[174] See National Institute of Standards and Technology, "Alliance for 5G Networks," https://www.nist.gov/industry-impacts/alliance-5g-networks.
[175] For instance, NIST has promoted security standards for IoT devices.
[176] For one example of how secure slicing could mitigate distributed denial-of-service (DDoS) attacks, see this recent paper: Danish Sattar and Ashraf Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," *arXiv preprint arXiv:1901.01443* (2019), https://arxiv.org/abs/1901.01443 //
[177] See, for instance, forthcoming research on this topic: Zhihong Tian, Shen Su, Mohan Li, Xiaojiang Du, and Mohsen Guizani, "Automated Attack and Defense Framework for 5G Security on Physical and Logical Layers," *arXiv preprint arXiv:1902.04009* (2019), https://arxiv.org/pdf/1902.04009.pdf. For an example of the proposed employment of machine learning for intrusion detection for software-defined 5G networks from researchers with Zhejiang University, see Jiaqi Li, Zhifeng Zhao, and Rongpeng Li, "A Machine Learning Based Intrusion Detection System for Software Defined 5G Network," *arXiv preprint arXiv:1708.04571* (2017), https://arxiv.org/abs/1708.04571.
[178] "Ready for 6G? How AI will shape the network of the future," MIT Technology Review (April 19, 2019), https://www.technologyreview.com/s/613338/ready-for-6g-how-ai-will-shape-the-network-of-the-future.
[179] National Institute of Standards and Technology, "Alliance for 5G Networks."
[180] For further details on this initiative, see National Science Foundation, "Advanced Wireless Research @ NSF," https://www.nsf.gov/cise/advancedwireless.
[181] National Science Foundation, "PPO: Platforms for Advanced Wireless Research (PAWR) Project Office," September 14, 2017, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1719547&HistoricalAwards=false.
[182] For instance, ONR's Division 312 Research Programs could scale up and/or prioritize research in 5G, including potential military applications of it. Office of Naval Research, "Division 312: Electronics, Sensors and Networks Research," https://www.onr.navy.mil/en/Science-Technology/Departments/Code-31/All-Programs/312-Electronics-Sensors.

[183] The Chinese government is also investing in network virtualization techniques through the 863 Plan. "863 Plan Information Domain "5G Wireless Network Cognitive and Virtualization Key Technology Research and Verification" Project Through Technical Acceptance" [863计划信息领域 "5G无线网络认知与虚拟化关键技术研究与验证" 课题通过技术验收], Ministry of Science and Technology [科技部], January 15, 2018, http://www.stdaily.com/zhuanti01/5G/2018-01/15/content_622971.shtml.

[184] "Migration from Physical to Virtual Network Functions: Best Practices and Lessons Learned" (GSMA, October 12, 2018), https://www.gsma.com/futurenetworks/5g/migration-from-physical-to-virtual-network-functions-best-practices-and-lessons-learned.

[185] National Telecommunications and Information Administration, "Spectrum Sharing Innovation Test-Bed," https://www.ntia.doc.gov/category/spectrum-sharing-innovation-test-bed.

[186] "DARPA Awards Six Teams During Final Spectrum Collaboration Challenge Qualifier," December 19, 2018, https://www.darpa.mil/news-events/2018-12-19.

[187] "How AI Could Enable Spectrum Frequency Multitasking," GovernmentCIO, March 19, 2019, https://www.spectrumcollaborationchallenge.com/how-ai-could-enable-spectrum-frequency-multitasking.

[188] For instance, such a program might build upon the DHS Silicon Valley Innovation Program. U.S. Department of Homeland Security, "Silicon Valley Innovation Program," https://www.dhs.gov/science-and-technology/svip.

[189] For context on this new initiative, see O-Ran Alliance, "Operator Defined Next Generation RAN Architecture and Interfaces," https://www.o-ran.org.

[190] Thanks so much to Andrea Kendall-Taylor for recommending this point.

[191] On the importance of messaging, and problems that have arisen to date from a lack of clarity, see Julian Ku, "The Detention of Huawei's CFO is Legally Justified. Why Doesn't the U.S. Say So?," Lawfare, December 12, 2018, https://www.lawfareblog.com/detention-huaweis-cfo-legally-justified-why-doesnt-us-say-so.

[192] Danielle Cave, "The African Union headquarters hack and Australia's 5G network," The Strategist, July 13, 2018, https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network.

[193] For more context on the challenges of and opportunities for interoperability, see this piece, which discusses the various lines of effort that have been operant under the Connected Forces Initiative: Dr. James Derleth, "Enhancing interoperability: the foundation for effective NATO operations," NATO Review, 2015, https://www.nato.int/docu/review/2015/also-in-2015/enhancing-interoperability-the-foundation-for-effective-nato-operations/EN/index.htm.

[194] Of course, creating a 5G network that is dedicated for defense applications could make that system a potential target for disruption, but leveraging primarily civilian infrastructure also has risks, such that creating new architectures that may ensure greater optionality is worth exploring. In the process, the security, resilience, and redundancy of these systems should be a priority.

[195] For a more detailed discussion of such policy options, including the idea of a new fund or bank for digital development, see Daniel Kliman and Abigail Grace, "Power Play: Addressing China's Belt and Road Strategy" (Center for a New American Security, September 20, 2018), https://www.cnas.org/publications/reports/power-play.

[196] For further discussion of the challenges of U.S. defense mobilization, see Elsa Kania, "Testimony before the National Commission on Service Hearing on "Future Mobilization Needs of the Nation," National Commission on Service, April 24, 2019, https://www.inspire2serve.gov/_api/files/200.

[197] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (Routledge, May 2013).

[198] Jameson Berkow, "Nortel hacked to pieces," *Financial Post*, February 25, 2012, https://business.financialpost.com/technology/nortel-hacked-to-pieces; and Laura Payton, "Former Nortel exec warns against working with Huawei," CBC News, October 11, 2012, https://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006.

[199] Heather Somerville and Jane Lanhee Lee, "U.S. universities unplug from China's Huawei under pressure from Trump," Reuters, January 24, 2019, https://www.reuters.com/article/us-usa-china-security-universities-insig/u-s-universities-unplug-from-chinas-huawei-under-pressure-from-trump-idUSKCN1PI0GV.

[200] For an excellent analysis of the importance of LVC training, see Jennifer McArdle, "Victory Over and Across Domains: Training for Tomorrow's Battlefields" (Center for Strategic and Budgetary Assessments, 2019), https://csbaonline.org/uploads/documents/Victory_Over_and_Across_Domains.pdf.

[201] Megan Eckstein, "Navy Rolls Out NavalX Agility Office to Connect Innovators With Support, Tools," USNI News, February 14, 2019, https://news.usni.org/2019/02/14/navy-rolls-navalx-agility-office-connect-innovators-support-tools.

[202] This phrase and concept, which can also be rendered "turning sharply to surpass," implies how a change in direction (e.g., in technological development) can provide an opportunity for disruption, including because the United States and China are starting closer to the same level. "In the 5G era, [can] the communications industry 'surpass at a turning point'?" [5G时代通信产业"弯道超车"？], *People's Daily*, December 4, 2017, http://www.ce.cn/xwzx/gnsz/gdxw/201811/02/t20181102_30692220.shtml.

[203] For instance, China's attempts to advance "civil-military integration" (军民结合) and military-civil fusion (军民融合) have drawn evident inspiration from the successful synergies of the American defense industry and innovation ecosystem. The Chinese military has apparently established its own counterpart to DARPA, the Central Military Commission Science and Technology Commission, in its efforts to advance defense innovation.