CHAPTER 4

CHINA'S HIGH-TECH DEVELOPMENT

SECTION 1: NEXT GENERATION CONNECTIVITY

Key Findings

- The Chinese government has strengthened its strategic support for the Internet of Things (IoT) (physical devices embedded with sensors that can collect data and connect to each other and the broader internet) and fifth-generation wireless technology (5G) networks. The government has laid out comprehensive industrial plans to create globally competitive firms and reduce China's dependence on foreign technology through: significant state funding for domestic firms and 5G deployment, limited market access for foreign competitors, China-specific technical standards, increased participation in global standards bodies, localization targets, and alleged cyber espionage and intellectual property theft. This state-directed approach limits market opportunities for foreign firms in China and raises concerns about the ability of U.S. and other foreign firms to compete fairly both in China's domestic market and abroad.
- 5G networks are expected to quicken data speeds by 100 times, support up to 100 times more IoT devices, and provide near-instant universal coverage and availability. U.S. and Chinese companies are engaged in a fierce competition to secure first mover advantage and benefit from the trillions in economic benefits 5G and subsequent technologies are expected to create.
- IoT devices collect enormous amounts of user information; when aggregated and combined with greater computing power and massive amounts of publicly available information, these data can reveal information the user did not intend to share. U.S. data could be exposed through unsecure IoT devices, or when Chinese IoT products and services transfer U.S. customer data back to China, where the government retains expansive powers to access personal and corporate data.
- The Chinese government is leveraging its comparative advantage in manufacturing and state-led industrial policies to secure an edge in the IoT's wide-ranging commercial and military applications. U.S. firms and the U.S. government rely on global supply chains that in many cases are dominated by China. While not all products designed, manufactured, or assembled in China are inherently risky, the U.S. government lacks essential tools to conduct rigorous supply chain risk assessments. Federal

procurement laws and regulations are often contradictory, and are inconsistently applied.

- International 5G standards will be set by 2019, facilitating large-scale commercial deployment expected by 2020. The Chinese government is encouraging its companies to play a greater role in international 5G standards organizations to ensure they set global standards; such leadership may result in higher revenues and exports from internationally accepted intellectual property and technology and more global influence over future wireless technology and standards development.
- China's central role in manufacturing global information technology, IoT devices, and network equipment may allow the Chinese government—which exerts strong influence over its firms—opportunities to force Chinese suppliers or manufacturers to modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of IoT devices or 5G network equipment.
- The lax security protections and universal connectivity of IoT devices create numerous points of vulnerability that hackers or malicious state actors can exploit to hold U.S. critical infrastructure, businesses, and individuals at risk. These types of risks will grow as IoT devices become more complex, more numerous, and embedded within existing physical structures. The size, speed, and impact of malicious cyber attacks against and using IoT devices will intensify with the deployment of 5G.

Recommendations

The Commission recommends:

- Congress require the Office of Management and Budget's Federal Chief Information Security Officer Council to prepare an annual report to Congress to ensure supply chain vulnerabilities from China are adequately addressed. This report should collect and assess:
  - Each agency's plans for supply chain risk management and assessments;
  - Existing departmental procurement and security policies and guidance on cybersecurity, operations security, physical security, information security, and data security that may affect information and communications technology, 5G networks, and Internet of Things devices; and
  - Areas where new policies and guidance may be needed—including for specific information and communications technology, 5G networks, and Internet of Things devices, applications, or procedures—and where existing security policies and guidance can be updated to address supply chain, cyber, operations, physical, information, and data security vulnerabilities.
- Congress direct the National Telecommunications and Information Administration and Federal Communications Commission to identify (1) steps to ensure the rapid and secure deployment

of a 5G network, with a particular focus on the threat posed by equipment and services designed or manufactured in China; and (2) whether any new statutory authorities are required to ensure the security of domestic 5G networks.

Introduction

The Chinese government is implementing a series of policies aimed at establishing China as a global innovation and technology center of next generation connectivity,* with significant implications for U.S. competitiveness, data privacy, and national security. Building upon its success in creating globally competitive telecommunications firms, the Chinese government wants to seize leadership in next generation information technology (IT). Currently, U.S. firms such as Qualcomm, Intel, Cisco, Amazon, and Google are global leaders in next generation network development. However, China's state-directed approach is eroding U.S. dominance as Chinese regulations, foreign investment restrictions, and China-specific technical standards limit U.S. and other foreign firms' access to China, the world's second-largest economy.[1] Chinese companies have already secured multiple influential positions in global standards-setting fora to advance their interests. In some cases, cyber espionage and intellectual property (IP) theft weaken U.S. and other market leaders.[2]

The dominance of Chinese firms and China-based manufacturing in global network equipment raises serious supply chain concerns about the secure deployment of U.S. fifth-generation wireless technology (5G) networks. In addition, China is the world's largest manufacturer of Internet of Things (IoT) devices—physical devices embedded with sensors that can collect data and connect to each other and the broader internet.[3] The rapid increase in these largely unsecure IoT devices is creating numerous points of vulnerability for intelligence collection, cyber attacks, industrial control, or censorship. In addition, through IoT products and services, Chinese firms may be transferring data from their U.S. consumers to China, where the government retains expansive powers to collect and exploit data with little regard for privacy or ownership concerns.[4]

This section lays out China's industrial policies to support the IoT and 5G technologies, compares U.S. and Chinese technological leadership and market access in these industries, and analyzes the implications of these developments for U.S. competitiveness, national security, supply chains, and data privacy and security. It draws from the Commission's March 2018 hearing on China's pursuit of next generation connectivity; contracted research; consultations with government officials, academics, and industry experts; and open source research and analysis.

Overview of China's Industrial Policy Blueprints

The Chinese government plays a leading role in setting Chinese companies' priorities and guiding China's industrial transformation. In a series of industrial plans, the Chinese government laid out strategies for transforming Chinese firms into internationally

*Next generation connectivity refers to highly interconnected and autonomous devices and sensors enabled by reliable, near-instant communications.

competitive domestic firms, and replacing foreign technology and products with those designed and made by Chinese companies, first in the domestic market and then the global market.*

The influential "Internet Plus" and "Made in China 2025" initiatives seek to capitalize on the rise of integrated digital technology and automation to transition China's economy to higher-value-added manufacturing and services and transform China into a technological powerhouse.[5] Internet Plus seeks to leverage China's huge online consumer market to build up the country's domestic mobile internet, cloud computing, big data, and the IoT, and create global competitors by assisting domestic firms' expansion abroad.[6]

Made in China 2025 reiterates China's long-held indigenous innovation and import substitution goals, but is larger in scope, resources, and intergovernmental coordination than previous plans.[7] Next generation IT—a broad category that encompasses telecommunications, artificial intelligence (AI),† semiconductors, and the IoT—is one of the ten key sectors‡ designated for additional government support.[8] According to the U.S. Chamber of Commerce, Made in China 2025 "aims to leverage the power of the state to alter competitive dynamics in global markets in industries core to economic competitiveness."[9]

The Internet of Things

The rapid increase in the number, data usage, and connectivity of IoT devices is transforming every aspect of how we work, live, and fight wars. One of the core utilities of the IoT is its ability to collect and share data between devices to optimize desired outcomes (e.g., efficiency, performance, or profit) with ever greater automation. For example, IoT devices can monitor a user's physical activity (e.g., wearable fitness trackers); automatically adjust the temperature of a residence or office based on motion, temperature, humidity, and light to conserve energy (e.g., smart thermostats); and remotely deliver products and services (e.g., smart drones) (see Table 1).[10] The IoT will also yield significant military technological advantages in strategic deterrent and warfare capabilities; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); and supply chain management.[11] Some examples include autonomous unmanned systems that enhance C4ISR, strike missions, and electronic warfare, and swarms of drones that enable future asymmetric battlefield capabilities.[12]

---

*For a comprehensive analysis of China's industrial plans and their impact on 11 sectors, see Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016.

†AI comprises machine programs that can teach themselves by harnessing high-performance computing and big data and eventually mimicking how the human brain thinks. For more information on China's efforts to build its AI capabilities, see Tate Nurkin et al., "China's Advanced Weapons Systems," *Jane's by IHS Markit* (prepared for the U.S.-China Economic and Security Review Commission), May 10, 2018, 110–124; for a comparison of U.S. and Chinese AI and high-performance computing capabilities, see U.S.-China Economic and Security Review Commission, Chapter 4, Section 1, "China's Pursuit of Dominance in Computing, Robotics, and Biotechnology," in *2017 Annual Report to Congress*, November 2017, 507–539.

‡Made in China 2025 targets ten key sectors: (1) energy-saving and new energy vehicles, (2) next generation IT, (3) biotechnology, (4) new materials, (5) aerospace, (6) ocean engineering and high-tech ships, (7) railway, (8) robotics, (9) power equipment, and (10) agricultural machinery. State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015. Translation. *http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm*.

Estimates on the global number of IoT devices vary: the industry association Global System for Mobile Communications Association (GSMA) estimates the number of IoT devices worldwide will increase from 7.5 billion in 2017 to 25 billion by 2025, while the global information provider IHS estimates that the number of IoT devices will increase from 27 billion in 2017 to 125 billion by 2030.[13] McKinsey & Company estimates the IoT will unlock $4 trillion to $11 trillion in global annual economic benefits by 2025 through productivity gains, cost savings, automation, and extended life of equipment and products.[14] Operations optimization (e.g., inventory management and condition-based maintenance) is expected to account for 63 percent of the annual economic benefits.[15]

Table 1: Commercial and Military Applications of the IoT

Sector	Examples of IoT Applications
Consumer	• Augmented reality and virtual reality entertainment • Smart appliances • Wearable devices (e.g., fitness trackers)
Buildings	• Smart thermostats • Energy and water management • Automated networked surveillance
Retail	• Delivery drones • Supply chain management • Targeted advertisements • In-store customer behavior monitoring
Transportation	• Self-driving cars • Traffic management • Remote vehicle performance monitoring
Healthcare	• Telemedicine • Robot-assisted surgery • Remote medical device and physiological monitoring
Military	• Unmanned systems (e.g., drone swarms) • Integrated missile defense systems • 360-degree battlefield awareness • Logistics and inventory management

Source: Various.[16]

IoT devices can be linked into systems with a variety of applications: for instance, interconnected sensors in roads, smart traffic signals, and autonomous vehicles can exchange data to manage traffic in congested cities; several smart appliances in a home or building can exchange data and communicate to efficiently optimize energy usage; or integrated production, warehouse, and delivery facilities can track supplies and equipment throughout military and commercial supply chain networks in real-time to ensure security and timely delivery.[17] Chuck Benson, assistant director for IT in facilities services at the University of Washington, noted in his testimony before the Commission that there are six distinct characteristics of IoT systems:

(1) the large number of devices; (2) the high variability of types of devices and components within those devices; (3) the lack of language and conceptual frameworks to discuss and easily categorize and classify devices; (4) the fact that they span many organizations within an institution; and (5) the fact that the hundreds or thousands of devices embedded in the physical infrastructure around us tend to be out of sight and out of mind; (6) lack of precedence for IoT systems implementation and management.[18]

Advancements in components, data storage, connections, and data processing are enhancing IoT device capabilities and proliferation. Inexpensive miniaturized electronics enable the proliferation of IoT devices and the collection of greater amounts of data. Cloud computing provides additional data storage, processing, and AI capabilities the IoT can leverage for greater impact.* The deployment of 5G networks is expected to provide greater bandwidth, speed, reliability, and, eventually, ubiquitous connectivity that is needed to support the continual exchange of data between IoT devices and systems. In addition, the low latency—the amount of time it takes data to travel from one point to another—of 5G networks will enable the transmission of real-time commands and data necessary for complex, high-value-added IoT devices such as autonomous vehicles (see "Fifth-Generation Wireless Technology" later in this section).[19] AI enables these devices to become "smart," acting with ever greater automation upon the data they collect, process, and exchange.[20]

China's Industrial Policies

Recognizing the IoT's enormous economic and military potential, the Chinese government is seeking to become the global IoT leader.† To meet this objective, the Chinese government is leveraging its comparative advantage in manufacturing and strengthening its support for the IoT and its ecosystem through:

- *Comprehensive industrial plans:* The Chinese government first identified the IoT as a strategic emerging industry in 2010 and reaffirmed the IoT as a cornerstone of the Made in China 2025 and Internet Plus industrial plans in 2015.[21] Under the 13th Five-Year Plan (2016–2020),‡ the Chinese government prioritized IoT applications in manufacturing and automobiles and

*Cloud computing refers to the storage, management, and processing of data and software services on remote servers rather than a local or personal computer. U.S.-China Economic and Security Review Commission, *Hearing on China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology*, written testimony of Mark Brinda, March 16, 2017, 1–2; for more information on China's state-led development of cloud computing, see Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 184–192; Leigh Ann Ragland et al., "Red Cloud Rising: Cloud Computing in China," *Defense Group, Inc.* (prepared for the U.S.-China Economic and Security Review Commission), September 5, 2013.

†For an in-depth analysis of China's IoT and 5G development, see John Chen et al., "China's Internet of Things," *SOS International* (prepared for the U.S.-China Economic and Security Review Commission), October 2018.

‡For more information on China's 13th Five-Year Plan and its targets, see Katherine Koleski, "The 13th Five-Year Plan," *U.S.-China Economic and Security Review Commission*, February 14, 2017.

strengthened support for enabling technologies such as 5G, AI, big data, and semiconductors.[22]

- *State funding for domestic firms:* Since 2011, China's central and local governments have rolled out over $24.2 billion* (renminbi [RMB]† 160 billion) in direct financial support for China's IoT development. In addition, national and local governments are providing significant financial support for key IoT-enabling technologies such as semiconductors and AI: $108.8 billion (RMB 720 billion) in national and local government semiconductor funds in 2014; a $3.2 billion (RMB 20 billion) national Advanced Manufacturing Fund in 2016; a second $18.1 billion (RMB 120 billion) national semiconductor fund in 2018; and more than $7.2 billion in local government funding for AI development.[23]
- *Localization targets:* The Chinese Academy of Engineering's *Made in China 2025 Key Area Technology Roadmap* lists targets for increasing Chinese firms' share of the domestic market for autonomous manufacturing robotics to 70 percent, smart manufacturing equipment to 60 percent, and partially autonomous vehicles to 50 percent by 2025.[24]
- *Cyber espionage and IP theft:* The Chinese government and firms have allegedly committed IP theft or cyber espionage against U.S. firms in high-value IoT and IoT-enabling sectors.[25] For example, in July 2018 a federal grand jury indicted former Apple employee Xiaolang Zhang for stealing trade secrets and IP for Apple's autonomous vehicles with the intent to transfer these proprietary documents to a Chinese competitor, Xiaopeng Motors.[26] Chinese firms have also targeted U.S. telecommunications and semiconductor firms.[27]

Comparison of U.S. and Chinese Capabilities

The IoT's universal applicability makes it inherently difficult to measure the overall competitiveness of any given country, but a review of key enabling technologies such as telecommunications, semiconductors, cloud computing, and AI can serve as a proxy. China has a competitive edge as the world's largest manufacturer of IT, IoT devices, and network equipment.[28] China is the world's largest IT manufacturer: from 2012 to 2017, around 51 percent of total shipments made by leading U.S. IT firms HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel originated in China.[29] The French insurance firm AXA estimates that by 2020, 95 percent of IoT devices will

*This figure includes a $755.3 million (RMB 5 billion) special fund for IoT development for 2011–2016, the $15.1 billion (RMB 100 billion) China Internet Investment Fund, the Ministry of Industry and Information Technology's $7.6 billion (RMB 50 billion) in smart city research and projects, the $61.7 million (RMB 408.5 million) Shanghai IoT Entrepreneurial Investment Fund, and the $755.3 million (RMB 5 billion) Wuxi IoT industry fund. Zhang Xin and Chen Tianyuan, eds., "Wuxi Forms 5 Billion Yuan Internet of Things Industry Fund to Usher in Industry Development," *People's Daily Jiangsu Channel*, September 11, 2017, Translation; *Xinhua*, "China Launches $14.6B Internet Investment Fund," *State Council of the People's Republic of China*, January 23, 2017; Simi Holdings, "Venture Capital Fund." Translation; Qichacha, "Shanghai IoT Second Round Innovation Investment Fund," Translation. Matthew Fulco, "Poised for Takeoff: China's Internet of Things," *CKGSB Knowledge*, September 24, 2015; GSMA, "How China's Scaling the Internet of Things," July 2015, 8; Hao Yan, "China Sets 5b Yuan Fund for IoT Industry," *China Daily*, August 23, 2011.

†Unless noted otherwise, this section uses the following exchange rate throughout: $1 = RMB 6.62.

be manufactured in China.[30] In 2017, Huawei and ZTE together accounted for 41 percent of the $37.2 billion global mobile infrastructure hardware revenue.[31] U.S. and Chinese firms are global competitors in AI and 5G development (discussed in greater detail in the "Fifth-Generation Wireless Technology" section).[32]

By comparison, U.S. firms are currently market leaders in industrial IoT and key high-value-added IoT-enabling technologies such as semiconductors and cloud computing.[33] According to research platform IoT One's 2018 assessment of 2,000 providers of industrial IoT (i.e., application of the IoT to manufacturing and industrial processes), U.S. firms accounted for 230 of the 500 most impactful firms compared to Germany (52) and China (27); U.S.-headquartered ThingWorx, Texas Instruments, and Intel ranked as the top three.* In 2017, Intel, Micron, Qualcomm, and Nvidia together comprised 25.2 percent of the $438.5 billion in global semiconductor sales, followed by South Korean firms Samsung and SK Hynix with 21 percent.[34] Amazon Web Services, Microsoft, IBM, and Google together accounted for over half of the $180 billion global cloud computing revenue in 2017.[35]

Seeking to catch up, the Chinese government utilizes state financing, technology transfer and joint venture requirements, state-directed procurement orders, China-specific standards, data storage and transfer regulations, and security and investment screenings to build globally competitive cloud computing and semiconductor† companies.[36] (For more information on China's data transfer regulations, see Chapter 1, Section 2, "Tools to Address U.S.-China Economic Challenges.")

U.S. Market Access in China

U.S. firms can establish operations and sell IoT products and services in China; however, they must also store Chinese customer data within China and face significant restrictions on transferring data overseas.[37] Such restrictions impede data analytics, technology optimization, and integrated global service and research and development (R&D).[38] For example, firms combine and analyze data in real time from their global locations to lower costs, improve business performance, and personalize products and services.[39] In 2017, the Chinese government loosened foreign investment restrictions in augmented reality and virtual reality devices and intelligent emergency medical rescue devices, where there is growing domestic demand for those products and services in China and need for foreign investment to transform domestic firms into global competitors.[40] However, U.S. firms in IoT-enabling technologies—particularly cloud computing and telecommunications—face significant market barriers, including:

- *Chinese IP requirements:* Since 2007, China's Multi-Level Protection Scheme, which covers around 140,000 information sys-

*The ranking is based on technology innovation, brand influence, ecosystem openness, and input from industry experts and end users. IoT One, "2018 Top 500 Industrial IoT Companies." *https://www.iotone.com/iotone500*.

†For more information on China's efforts to develop its semiconductor industry, see U.S.-China Economic and Security Review Commission, Chapter 1, Section 3, "China's 13th Five-Year Plan," in *2016 Annual Report to Congress*, November 2016, 155–161.

tems,* requires Chinese IP in core IT technology and components and annual testing, certification, and authentication for the top three of the five tiers of IT users,† effectively excluding foreign competitors unless there is no domestic equivalent.[41] Article 34 of the draft guidelines would expand this scheme to cloud computing platforms, big data systems, industrial control systems and mobile networks, AI, and IoT devices.[42]

- *High restrictions on foreign ownership and investment:* Under China's 2016 Telecommunications Regulations, foreign firms can own up to 50 percent of Chinese telecommunications and cloud computing providers.[43] China's 2016 Telecom Services Catalogue requires foreign telecommunications and cloud computing firms wishing to sell in the Chinese market to form joint ventures with Chinese firms.[44] For example, AT&T has a joint venture with state-owned China Telecom; IBM, Microsoft, and Amazon have separate joint ventures with the Chinese firm 21Vianet for data storage.[45] In February 2017, AT&T and China Mobile agreed to jointly develop an IoT platform, which will allow AT&T to deploy IoT assets and offerings in the Chinese market using China Mobile's services.[46]
- *China-specific technical standards:* The Mercator Institute for China Studies (MERICS) found "China sometimes formulates national standards in strategic industries that deliberately differ from international standards in order to impede market access for foreign technology and to favor Chinese technology on the domestic market."[47] Chinese technical standards for cloud computing, industrial software, and big data have no correlation with international standards.[48] Only around half of China's key smart manufacturing technology standards—critical for controlling a technology—align with international standards; by comparison, around 70 percent of China's standards for low-level smart manufacturing (e.g., safety and management requirements) correlate with international standards.[49] U.S. and other foreign firms must alter their products or services or pay royalty fees to meet the China-specific standards and sell in China's market.[50] (For an example of the impact of a China-specific standard on U.S. firms, see Chapter 1, Section 2, "Tools to Address U.S.-China Economic Challenges.")
- *Restrictions on data storage and transfer:* Under China's Cybersecurity Law, U.S. firms face significant restrictions on data storage and cross-border transfers—essential services for IoT

*The U.S. National Institute of Standards and Technology defines an information system as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems." U.S. National Institute of Standards and Technology, Computer Security Resource Center, *Glossary*.

†The Multi-Level Protection Scheme separates information systems into five levels based on impact. Damage to a Level 1 (the lowest) information system could result in harm to legal rights of citizens, legal persons, or other organizations without harming national security, social order, or public interest. Damage to a Level 5 (the highest) information system results in very serious harm to national security. Level 3 and above encompasses finance, banking, tax, customs, commerce, communications, health, education, and social services. Nick Marro, "The 5 Levels of Information Security in China," *China Business Review*, December 6, 2016; Adam Segal, "China, Encryption Policy, and International Influence," *Hoover Institution*, No. 1610, November 28, 2016.

devices.[51] U.S. firms such as IBM, Apple, and Microsoft are required to form joint ventures with Chinese partners in order to operate.[52] In addition, foreign firms must rely on domestic partners and government-approved encryption technology, potentially placing foreign IP and data at risk.[53] (For more information on the data transfer problems, see Chapter 1, Section 2, "Tools to Address U.S.-China Economic Challenges.")

Chinese Market Access in the United States

Foreign firms are able to sell their IoT products and services freely in the United States with limited restrictions on the collection, storage, and transfer of data (including data from IoT devices).[54] (For more information on U.S. data restrictions, see "Data Privacy and Security Risks" later in this section).[55] DJI, a Chinese smart drone manufacturer, accounted for 62 percent of the 2016 U.S. and Canadian commercial drone market.[56] Other Chinese IoT firms such as the household appliance manufacturer Haier, smartphone and smartwatch manufacturer Xiaomi, and dockless bikesharing firms Ofo and Mobike are also able to sell their IoT products and services freely in the United States.[57]

Chinese firms have also increased their investment in U.S. IoT-enabling sectors such as AI and semiconductors.[58] Examples include:

- Chinese venture capital firm Haiyin Capital's June 2016 investment in the AI unmanned system software developer Neurala (which had provided technology used by the U.S. Air Force and the National Aeronautics and Space Administration);[59]
- The November 2016 acquisition of automated supply chain technology firm Dematic by Kion (a subsidiary of Chinese state-owned enterprise Weichai Power);[60]
- Beijing Shanhai Capital Management's April 2017 acquisition of Analogix Semiconductor;[61] and
- Baidu's 2017 acquisitions of the visual perception software and hardware firm xPerception and the AI language processing and comprehension firm Kitt.ai.[62]

The U.S. government has recently imposed some restrictions on federal procurement of Chinese IoT devices and blocked Chinese investment in two U.S. semiconductor firms due to national security concerns.[63] For example:

- In August 2017, U.S. Immigration and Customs Enforcement's Los Angeles office alleged DJI is targeting U.S. customers in critical infrastructure, utilities, and law enforcement and had "moderate confidence" that DJI was "providing U.S. critical infrastructure and law enforcement data to the Chinese government."[64] The U.S. Army Research Laboratory and U.S. Navy similarly found operational risks and user vulnerability risks, and subsequently discontinued the use of DJI drones, electronic components, and software.[65] In June 2018, the U.S. Department of Defense (DOD) suspended the purchase of all commercial-off-the-shelf (COTS) drones until a cybersecurity risk assessment strategy has been established.[66]

- Chinese acquisitions of the semiconductor firms Aixtron (2016) and Lattice (2017) were blocked by presidential order following a review by the Committee on Foreign Investment in the United States (CFIUS).[67]
- In January 2018, Ant Financial (Alibaba's financial services affiliate) withdrew its $1.2 billion bid for U.S. money transfer firm MoneyGram after CFIUS deemed inadequate Ant Financial's proposed measures to protect personal data associated with U.S. customers.[68]

Fifth-Generation Wireless Technology

In his testimony to the Commission, Anthony Ferrante, senior managing director at FTI Consulting, explained the evolution of wireless technology, saying,

> *2G networks were designed for voice, 3G networks were designed for voice and data, 4G networks were designed for broadband Internet experiences. Now 5G networks are being developed to fuse computing capabilities with communications in real time.*[69]

5G is expected to quicken data speeds 100 times, support up to 100 times more IoT devices, and provide near-instant universal coverage and availability (see Table 2). Based on estimates from IHS, 5G networks will enable $12.3 trillion in global sales and support nearly 22 million jobs by 2035.[70] Manufacturing is expected to account for 27.3 percent, or $3.4 trillion, of total 5G-enabled global sales, followed by information and communications technology at 11.4 percent or $1.4 trillion.[71]

Table 2: Comparison of 4G and Future 5G Capabilities

	4G	5G (Expected 2020)
Latency	25 milliseconds	1 millisecond
Peak Data Rates	100 megabits per second	10,000 megabytes per second
Number of Devices*	10,000 devices per square kilometer	1,000,000 devices per square kilometer
Mobility†	350 kilometers per hour	500 kilometers per hour

Source: Various.[72]

5G will enhance existing mobile broadband coverage and experiences (e.g., augmented reality and virtual reality and faster streaming). It will also facilitate massive machine-type communications (e.g., smart cities and smart homes) and sustain ultrareliable and low-latency communications (e.g., autonomous vehicles).[73] 5G will support greater numbers of IoT devices and enable high-value-added IoT devices and IoT systems (i.e., autonomous vehicles and smart factories).[74] Governments and telecommunications providers are

*Connection density is the total number of devices that can be supported while maintaining quality of service.
†Mobility is the maximum speed at which a user or device can be moving while maintaining quality of service.

rushing to deploy 5G networks to lead innovation and gain first access to new revenue streams from the expanded use of the IoT and other 5G-enabled technologies (for more information, see "Comparison of U.S. and Chinese Capabilities" later in this section).[75]

China's Industrial Policies

Over the past three decades, the Chinese government successfully created globally competitive Chinese telecommunications firms and reduced China's dependence on foreign technology by: (1) providing significant financial support;* (2) utilizing localization targets and government procurement; (3) promoting Chinese technology standards domestically and internationally; (4) constraining foreign market access; (5) cultivating national champions (e.g., Huawei and ZTE); and (6) allegedly engaging in cyber espionage and IP theft.[76]

Building upon its success at creating global network equipment manufacturers, China is positioning itself to be a global leader in 5G through:†

- *Comprehensive industrial plans:* The Chinese government identified 5G as a cornerstone of its Made in China 2025 and Internet Plus initiatives in 2015.[77] China's 13th Five-Year Plan (2016–2020) reads: "[China] will drive forward research in key technologies for 5G mobile networks and ultra-wideband applications, and develop commercial applications of 5G technology."[78]
- *Establishment of a state-owned network operator:* In 2014, the Chinese government combined the cellular tower assets from China Mobile, China Telecom, and China Unicom (the country's three telecommunications providers) into a new state-owned enterprise, China Tower.‡ The three carriers, rather than each building its own network, will pay China Tower to operate a national cellular network.[79] This consolidation will allow China to accelerate 5G network deployment by combining state funding and eliminating competition or redundant infrastructure

*China Development Bank provided Huawei a $10 billion loan in 2004 and a $30 billion credit line in 2009. China Development Bank provided ZTE an $8 billion credit line in 2005 that it increased to $15 billion in 2009 and to $20 billion in 2012. In addition, the Export-Import Bank of China provided ZTE a $10 billion credit line in 2009. Huawei and ZTE leveraged their access to low-cost government financing to offer more competitive prices and loans to their customers, often undercutting their foreign competitors' prices by 30 percent. Nathaniel Ahrens, "China's Competitiveness: Myths, Reality, and Lessons for the United States and Japan—Case Study: Huawei," *Center for Strategic and International Studies*, February 2013, 8; ZTE Corporation, "Announcement on the 'Development Financing Strategic Cooperation Agreement' with China Development Bank," *Hong Kong Stock Exchange*, December 4, 2012; ZTE, "The Export-Import Bank of China Provides ZTE US$10 Billion Credit Line," May 25, 2009; ZTE, "China Development Bank Provides ZTE US$15 Billion Credit Line," March 23, 2009; Peilei Fan, "Catching up through Developing Innovation Capability: Evidence from China's Telecom-Equipment Industry," *Technovation* 26 (2006): 364; Ali Farhoomand and Phoebe Ho, "Huawei: Cisco's China Challenger," *University of Hong Kong Case HK U599*, 2006, 9.

†For an overview of China's efforts to develop its 5G technologies, see John Chen et al., "China's Internet of Things," *SOS International* (prepared for the U.S.-China Economic and Security Review Commission), October 2018; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 177–184.

‡China Tower is owned by China Mobile (28.5 percent), China Unicom (28.1 percent), China Telecom (27.9 percent), and the state-owned investment fund China Reform Holdings Corporation (6 percent). China Mobile, China Unicom, and China Telecom together accounted for 99.8 percent of China Tower's 2017 operating revenue. China Tower, "Global Offering," *Hong Kong Stock Exchange*, 10, 45.

spending.[80] In July 2018, China Tower raised $6.9 billion in an initial public offering on the Hong Kong Stock Exchange; more than half of the funding raised will be directed toward network construction.[81]

- *Financial support for 5G network deployment:* Since 2015, China Tower has invested $17.7 billion to add more than 350,000 cellular network sites.[82] The government-run Chinese Academy of Information and Communications Technology estimated that China will invest $445 billion (RMB 2.8 trillion) toward 5G networks between 2020 and 2030.[83] By comparison, the consulting firm Accenture estimates that U.S. telecommunications firms will invest around $275 billion in 5G infrastructure by 2024.[84]
- *Limited market access for foreign competitors:* GSMA estimates that China's 5G networks will be the world's largest, accounting for a third of global 5G network users.[85] The Chinese government has guaranteed Huawei and ZTE each a third of domestic 5G network contracts, limiting the opportunities for U.S. and other foreign competitors.[86]
- *Localization targets:* The Chinese Academy of Engineering's *Made in China 2025 Key Area Technology Roadmap* lays out targets to increase the global market share of Chinese-branded fiber communication network equipment to 60 percent, network equipment to 40 percent, and routers and switches to 25 percent by 2025.[87]

China's Growing Influence on International Standards Bodies for 5G

The timeline for establishing international 5G standards is very short: the first international 5G standard was adopted in December 2017; the remaining standards are expected to be finalized by December 2019, facilitating large-scale commercial deployment by 2020.[88] These standards* are largely based on consensus among competing company, academic, and government technical experts to maximize buy-in and adherence. Once set, these standards will enable global interoperability of technology and data transfers.[89]

Patented technology is increasingly incorporated into international standards provided that the IP is available under royalty-free or fair, reasonable, and nondiscriminatory† licensing terms.[90] The company that owns the patent necessary to comply with international standards (also known as a standards-essential patent) gains global market share, licensing revenues, and a competitive edge in subsequent technology development.[91] The commercial value of standards-essential patents has contributed to a rise in protracted, costly legal battles over ownership and fair licensing terms, where a

*Standards establish requirements for a specific item, material, component, system, or service, covering vocabulary, technical engineering processes, and safety, among other things. These commonalities enable interoperability among products and services. International Telecommunications Union, "Understanding Patents, Competition, and Standardization in an Interconnected World," July 1, 2014.

†Fair, reasonable, and nondiscriminatory commonly refers to fair licensing terms at reasonable rates similar to the rates and terms offered to other licensees. Anne Layne-Farrar, A. Jorge Padilla, and Richard Schmalensee, "Pricing Patents for Licensing in Standard-Setting Organizations: Making Sense of Frand Commitments," *Antitrust Law Journal* 74:3 (2007): 671–706.

delay in a fast-moving industry like IT and telecommunications can place a competitor's projects and product lines on hold.[92]

The Chinese government supports Chinese firms and associations' international standardization efforts through funding the participation of technical experts from government research institutes and setting mandatory national technical standards.[93] In the 2000s, the Chinese government unsuccessfully tried to leverage its large market to establish its domestic standards as international 3G and 4G standards.[94] Since then, Chinese technical experts and firms have been increasing the number of standards and technology submissions, participants, and leadership roles at international standards-setting bodies to ensure Chinese developed technologies are reflected in global standards.[95] In comparison to China's government-led approach, industry leads the U.S. standards-setting process, with the U.S. government providing technical expertise and policy support.[96] In July 2017, U.S. Federal Communications Commission (FCC) member Michael O'Rielly alluded to U.S. concerns related to China's increased participation in the International Organization for Standardization (ISO), International Telecommunications Union (ITU), and the 3rd Generation Partnership Project (3GPP) stating:

> *[L]ately, there has been a concerted effort by some countries to manipulate these multi-stakeholder bodies. I have heard several reports that some authoritarian governments are now focusing their attention on leadership positions at these organizations so that they can promote their agendas and dictate the future design of not only wireless networks, but also the internet.*[97]

Chinese companies and experts are playing a greater role in contributing to and leading 5G-related standards-setting bodies such as:

- *International Telecommunications Union:* ITU is an intergovernmental public-private partnership under the UN that allocates global radio spectrum and satellite orbits and establishes international technical standards for information and communication technologies.* Chinese firms and government bodies have been particularly active in ITU's 5G-related bodies. Huawei and China Mobile served as the chair and vice chair of the five leadership positions in ITU's 5G Focus Group (2015–2016).[98] As of September 2018, Chinese firms and government research institutes account for the largest number of chairs or vice chairs in 5G-related standards-setting bodies, holding 8 of the 39 available leadership positions.† By comparison, the U.S. telecommunications provider Verizon currently serves as the only U.S. representative in leadership at these bodies.[99]

*ITU is composed of 193 governments, approximately 800 companies, and various academic and other international and regional bodies. International Telecommunication Union, "About International Telecommunication Union (ITU)."

†This number comprises chair and vice chair positions at the 5G-related ITU-T Study Group 13 and its subgroups. South Korea, the second largest, holds 6 of the 39 available leadership positions. International Telecommunications Union, "SG13—Management Team (Study Period 2017–2020)"; International Telecommunications Union, "Focus Groups: ITU-T Focus Groups"; International Telecommunications Union, "Focus Group on Technologies for Network 2030"; International Telecommunications Union, "Focus Group on Machine Learning for Future Networks Including 5G."

- *3rd Generation Partnership Project:* The 3GPP leads international private sector efforts to set technical specifications (de facto standards) for 3G, 4G, and 5G cellular telecommunications network technologies.* The number of Chinese representatives serving in chair or vice chair leadership positions rose from 9 of the 53 available positions in December 2012 to 11 of the 58 available positions in December 2017.† In these roles, Chinese companies can set the agenda and guide standards discussions.[100] U.S. firms served in 14 leadership positions in 2017 compared with 7 in 2012.‡ Most notably, Qualcomm currently chairs the most important 5G standards-setting group (RAN1), beating Huawei for the position in August 2017.[101]
- *International Organization for Standardization:* ISO is an international nongovernmental organization that sets global consensus-based standards on virtually all technologies.§ China's participation on ISO standards-setting technical committees and its sub-groups increased from 706 participants in December 2012 to 731 (tied with Germany as the third largest)¶ in September 2018.[102] By comparison, U.S. participation fell from 620 to 595 (tied with Finland for 16th largest) from December 2012 to September 2018.[103] Chinese representatives have increased their share from 126 of the 3,253 available ISO leadership positions** in 2012 to 223 of the 3,430 available positions in 2017.[104] The United States has the largest number of leadership positions overall, but the number held has fallen from 653 in 2012 to 540 in 2017.[105] U.S. representatives currently lead several higher-value-added IoT-related technical committees important for the U.S. economy, to include: IT, smart drones, smart transportation vehicles, cloud computing, and data management.[106] By comparison, Chinese representatives primarily lead metal-related committees to include copper, aluminum, steel, various steel products, rare earths, and the railway.[107]

Comparison of U.S. and Chinese Capabilities

Chinese firms such as Huawei and ZTE are building upon their success as global leaders in key telecommunications technologies (see Table 3) and racing to become leaders in 5G patents and network deployment.[108] In 2017, Huawei unseated Ericsson, its Swed-

*The 3GPP unites seven telecommunications standards organizations and is composed of around 490 companies, 40 government agencies, and nearly 50 research institutes and universities. 3GPP, "About 3GPP Home."; 3GPP, "3GPP Membership."

†In 2017, China's 11 representatives included Huawei (5), China Mobile (3), ZTE (1), Lenovo via its subsidiary Motorola Mobility (1), and China Academy of Telecommunications Technology (1). Compiled by Commission staff from 3GPP website; 3GPP, "Specification Groups."

‡In 2017, the United States' 14 representatives were Qualcomm (4), Intel (3), Sprint (2), NEC Corporation (1), InterDigital (1), Motorola Solutions (1), Apple (1), and AT&T (1). Compiled by Commission staff from 3GPP website; 3GPP, "Specification Groups."

§ISO is composed of 162 national standards body subscribers. Companies or individuals can participate but cannot become members, and there is only one member representative per country. ISO cooperates with ITU, the International Electrotechnical Commission, and the World Trade Organization to set global consensus-based standards. ISO, "All About ISO—Structure and Governance."; ISO, "ISO in Figures 2017."

¶The two countries with the highest technical committee participation as of September 2018 were France (741) and the UK (735). International Organization for Standardization, "ISO: A Global Network of National Standards Bodies."

**This figure includes technical committee and subcommittee secretariats and working group convenors. International Organization for Standardization, "ISO in Figures 2012."; International Organization for Standardization, "ISO in Figures 2017."

ish competitor, to become the world's largest telecommunications equipment manufacturer, with 28 percent of the $37.2 billion in mobile infrastructure hardware revenue.[109] ZTE is the fourth largest, with 13 percent.[110] Huawei supplied more than half of the 537 global 4G networks and roughly two-thirds of the 90 global 4G LTE networks in 2016.[111] Stefan Pongratz, an industry analyst at the research firm Dell'Oro, stated, "Existing network footprint is important because operators still need to maintain their legacy … networks and could save money by using the same vendors."[112] Huawei has signed Memoranda of Understandings—a necessity for future contracts—with at least 45 telecommunications operators to try Huawei's 5G networks equipment, including Germany's Deutsche Telekom, Britain's BT, and Bell Canada.[113] By comparison, Ericsson has signed 38 and Finnish firm Nokia has signed 31.[114] Beyond telecommunications equipment, Huawei is the world's second-largest firm in Ethernet switches and routers based on 2017 revenue, after U.S. telecommunications firm Cisco.[115]

Table 3: World's Largest Firms in Select Telecommunications Technologies, 2017

Key Technologies	Leading Firms (global market share based on revenue)
Mobile infrastructure hardware	Huawei (28 percent), Ericsson (27 percent), Nokia (23 percent), and ZTE (13 percent)
Enterprise wireless local area network (WLAN)	Cisco (43.6 percent), Aruba Networks* (14.9 percent), ARRIS/Ruckus† (5.9 percent), Ubiquiti‡ (5.6 percent), and Huawei (5 percent)
Ethernet switches	Cisco (54.9 percent), Huawei (8.3 percent)
Routers	Cisco (36.7 percent), Huawei (23.8 percent), Juniper (18 percent)
Smartphone semiconductors	Qualcomm (42 percent); Apple (22 percent); MediaTek§ (15 percent)

Note: Mobile infrastructure hardware comprises radio access network, switching, and core equipment.
Source: Various.[116]

Based on share of 2017 global revenue, U.S. firm Cisco is the world leader in enterprise WLAN equipment (which provides communication networks), Ethernet switches (which manage network traffic), and routers (which forward data between networks).[117] The U.S. network technology firm Juniper is the world's third-largest firm in the $15.2 billion global router market at 18 percent after Huawei (23.8 percent).[118] Qualcomm and Apple together accounted for 64 percent of the $20.2 billion in 2017 global revenue in smartphone

*Hewlett Packard Enterprise's subsidiary, Aruba Networks, is a U.S.-based wireless network switch technology company. Aruba, "Networking Products."
†ARRIS/Ruckus is a U.S-based wireless network technology, equipment, and software company. In December 2017, U.S. firm ARRIS completed its acquisition of U.S.-based firm Ruckus Wireless. ARRIS, "Investors"; Rukcus Wireless, "ARRIS Completes Acquisition of Rukus Wireless and ICX Switch Business," December 1, 2017.
‡Ubiquiti Networks is a U.S.-based wireless network technology firm. Ubiquiti Networks, "Investor Relations."
§MediaTek is a Taiwan-based fabless semiconductor firm. MediaTek, "About MediaTek."

semiconductors, which allow smart phones to connect to telecommunications networks.[119]

In addition, U.S. firms such as Qualcomm and Intel remain global leaders in wireless technology IP development but are facing greater competition from China in the development of 5G-essential patents. Based on 2016 estimates from IP law firm LexInnova Technology, Chinese firms—led by Huawei and ZTE—already own almost 10 percent of the essential 5G IP patents, nearly a ten-fold increase from the number of patents they registered for 4G-LTE.[120] By comparison, U.S. firms Qualcomm, InterDigital, and Intel together own roughly 31 percent of 5G-essential IP patents.[121] Edison Lee, an analyst with the investment firm Jeffries Franchise, expects Chinese firms to control up to 20 percent of essential 5G patents given their significant R&D investments.[122]

U.S., Chinese, South Korean, and Japanese telecommunications providers are rushing to deploy 5G networks in the next two years.[123] First mover advantage in deployment will create new revenue streams from expanded use of the IoT and other 5G-enabled technologies and enable faster advancements in a country's development.[124] Previous U.S. leadership in 4G and 4G-LTE deployment provided the United States a competitive edge in testing and commercializing mobile phone, social network, and streaming applications.[125] The telecommunications research firm Recon Analytics found that U.S. 4G leadership contributed to around $125 billion in U.S. company revenue from abroad and more than $40 billion in U.S. application and content developer revenue, and created 2.1 million new jobs from 2011 to 2014.[126]

U.S. telecommunications providers are set to deploy 5G networks first with a nationwide roll-out occurring in stages. U.S. telecommunications provider AT&T plans to deploy 5G networks in 15 cities by December 2018; T-Mobile plans to deploy 5G networks in 30 cities in 2018 but noted that 5G-compatible phone service would not be available until 2019.[127] By comparison, China Tower is aiming to deploy 5G nationwide between 2019 and 2021.[128] Already, China Tower is investing more and constructing cellular infrastructure faster and in greater numbers than the United States.[129] Based on estimates from the consulting firm Deloitte, China Tower constructed more cellular network sites in three months than U.S. firms added in the last three years.[130] China now surpasses the United States, with 14.1 sites per 10,000 people and 5.3 sites per 10 square miles as compared to the United States at 4.7 and 0.4 respectively.[131] Additionally, since 2015, China has annually outspent the United States by $8 billion to $10 billion in wireless infrastructure construction.[132]

U.S. Market Access in China

The Chinese government guarantees Huawei and ZTE two-thirds of domestic 5G network contracts.[133] Foreign firms have to compete with other Chinese firms for the remaining one-third.[134] Samm Sacks, senior fellow at the Center for Strategic and International Studies, identified three additional regulatory barriers for U.S. telecommunications firms operating in China: "cybersecurity reviews, restrictions on cross-border data transfer, and an

overall trend toward localization under the guise of security."[135] She noted that U.S. IT and telecommunications firms face several security reviews that "can be used for political purposes to delay or block market access."[136] These reviews are nontransparent and cover critical information systems, cybersecurity and supply chain risks of network products and services, cross-border data transfers, internal virtual private network services, internet technologies and applications, personal data and important data protection, encryption, and foreign investment.[137]

Chinese Market Access in the United States

Chinese telecommunications firms such as Huawei, ZTE, and China Mobile have limited access to the U.S. telecommunications market and have struggled to acquire* U.S. firms and other U.S. assets. Huawei and ZTE provide low-cost network equipment for small, rural telecommunications carriers (e.g., Sagebrush Cellular and United Wireless) but not for larger carriers such as AT&T and Verizon due to longstanding security concerns (see "National Security Risks Associated with Major Chinese Telecommunications Firms" later in this section).[138] In March 2018, the FCC proposed barring the use of money from its nearly $9 billion Universal Service Fund† to "purchase or obtain any equipment or services produced or provided by any company posing a national security threat to communications networks or the communications supply chain," such as ZTE and Huawei.[139] As of October 9, 2018, the FCC was seeking public input on the implementation of this proposal.[140] If enacted, this measure would limit Huawei and ZTE's market access to rural U.S. wireless providers, who are dependent on the Universal Service Fund.

In January 2018, the U.S. government reportedly pressured AT&T and Verizon to stop selling Huawei smartphones in the United States.[141] In March 2018, Best Buy announced it would stop selling Huawei smartphones, laptops, and smartwatches in the United States; as of October 2018, Huawei products were still available for purchase on their website.[142] In May 2018, DOD spokesperson Dave Eastburn stated that "Huawei and ZTE devices may pose an unacceptable risk to the department's personnel, information and mission. In light of this information, it was not prudent for the department's exchanges to continue selling them."[143] DOD is considering a wider advisory on military personnel's purchase of Huawei and ZTE devices for personal use.[144]

Additionally, President Donald Trump signed into law restrictions on U.S. government agencies or government contractors using or procuring telecommunications or video surveillance equipment or services from Huawei, Hytera Communications Corporation, Hikvision, Dahua Technologies, ZTE, or other entities controlled by the Chinese government.[145] Agencies can obtain waivers from agency heads and the director of national intelligence; purchases by private firms such as AT&T and Verizon are not covered.[146]

---

*In 2008, Huawei withdrew from a deal to purchase U.S. software firm 3Com, which supplied network security software to the U.S. military, because the deal would not pass CFIUS review. Richard Waters, "Huawei-3Com Deal Finally Collapses," *Financial Times*, March 21, 2008.

†U.S. telecommunications firms contribute a percentage of their end user interstate and international end user revenues to the Universal Service Fund, which subsidizes telecommunications service to low-income households and high-cost areas. United Service Administration Co., "Universal Service"; U.S. Federal Communications Commission, *Universal Service Fund*.

National Security Risks Associated with Major Chinese Telecommunications Firms

Telecommunications are integral for critical infrastructure (e.g., public utilities or banking), businesses, governments, and society.[147] The Chinese government seeks to maintain a capability to hold U.S. and other foreign telecommunications networks at risk and leverage these networks for espionage.[148] Beyond direct control over its state-owned firms, the Chinese government maintains significant influence over private Chinese firms through financial incentives, political arrangements, and agreements among company shareholders.[149] The Chinese government could leverage this influence to pressure Chinese suppliers or manufacturers to modify products or otherwise compromise telecommunications network equipment.[150] The U.S., Australian, British, and other foreign governments are concerned that the Chinese government's involvement could compromise their networks.[151] Select concerns associated with four Chinese companies are highlighted below:

- *Huawei:* Huawei has long sought to enter the U.S. market, but its close ties to China's political and military leadership have raised significant national security concerns.[152] Its founder, Ren Zhengfei, served as an officer in the People's Liberation Army, and a 2002 book quoted Mr. Ren as saying, "If there had been no government policy to protect [nationally owned companies], Huawei would no longer exist."[153] In 2012, an investigation by the U.S. House of Representatives Permanent Select Committee on Intelligence concluded "that the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national-security interests."[154] Australia banned Huawei from supplying its National Broadband Network in 2012 and banned Huawei and ZTE from participating in its 5G broadband network in August 2018.[155]
- *ZTE:* In 2012, Congress expressed concerns about the degree of Chinese government influence as ZTE's largest shareholder, and ZTE's role in China's military R&D.[156] In April 2018, the United Kingdom's (UK) National Cyber Security Center assessed that "the national security risks arising from the use of ZTE equipment or services within the context of the existing UK telecommunications infrastructure cannot be mitigated"—in effect barring ZTE from the UK telecommunications market.[157] Beyond national security risks, the U.S. Department of Commerce fined ZTE for violation of U.S. export laws in 2016 and again in 2018 for noncompliance with the earlier settlement (for more information, see Chapter 1, Section 1, "Year in Review: Economics and Trade").
- *China Mobile:* In September 2011, state-owned China Mobile applied to the FCC to be a U.S. common carrier.[158] If approved, China Mobile would be able to "carry international voice traffic between the United States and foreign countries and to interconnect such traffic with the U.S. telecommunications network."[159] In July 2018, the U.S. government assessed that China Mobile "is vulnerable to exploitation, influence, and control by the Chinese government" and "would likely comply with

requests made by the Chinese government."[160] The U.S. Departments of Justice, Homeland Security, Defense, State, and Commerce, as well as the Office of the U.S. Trade Representative and the Office of Science and Technology Policy, recommended that the FCC deny China Mobile's 2011 application to offer telecommunications services as an international common carrier in the United States, citing "substantial and unacceptable national security and law enforcement risks."[161] In August 2018, China Mobile formally challenged this recommendation.[162] In September 2018, the U.S. Departments of Justice, Homeland Security, Defense, State, and Commerce, as well as the Office of the U.S. Trade Representative and the Office of Science and Technology Policy responded to China Mobile's petition and reiterated their recommendation that the FCC deny China Mobile's application.[163] As of October 9, 2018, the FCC has not reached a decision.

- *China Electronics Technology Group:* In August 2018, the U.S. Department of Commerce found that state-owned China Electronics Technology Group was involved in the "illicit procurement of commodities and technologies for unauthorized military end-use in China."[164] In response, the U.S. Department of Commerce imposed export licensing and review requirements on all items subject to Export Administration Regulations to be sold or used by China Electronics Technology Group and 12 of its subordinate institutions.[165]

Implications for the United States

The IoT and 5G are transforming how countries conduct business, fight wars, and interact as a society. The Chinese government seeks to overtake the United States in these industries to gain a higher share of the economic benefits and technological innovation. Chinese firms have leveraged strong state support to become global leaders in IT and network equipment manufacturing, and to strengthen their roles in global 5G standards-setting and deployment. The scale of Chinese state support for the IoT and 5G undermines the ability of U.S. firms to compete fairly either within China or in third markets.

As Chinese companies gain prominence in the IoT and 5G, U.S. dependence on Chinese manufacturers will deepen. In addition, the rapid advances in the number and capabilities of IoT devices and 5G networks are strengthening military capabilities, expanding U.S. data privacy and security risks, and worsening U.S. cybersecurity vulnerabilities. But China's leadership in these industries is not a foregone conclusion. Continued innovation from U.S. companies will extend the United States' technological edge, and rising cost pressures may force Chinese manufacturing to move to Southeast Asia, potentially diversifying U.S. supply chains in the long term.[166]

The Internet of Things

The scale of Chinese state support for the IoT, the close supply chain integration between the United States and China, and China's role as an economic and military competitor to the United States create enormous economic, security, supply chain, and data privacy

risks for the United States.[167] The United States is well positioned to take advantage of the expected $4 trillion to $11 trillion in productivity, economic growth, jobs, and novel capabilities the IoT creates.[168] But the Chinese government leverages its large domestic market and whole-of-government approach to supplant U.S. firms with its own.[169] U.S. semiconductor, cloud computing, and autonomous vehicle firms face high market access barriers and must partner with Chinese companies—their future competitors—to gain access to China's market.[170] In addition, the Chinese government has rolled out localization targets, China-specific technical standards, and significant state support to create globally competitive IoT firms.[171] Losing this advantage will weaken U.S. firms' competitive edge in high-value-added sectors of the future economy, and will undermine the capabilities, capacity, and resilience of the U.S. defense industrial base.

Supply Chain Vulnerabilities

China's central role in IT and IoT device manufacturing, combined with its position as an economic and military competitor of the United States, creates extensive supply chain vulnerabilities. The degree of risk depends on the type of product; who produces it and at what stage; the production location; the commercial, financial, and other relationships the producer and its suppliers have; and the end user.[172] China's large market and dominance of IT and IoT manufacturing provide the Chinese government leverage in extracting concessions from leading foreign firms.[173]

The Chinese government—which exerts strong influence over its firms—may force Chinese suppliers or manufacturers to modify products to perform below expectations or fail, facilitate state or corporate espionage, or otherwise compromise the confidentiality, integrity, or availability of IoT devices.[174] These risks are higher for the U.S. government, which depends on commercial-off-the-shelf (COTS) products for over 95 percent of its electronics components and IT systems.[175] While COTS products are generally lower in cost and available faster than government-developed or government-customized products, Gregory Falco, research fellow at Harvard University Kennedy School's Belfer Center, warned:

> *(1) the wide distribution of COTS products means that many people have access to the devices, so a hacker can extensively analyze the device for vulnerabilities, (2) COTS products need to be actively maintained and upgraded for security patches that are often not applied by users, and (3) anyone could have contributed to the code behind open source technology, which means that vulnerabilities or backdoors to the software could be intentionally planted by adversaries.*[176]

In addition, Jennifer Bisceglie, chief executive officer at the supply chain risk management firm Interos, noted in her oral testimony before the Commission that the U.S. government "lacks a consistent, holistic supply chain risk management approach" to address such risks due to conflicting and confusing federal procurement laws and regulations and inconsistently applied procurement policies.[177] For example, in 2018, DOD's inspector general found that DOD incorpo-

rated COTS drones—largely from China—into its operations without an adequate assessment of their cybersecurity risks or a mitigation strategy.[178] In June 2018, DOD's inspector general expanded its audit on DOD cybersecurity and physical security assessments and mitigation strategies for other COTS products.[179]

Security Vulnerabilities

Advancements in the IoT are strengthening military capabilities, but can worsen global cybersecurity threats without proper risk management. The IoT will yield significant military technological advantages in strategic deterrent and warfare capabilities, C4ISR, and supply chain management, and will create future asymmetric battlefield capabilities such as swarms of drones.[180] For example, China's advancements in unmanned undersea drones and networks of undersea sensors are enhancing China's detection of U.S. submarines and undersea assets, eroding the ability of the United States to operate freely in the region.[181]

The rapid proliferation of IoT devices is outstripping industry standards and worsening global cybersecurity risks.[182] A May 2018 report by the U.S. Department of Homeland Security and U.S. Department of Commerce found that "product developers, manufacturers, and vendors are motivated to minimize cost and time to market, rather than to build in security or offer efficient security updates."[183] The research firm Ponemon Institute's 2017 survey of 593 mobile and IoT application developers and users found that vendors test only 20 percent of IoT applications for vulnerabilities; of the ones that are tested, an average of 38 percent contain significant vulnerabilities.[184] Additionally, once an IoT device is sold, few firms provide lifecycle management to ensure discovered software vulnerabilities are fixed.[185]

Daniel R. Coats, Director of National Intelligence, warned in May 2017,

> *Our adversaries are likely to seek capabilities to hold at risk U.S. critical infrastructure as well as the broader ecosystem of connected consumer and industrial devices known as the "Internet of Things" (IoT) … Their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks.*[186]

The universal connectivity of unsecured IoT devices could enable the remote exploitation* of a device to deny service, eavesdrop, or be used in a botnet for a cyber attack (see Table 4).[187] In 2017, the U.S. cybersecurity software firm Symantec found a 600 percent year-on-year increase in the number of IoT attacks.[188] Mr. Benson noted

*For example, the Tel Aviv-based startup firm Toka is developing cyber tools that can exploit vulnerabilities in IoT devices for government surveillance. Thomas Fox-Brewster, "Alexa, Are You a Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT," *Forbes*, July 15, 2018.

that the shortage of trained staff, insufficient risk assessments, and lack of capacity contribute to misconfigured and poorly managed IoT systems, limit the value added, and degrade cybersecurity for the end user (e.g., city, institutional campus, or military base).[189] In addition, Mr. Benson warned that "there's no limit on the type of data that could be sent back if something was maliciously developed or there's a vulnerability in it."[190]

Table 4: Potential Vulnerabilities of IoT Technologies

	Device	Communication Network	Data
Types of Vulnerabilities	• Hardware • Firmware • Software • Sensor failure • Default passwords • Denial-of-service attack	• Compromised or fake communication network (e.g., Wi-Fi or cellular) • Denial-of-service attack	• Software • Unsecure or compromised communication network
Risks	• Modification of firmware, hardware, or software without authorization • Unauthorized access to information or services • Loss of service	• Loss of service • Physical tracking of user • Unauthorized access to information or services	• Unauthorized access to information • Physical tracking of user • Modification of data without authorization • Impersonating a device, user, or recipient

Source: Adapted from Zubair A. Baig, "Future Challenges for Smart Cities: Cyber-Security and Digital Forensics," *Digital Investigation*, August 15, 2017; U.S. Department of Homeland Security and the National Institute of Standards and Technology, *Study on Mobile Device Security*, April 2017, 18.

The U.S. Office of Management and Budget and the U.S. Department of Homeland Security's May 2018 report evaluated 96 agencies' cybersecurity risk mitigation programs and found 59 agencies at risk and 12 at high risk.[191] Federal agencies could not identify the method of attack for 38 percent of the 30,899 cyber incidents that compromised information or information system functionality in 2016.[192] Furthermore, only 27 percent of federal agencies have the ability to detect and investigate attempts to access large volumes of data, and only 16 percent of federal agencies met the government-wide target for encrypting stored data.[193] Protecting U.S. national security from malicious cyber actors will become harder as the technology gets more complex, diverse, and abundant, and embedded within existing physical structures.[194] In a 2018 report prepared for the Commission,* Interos found that "software supply chain attacks will become easier—and more prevalent—as developing technologies such as fifth generation (5G) mobile network technology and the IoT exponentially increase the avenues for attack."[195]

*For an analysis of federal information and communications technology vulnerabilities from China, see Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018.

Hackers are creating ever larger botnets from the rapid growth in unsecure IoT devices to launch record-breaking denial-of-service attacks.[196] For example, in September 2016, hackers exploited the lax security settings on Chinese firm Dahua Technology's IoT security cameras to create a massive botnet that launched one of the world's largest denial-of-service attacks on a well known cybersecurity blog.[197] In October 2016, hackers utilized weak default usernames and passwords on Chinese firm Hangzhou Xiongmai Technology's IoT security cameras and digital video recorders to launch a denial-of-service attack against U.S. domain name system provider Dyn.[198] This large-scale attack temporarily prevented internet access to the websites of major U.S. firms such as Twitter, Spotify, PayPal, GitHub, the *New York Times*, and the *Boston Globe*.[199] The Seattle-based cybersecurity firm F5 found that during the July 2018 meeting between President Trump and Russian President Vladimir Putin in Finland, 34 percent of the brute force attacks against Finland's ports and protocols originated in China; around 62 percent of the attacks were targeting SSH protocol (commonly used for "secure" remote administration of IoT devices).[200]

Data Privacy and Security Risks

IoT devices collect enormous amounts of user information. In 2016, an investigation by 25 countries' government data protection regulators found that 60 percent of the more than 300 reviewed IoT devices did not "provide adequate information on how personal data is collected, used and communicated to third parties."[201] In addition, when user data are aggregated and combined with greater computing power and massive amounts of publicly available information, the data can reveal information the user did not intend to share—even if the data have been anonymized per federal regulations.[202]

Location-based data are widely collected and "generat[e] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about … familial, political, professional, religious, and sexual associations."[203] For example, in January 2018 researchers cross-referenced location-based data collected by the U.S. exercise tracking application Strava with Google Maps to reveal the location of military bases and patrol routes and track an individual's movements.[204] In August 2018, DOD issued a department-wide edict that immediately banned geolocation-capable non-government- and government-issued devices, applications, and services (e.g., fitness trackers, smart phones, and smart watches) in operational areas.*[205] DOD cited the exposure of "personal information, locations, routines, and numbers of DoD personnel" and the potential of "unintended security consequences and increased risk to the joint force and mission" as reasons for the ban.[206]

Despite the amount of information these data can reveal, the U.S. Government Accountability Office found "there is no overarching federal privacy law that covers the collection and sale of … personal information among private-sector companies. There are also no federal laws designed specifically to address all the products sold and information maintained by information resellers."[207] Existing U.S.

*Operational area refers to geographic areas in which military operations are conducted. U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, June 2018, 172.

data protections are limited to children under 13, financial information, credit, medical records, or deceitful business practices (see Table 5). The amount of data collected, the value of such data to criminal and state actors, and lax security and legal protections are creating privacy, safety, and security risks for U.S. citizens, businesses, and democracy.[208]

Table 5: U.S. Laws on Data Collection, Use, and Protection

U.S. Laws	Protections
Federal Trade Commission Act	Unfair or deceptive practices by companies
Financial Services Modernization Act	Collection, use, and disclosure of financial information by banks, security firms, insurance companies, or other financial services and product businesses
Fair Credit Reporting Act	Accuracy, collection, use, and disclosure of medical records, housing, credit, and employment information by consumer reporting agencies and other relevant agencies
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Data collected, stored, or sent by or to healthcare providers and their business associates, healthcare insurance firms, or medical billing clearing houses
Children's Online Privacy Protection Act of 1998	Collection or storage of personal information on children under the age of 13 by website operators, online services, and operators of websites or online services

Source: Various.[209]

Chinese firms are increasing their access to U.S. customer data through IoT products and services. Similar to U.S. firms, Chinese firms aggregate these data with their global customers to enhance their product and service offerings, among other uses. For example, Chinese dockless bikesharing firms Ofo and Mobike reserve the right to transmit, store, and process U.S. customer data outside of the United States.[210] Some U.S. firms have also agreed to share data on U.S. customers with their Chinese partners. For example, Facebook shared user data and contents—without explicit permission—with at least 60 device manufacturers, including Chinese mobile device manufacturers Huawei, Lenovo, OPPO, and TCL.[211] On June 6, 2018, Facebook announced it had ended more than half its 60 partnerships, including ones with Huawei, Lenovo, OPPO, and TCL.[212]

Chinese IoT devices may also expose U.S. data because IoT developers, vendors, and manufacturers did not thoroughly check components, firmware, or software for security vulnerabilities before bringing the product to market.[213] For example, lax security settings on IoT surveillance cameras from Dahua and Hikvision exposed thousands of customers to remote exploitation and monitoring before the companies released security patches.[214] And, once deployed, IoT devices often lack update protocols, leaving them vulnerable as new threats evolve.

The Chinese government retains expansive powers to access personal and corporate data in order to support its domestic firms, maintain control over its citizens, enhance governance, and ensure the security of sensitive data and related infrastructure.[215] The Chi-

nese government could potentially force Chinese firms to provide access to data collected on U.S. users—data that, when aggregated and analyzed, could reveal sensitive information.[216] For example, U.S. Immigration and Customs Enforcement in August 2017 alleged that DJI's commercial drones and software likely provided the Chinese government "with first and secondhand access" to U.S. critical infrastructure and law enforcement data.[217] The sharing of such sensitive data with the Chinese government—an economic and military competitor—could facilitate China's ability to coordinate physical or cyber attacks against U.S. critical infrastructure.[218] DJI denied these allegations.[219]

5G Wireless Technology

Huawei and ZTE are competing against U.S. companies for 5G IP and an expected $12.3 trillion in economic output, creating new challenges for the secure deployment of critical next generation telecommunications infrastructure in the United States.[220] As Doug Brake, director of telecommunications policy at the Information Technology and Innovation Foundation, noted, the "successful deployment of next generation wireless is a matter of national competitiveness."[221]

U.S. leadership in 4G spurred rapid advancements in mobile phone applications.[222] Setting international standards provides a country a competitive edge in subsequent technology development. In a 2016 report prepared for the Commission, the University of California Institute on Global Conflict and Cooperation warned:

> *If China leads in 5G technology, U.S. telecommunication companies could lose significant amounts of royalty income on patents. Chinese telecommunication companies have been able to negotiate waivers of royalty payments to U.S. semiconductor firm Qualcomm for TD-SCDMA and TD-LTE networks. However, they are still paying high licensing fees to Qualcomm when using the CDMA, WCDMA (3G), and FDD-LTE (4G) standards.*[223]

The loss of these licensing and royalty payments will affect the ability of U.S. firms to continue reinvesting in R&D, maintaining brand recognition, and achieving economics of scale, key factors in a firm's long-term economic competitiveness. In addition, if U.S. firms become uncompetitive (as they currently are in network equipment manufacturing), the United States will need to rely on foreign suppliers, creating supply chain vulnerabilities and a potential loss in the United States' technological edge. Mark Natkin, managing director of Marbridge Consulting, noted that beyond a commercial advantage, owning a significant portion of the patents is also a security advantage: "Whoever controls the technology knows, intimately, how it was built and where all the doors and buttons are."[224]

Supply Chain Vulnerabilities

U.S. telecommunications providers, particularly larger carriers such as AT&T and Verizon, lack U.S. network equipment suppliers and rely on global supply chains that Chinese firms and manufacturing dominate. Although they do not source from Huawei and ZTE, U.S. telecommunications providers (including AT&T, Sprint,

and T-Mobile) rely on other foreign 5G network equipment suppliers (such as Ericsson, Nokia, and Samsung) that incorporate Chinese manufacturing and assembly facilities into their global supply chains.[225] Even in enterprise WLAN, Ethernet switches, and routers—areas in which U.S. firm Cisco dominates—over a third of Cisco's total shipments between 2012 and 2017 originated in China (largely from Cisco's Chinese subsidiaries).[226]

While Cisco and other foreign firms may exert control over the location security, staff hiring, manufacturing, and quality control practices at their Chinese subsidiaries, these subsidiaries operate in a country where the government exerts significant influence over its businesses and legal systems.[227] This reliance on China-based manufacturing and the degree of Chinese government influence could provide opportunities for the Chinese government to force Chinese suppliers or manufacturers to modify products, facilitate espionage, or otherwise compromise telecommunications equipment.[228]

In February 2018, U.S. Federal Bureau of Investigation Director Christopher Wray reiterated longstanding concerns about the United States' use of products and services from Huawei—the world's largest telecommunications equipment manufacturer—stating:

> *We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks. That provides the capacity to exert pressure or control over our telecommunications infrastructure. It provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage.*[229]

In addition, U.S. allies and partners in Europe and Latin America have placed a greater share of their data and message traffic on Chinese-supplied telecommunications networks, potentially compromising their networks and facilitating China's intelligence collection.[230]

Security Vulnerabilities

Telecommunications networks are inherently vulnerable and targeted due to their critical importance to every facet of U.S. government, business, and society.[231] U.S. telecommunications infrastructure is largely built, owned, and operated by the private sector, which often prioritizes profit maximization over national security.[232] According to an April 2017 report by the U.S. Department of Homeland Security and U.S. National Institute of Standards and Technology, "There are no regulations requiring carriers to run encryption or provide privacy protections to users on their network."[233] FCC Chairman Ajit Pai warned, "[H]idden 'back doors' to our networks in routers, switches—and virtually any other type of telecommunications equipment—can provide an avenue for hostile governments to inject viruses, launch denial-of-service attacks, steal data, and more."[234]

For example, the existing routing systems used by major U.S. and foreign telecommunications carriers—Signaling System 7 and Diameter—contain longstanding cybersecurity vulnerabilities.[235] Foreign

governments exploit these vulnerabilities to track users, intercept calls and texts, and steal sensitive data.[236] A March 2018 report by the EU Agency for Network and Information Security found that around 72 percent of the 39 EU telecommunications providers surveyed believed the same routing vulnerabilities in 2G, 3G, and 4G will be present in 5G.[237] These vulnerabilities, combined with the greater speed and capacity of 5G networks, will increase the power and speed of malicious cyber attacks.[238]

According to a February 2017 report by the U.S. Defense Science Board, the Chinese and Russian governments are capable of holding existing U.S. telecommunications networks and other critical U.S. infrastructure at risk due to their massive resources and intelligence, supply chains, and cyber capabilities.[239] These governments could use their growing capabilities to undermine U.S. military responses, economic growth, financial services and systems, political institutions, and social cohesion.[240] In addition, the United States is increasingly dependent on China for IT and telecommunications manufacturing, creating supply chain vulnerabilities the Chinese government could exploit.

ENDNOTES FOR SECTION 1

1. International Monetary Fund, "World Economic Outlook," April 2018.
2. U.S.-China Economic and Security Review Commission, *Economics and Trade Bulletin*, July 9, 2018, 9–11; U.S. Department of Justice, *Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases*, January 2018; Mark Chandler, "Huawei and Cisco's Source Code: Correcting the Record," *Cisco*, October 11, 2012; Jameson Berkow, "Nortel Hacked to Pieces," *Financial Post*, February 25, 2012; Phil Wahba and Melanie Lee, "Motorola Sues Huawei for Trade Secret Theft," *Reuters*, July 22, 2010; Jamil Anderlini, "Motorola Claims Espionage in Huawei Lawsuit," *Financial Times*, July 21, 2010.
3. Frank Desvignes, "The Internet of Things Made in China," *AXA*, October 5, 2016; U.S. National Institute of Standards and Technology, *What is the Internet of Things (IOT) and How Can We Secure It?*
4. Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region," February 26, 2018; Laura Bliss, "Are Dockless Bikes a Cybersecurity Threat?" *City Lab*, February 15, 2018.
5. People's Republic of China, *Outline of the People's Republic of China's 13th Five-Year Plan on National Economic and Social Development*, March 17, 2016. Translation. *http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm*; State Council of the People's Republic of China, *State Council's Guidance on Actively Promoting the Internet Plus Action Plan*, July 1, 2015. Translation. *http://www.gov.cn/gongbao/content/2015/content_2897187.htm*; State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015. Translation. *http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm*.
6. State Council of the People's Republic of China, *State Council's Guidance on Actively Promoting the Internet Plus Action Plan*, July 1, 2015. Translation. *http://www.gov.cn/gongbao/content/2015/content_2897187.htm*.
7. Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 17.
8. People's Republic of China, *Outline of the People's Republic of China's 13th Five-Year Plan on National Economic and Social Development*, March 17, 2016. Translation. *http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm*; State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015. Translation. *http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm*.
9. U.S. Chamber of Commerce, "Made in China 2025: Global Ambitions Built on Local Protectionism," March 16, 2017, 7.
10. U.S. Government Accountability Office, *Internet of Things: Status and Implications of an Increasingly Connected World*, May 2017, 16–17; Denise E. Zhang and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military," *Center for Strategic and International Studies*, September 2015, 14.
11. Denise E. Zhang and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military," *Center for Strategic and International Studies*, September 2015, 13–16.
12. Tate Nurkin et al., "China's Advanced Weapons Systems," *Jane's by IHS Markit* (prepared for the U.S.-China Economic and Security Review Commission) May 10, 2018, 150–176.
13. GSMA, "The Mobile Economy 2018," May 2018, 7, 24; Jenalea Howell, "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says," *IHS Markit*, October 24, 2017; GSMA, "GSMA Articles of Association—Version 3.18," December 1, 2014.
14. James Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype," *McKinsey Global Institute*, June 2015, 4, 112, 116–117.
15. James Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype," *McKinsey Global Institute*, June 2015, 112.
16. GSMA, "The Mobile Economy 2018," May 2018, 51; U.S. Department of Defense, Missile Defense Agency, *Element: Command and Control, Battle Management, and Communications*, April 20, 2018; Matej Tonin, "The Internet of Things: Promises and Perils of a Disruptive Technology," *NATO Parliamentary Assembly*, October 8, 2017; Cathy Nolan, "Using the Internet of Things to Track Shoppers," *Dataversity*, February 13, 2017; Denise E. Zhang and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military," *Center for Strategic and International Studies*, September 2015, 6, 14; Joe Mariani, Brian Williams, and Brett Loubert, "Continuing the March: The Past, Present, and Future of the IoT in the Military," *Deloitte*, August 6, 2015.

17. TechTarget, "Smart Home or Building," October 2017; Anurag Saikar et al., "TrafficIntel: Smart Traffic Management for Smart Cities," *IEEE*, July 13, 2017; Denise E. Zhang and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military," *Center for Strategic and International Studies*, September 2015.
18. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Chuck Benson, March 8, 2018, 4.
19. Brice Murara, "5G," *International Telecommunication Union*; Ellen Warren, "5G Is Totally Changing How We Connect," *Nokia*, March 16, 2018.
20. U.S. Government Accountability Office, *Internet of Things: Status and Implications of an Increasingly Connected World*, May 2017, 4–6.
21. State Council of the People's Republic of China, *State Council's Guidance on Actively Promoting the Internet Plus Action Plan*, July 1, 2015. Translation. *http://www.gov.cn/gongbao/content/2015/content_2897187.htm*; State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015. Translation. *http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm*; *People's Daily*, "China's Internet of Things Center Will Hopefully Settle in Shanghai," February 23, 2010. Translation.
22. People's Republic of China, *Outline of the People's Republic of China's 13th Five-Year Plan on National Economic and Social Development*, March 17, 2016. Translation. *http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm*; Central Compilation and Translation Press, Central Committee of the Communist Party of China, *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China*.
23. Kane Wu, Julie Zhu, and Cate Cadell, "Exclusive: Chip Wars - China Closing in on Second $19 Billion Semiconductor Fund: Sources," *Reuters*, April 26, 2018; Paul Mozur and John Markoff, "Is China Outsmarting America in A.I.?" *New York Times*, May 27, 2017; Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 23; *Xinhua*, "China Establishes Fund to Invest in Advanced Manufacturing," June 8, 2016; PricewaterhouseCoopers, "A Decade of Unprecedented Growth: China's Impact on the Semiconductor Industry 2014 Update," January 2015, 74.
24. U.S.-China Business Council, "Unofficial USCBC Chart of Localization Targets by Sector Set in the MIIT Made in China 2025 Key Technology Roadmap," February 2, 2016; Chinese Academy of Engineering, Expert Commission for the Construction of a Manufacturing Superpower, *Made in China 2025 Key Area Technology Roadmap*, October 29, 2015. Translation, 40, 26, 114. *http://www.cae.cn/cae/html/files/2015-10/29/20151029105822561730637.pdf*.
25. U.S.-China Economic and Security Review Commission, *Economics and Trade Bulletin*, July 9, 2018, 9–11; U.S. Department of Justice, *Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and and Sanctions-Related Criminal Cases*, January 2018.
26. U.S. Attorney's Office, Northern District of California, *Former Apple Employee Indicted on Theft of Trade Secrets*, July 16, 2018; U.S. District Court for Northern California, *United States of America v. Xiaolang Zhang*, C.R. 18.70919, July 9, 2018.
27. U.S.-China Economic and Security Review Commission, *Economics and Trade Bulletin*, July 9, 2018, 9–11; U.S. Department of Justice, *Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and and Sanctions-Related Criminal Cases*, January 2018.
28. Stéphane Téral, "Global Mobile Infrastructure Market Down 14 Percent from a Year Ago," *IHS Markit*, March 13, 2018; U.S. Government Accountability Office, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, July 27, 2017; Frank Desvignes, "The Internet of Things Made in China," *AXA*, October 5, 2016; U.S. Department of Commerce, International Trade Administration, *2016 Top Markets Report Semiconductors and Related Equipment: A Market Assessment Tool for U.S. Exporters*, July 2016, 25, 28.
29. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 2.
30. Frank Desvignes, "The Internet of Things Made in China," *AXA*, October 5, 2016.
31. Stéphane Téral, "Global Mobile Infrastructure Market Down 14 Percent from a Year Ago," *IHS Markit*, March 13, 2018.
32. Elsa Kania, "Battle Field Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," *Center for a New American Security*, November 28, 2017.

33. Juniper Research, "IoT Connections to Grow 140% to Hit 50 Billion by 2022, as Edge Computing Accelerates ROI," June 12, 2018; Mike Robuck, "Report: Amazon Web Services Still Rules the Cloud Roost for Market Share," *Fierce Telecom*, April 27, 2018; Paige Tanner, "How the Semiconductor Industry Performed in 2017," *Markit Realist*, January 9, 2018.
34. Paige Tanner, "How the Semiconductor Industry Performed in 2017," *Markit Realist*, January 9, 2018.
35. Synergy Research Group, "Cloud Growth Rate Increased Again in Q1; Amazon Maintains Market Share Dominance," April 27, 2018; Synergy Research Group, "2017 Review Shows $180 Billion Cloud Market Growing at 24% Annually," January 4, 2018.
36. U.S.-China Economic and Security Review Commission, Chapter 4, Section 1, "China's Pursuit of Dominance in Computing, Robotics, and Biotechnology," in *2017 Annual Report to Congress*, November 2017, 518–520; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 184–192, 199–206.
37. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *Center for Strategic and International Studies*, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018.
38. Nick Marro, "Decoding China's Approach to Data Security," *Diplomat*, December 10, 2016; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation*, February 2015.
39. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation*, February 2015.
40. Tim Merel, "China Could Beat America in AR/VR Long-Term," *Tech Crunch*, May 2, 2018; Alexander Chipman Koty, "Investment Opportunities in China Open Up Following Regulatory Changes," *China Briefing*, September 19, 2017; Alexander Chipman Koty and Zhou Qian, "China's 2017 Foreign Investment Catalogue Opens Access to New Industries," *China Briefing*, July 11, 2017; Jing Sun et al., "mHealth for Aging China: Opportunities and Challenges," *Aging and Disease* 7:1 (January 2016): 53–67.
41. China's Ministry of Public Security, *Ministry of Public Security Draft for Comment for Multi-Level Protection Scheme on Internet Security*, June 27, 2018. Translation. *http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html*; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018, 9–10.
42. China's Ministry of Public Security, "*Ministry of Public Security Draft for Comment for Multi-Level Protection Scheme on Internet Security*, June 27, 2018. Translation. *http://www.mps.gov.cn/n2254536/n4904355/c6159136/contnt.html*; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018, 11.
43. BSA, "RE: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation (Docket No. USTR–2017–0016)," September 28, 2017; Scott Thiel, "Telecommunications Laws of the World: China," *DLA Piper*, May 25, 2017.
44. BSA, "Special 301 Submission," February 8, 2018; Gidon Gautel, "Establishing a Data Center in China," *China Briefing*, July 26, 2017; Norton Rose Fulbright, "China's New Telecom Catalogue Comes into Force on March 1, 2016," February 2016; Renee Barry and Matthew Reisman, "Policy Challenges of Cross-Border Cloud Computing (May 2012)," *Journal of International Commerce and Economics* 4:2 (November 2012).
45. Kelly Hill, "AT&T Extends Joint Venture with China Telecom," *RCR Wireless News*, June 27, 2017; *Business Cloud News*, "21Vianet, Microsoft Renew Vows on Chinese Public Cloud Services," April 7, 2015.
46. AT&T, "AT&T and China Mobile Collaborate on Internet of Things," February 26, 2017.
47. Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 56.
48. Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 56–57.
49. Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 56–57.

50. Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018; Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016, 56–57.
51. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *Center for Strategic and International Studies*, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018; *China Law Translate*, "2016 Cybersecurity Law." November 7, 2016.
52. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *Center for Strategic and International Studies*, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018; Nick Marro, "Decoding China's Approach to Data Security," *Diplomat*, December 10, 2016; Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries," *Information Technology and Innovation Foundation*, February 2015.
53. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *Center for Strategic and International Studies*, August 2018; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018, 9.
54. Dan Strumpf, Natasha Khan, and Charles Rollet, "Surveillance Cameras Made by China Are Hanging All Over the U.S.," *Wall Street Journal*, November 12, 2017; Hikvision, "About Hikvision North America"; OfO, "About OfO"; MoBike, "World's Largest Smart Bike Sharing Platform, Mobike, Rides into First U.S. City, Washington DC," September 19, 2017.
55. U.S. Federal Trade Commission, *Federal Trade Commission Act*; U.S. Federal Trade Commission, *Gramm-Leach Bliley Act*; U.S. Federal Trade Commission, *Fair Credit Reporting Act—Revised May 2016*; Federal Trade Commission, *A Summary of Your Rights Under the Fair Credit Reporting Act*; U.S. Department of Health and Human Services, Office of Civil Rights, interview with Commission staff, September 12, 2017; U.S. Department of Health and Human Services, Office of Civil Rights, *Covered Entities and Business Associates*, June 16, 2017; Federal Trade Commission, *Children's Online Privacy Protection Rule ("COPPA")*.
56. Haye Kesteloo, "DJI Dominates Drone Industry with a 72% Global Market Share," *DroneDJ*, September 19, 2017.
57. IDC, "Worldwide Wearables Market Ticks Up 5.5% Due to Gains in Emerging Markets, Says IDC," September 4, 2018; Yonhap News Agency, "(LEAD) Samsung Retains No. 1 Market Share in U.S. Home Appliance Market in 2017," January 28, 2018; Xie Yu, "Haier Bought GE Appliances for US$5.6 Billion. Now It's Working on Fixing It," *South China Morning Post*, October 23, 2017; OfO, "About OfO"; MoBike, "World's Largest Smart Bike Sharing Platform, Mobike, Rides into First U.S. City, Washington DC," September 19, 2017.
58. Tate Nurkin et al., "China's Advanced Weapons Systems," *Jane's by IHS Markit* (prepared for the U.S.-China Economic and Security Review Commission), May 10, 2018, 110–124; U.S.-China Economic and Security Review Commission, Chapter 4, Section 1, "China's Pursuit of Dominance in Computing, Robotics, and Biotechnology," in *2017 Annual Report to Congress*, November 2017.
59. Neurala, "Neurala Names Steve Walsh Vice President of Sales," July 19, 2018; Neurala, "Tim Draper and Haiyin Capital Lead $1.2-Million of New Investment in Neurala," June 2, 2016.
60. Modern Materials Handling, "KION Completes Acquisition of Dematic," November 1, 2016; Kion Group, "Q3 2016 Update Call," October 27, 2016.
61. *BusinessWire*, "Shanhai Capital Completes Acquisition of Analogix Semiconductor," April 6, 2017.
62. John Cook, "Chinese Search Giant Baidu Buys Seattle Startup Kitt.ai to Connect Natural Language Tech to Developers," *GeekWire*, July 5, 2017; *Marketwired*, "Baidu Further Strengthens Visual Perception Capabilities with Acquisition of xPerception," *Yahoo Finance*, April 13, 2017.
63. Gary Mortimer, "U.S.—DoD Pulls the Plug on COTS Drones," *sUAS News*, June 7, 2018; Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017; U.S. Department of the Treasury, *Statement on the President's Decision Regarding Lattice Semiconductor Corporation*, September 13, 2017.
64. Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017.
65. Gary Mortimer, "U.S. Army Calls for Units to Discontinue Use of DJI Equipment," *sUAS News*, August 4, 2017.

66. Gary Mortimer, "U.S.—DoD Pulls the Plug on COTS Drones," *sUAS News*, June 7, 2018.
67. U.S. Department of the Treasury, *Statement on the President's Decision Regarding Lattice Semiconductor Corporation*, September 13, 2017; Office of the Press Secretary, *Presidential Order -- Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMBH*, December 2, 2016.
68. Greg Roumeliotis, "U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns," *Reuters*, January 2, 2018.
69. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Anthony J. Ferrante, March 8, 2018, 86.
70. Karen Campbell et al., "The 5G Economy: How 5G Technology Will Contribute to the Global Economy," *IHS Economics and IHS Technology*, January 2017, 4, 16.
71. Karen Campbell et al., "The 5G Economy: How 5G Technology Will Contribute to the Global Economy," *IHS Economics and IHS Technology*, January 2017, 17.
72. Brice Murara, "5G," *International Telecommunication Union*; International Telecommunication Union, "Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s)," November 2017; Kathy Pretz, "5G: The Future of Communications Networks," *The Institute*, March 1, 2017.
73. Brice Murara, "5G," *International Telecommunication Union*; Ellen Warren, "5G Is Totally Changing How We Connect," *Nokia*, March 16, 2018.
74. Capgemini Digital Transformation Institute, "Unlocking the Business Value of IoT in Operations," March 2018, 9; International Telecommunications Union, *Setting the Science for 5G: Opportunities and Challenges*, 2018; Karen Campbell et al., "The 5G Economy: How 5G Technology Will Contribute to the Global Economy," *IHS Economics and IHS Technology*, January 2017, 17; Brice Murara, "5G," *International Telecommunication Union*.
75. Josh Chin, Sarah Krouse, and Dan Stumpf, "The 5G Race: China and the U.S. Battle to Control World's Fastest Wireless Internet," *Wall Street Journal*, September 9, 2018; Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 2, 4–5; Analysys Mason and Recon Analytics, "Race to 5G," *CTIA*, April 2018, 6.
76. U.S.-China Economic and Security Review Commission, *Hearing on China's Shifting Economic Realities and Implications for the United States,* written testimony of Roselyn Hsueh, February 24, 2016; John Kehoe, "How Chinese Hacking Felled Telecommunication Giant Nortel," *Financial Times*, May 26, 2014; Mark Chandler, "Huawei and Cisco's Source Code: Correcting the Record," *Cisco*, October 11, 2012; U.S.-China Economic and Security Review Commission, *The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector*, January 2011; Jamil Anderlini, "Motorola Claims Espionage in Huawei Lawsuit," *Financial Times*, July 21, 2010; Evan S. Medeiros et al., "A New Direction for China's Defense Industry," 2015, RAND Corporation; *Associated Press*, "Cisco Agrees to Settle Huawei Suit," *San Diego Union Tribune*, July 29, 2004.
77. State Council of the People's Republic of China, *State Council's Guidance on Actively Promoting the Internet Plus Action Plan*, July 1, 2015. Translation. *http://www.gov.cn/gongbao/content/2015/content_2897187.htm*; State Council of the People's Republic of China, *Made in China 2025*, May 8, 2015. Translation. *http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm*.
78. People's Republic of China, *Outline of the People's Republic of China's 13th Five-Year Plan on National Economic and Social Development*, March 17, 2016. Translation. *http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm*; Central Compilation and Translation Press, Central Committee of the Communist Party of China, *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China*.
79. China Tower, "Global Offering," *Hong Kong Stock Exchange*.
80. Yang Ge, "China Tower's Maiden Earnings Leave Investors Calling for More," *Caixin*, August 13, 2018.
81. Fiona Lau and Julie Zhu, "China Tower Raises $6.9 Billion in World's Largest IPO in Two Years: Sources," *Reuters*, August 1, 2018; China Tower, "Global Offering," *Hong Kong Stock Exchange*, 18.
82. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 4.
83. Bien Perez, Sarah Dai, and Catherine Wong, "Trump's Rush to Build a National 5G Network May Backfire, Give China the Technological Edge," *South China Morning Post*, January 29, 2018.
84. Majed Al Amine, Kenneth Mathias, and Thomas Dyer, "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," *Accenture Strategy*, 2017, 14.

85. Eric Auchard and Stephen Nellis, "What Is 5G and Who Are the Major Players?" *Reuters*, March 15, 2018.
86. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.
87. U.S.-China Business Council, "Unofficial USCBC Chart of Localization Targets by Sector Set in the MIIT Made in China 2025 Key Technology Roadmap," February 2, 2016; Chinese Academy of Engineering, Expert Commission for the Construction of a Manufacturing Superpower, *Made in China 2025 Key Area Technology Roadmap*, October 29, 2015. Translation, 14. *http://www.cae.cn/cae/html/files/2015-10/29/20151029105822561730637.pdf.*
88. 3GPP, "Release 16," July 16, 2018; Balazs Bertenyi, "Summary after TSG-RAN#80," *3GPP*, July 3, 2018, 5.
89. International Telecommunications Union, "Understanding Patents, Competition, and Standardization in an Interconnected World," July 1, 2014, 3, 19–24*;* International Organization for Standardization, "How We Develop Standards."
90. International Telecommunications Union, "Understanding Patents, Competition, and Standardization in an Interconnected World," July 1, 2014, 51.
91. International Telecommunications Union, "Understanding Patents, Competition, and Standardization in an Interconnected World," July 1, 2014, 52.
92. International Telecommunications Union, "Understanding Patents, Competition, and Standardization in an Interconnected World," July 1, 2014, 73–75.
93. Liu Hui and Carl F. Cargill, "Setting Standards for Industry: Comparing the Emerging Chinese Standardization System and the Current U.S. System," *East-West Center*, 2017, 24; Ping Wang and Zheng Liang, "Beyond Government Control of China's Standardization System: History, Current Status and Reform Suggestions," *East West Center*, January 2016; Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions" (prepared for the U.S.-China Economic and Security Review Commission), January 16, 2013, 11.
94. Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, 6–7; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 177–184.
95. Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, 9, 26; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 177–184.
96. U.S. National Institute of Standards and Technology, briefing to the Commission, March 7, 2018; Liu Hui and Carl F. Cargill, "Setting Standards for Industry: Comparing the Emerging Chinese Standardization System and the Current U.S. System," *East-West Center*, 2017, 4; Dong Geun Choi and Erik Puskar, "A Review of U.S.A. Participation in ISO and IEC," *National Institute of Standards and Technology*, June 2014; Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions" (prepared for the U.S.-China Economic and Security Review Commission), January 16, 2013, 11.
97. Michael O'Rielly, Federal Communications Commissioner, "Next Generation 5G Wireless Networks: Seizing the Opportunities and Overcoming the Obstacles," Free State Foundation, Washington, DC, July 25, 2017.
98. International Telecommunications Union, "Office of the Secretary-General"; International Telecommunications Union, "Focus Group on IMT-2020."
99. International Telecommunications Union, "SG13—Management Team (Study Period 2017–2020)"; International Telecommunications Union, "Focus Groups: ITU-T Focus Groups"; International Telecommunications Union, "Focus Group on Technologies for Network 2030"; International Telecommunications Union, "Focus Group on Machine Learning for Future Networks Including 5G."
100. International Organization for Standardization, "Getting Started Toolkit for ISO Working Group Convenors - 2018 Edition," 2018; International Organization for Standardization, "Getting Started Toolkit for ISO Committee Chairs - 2018 Edition," 2018; International Organization for Standardization, "Getting Started Toolkit for ISO Committee Secretaries - 2018 Edition," 2018.
101. Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, 6, 42.
102. Dong Geun Choi and Erik Puskar, "A Review of U.S.A. Participation in ISO and IEC," *National Institute of Standards and Technology*, June 2014; Internation-

al Organization for Standardization, "ISO: A Global Network of National Standards Bodies."

103. Dong Geun Choi and Erik Puskar, "A Review of U.S.A. Participation in ISO and IEC," *National Institute of Standards and Technology*, June 2014; International Organization for Standardization, "ISO: A Global Network of National Standards Bodies."

104. International Organization for Standardization, "ISO in Figures 2017"; International Organization for Standardization, "ISO in Figures 2012."

105. International Organization for Standardization, "TC Participation—ANSI"; International Organization for Standardization, "TC Participation—SAC."

106. International Organization for Standardization, "Technical Committees"; International Organization for Standardization, "TC Participation—ANSI."

107. International Organization for Standardization, "Technical Committees"; International Organization for Standardization, "TC Participation—SAC."

108. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018; Bien Perez, "China's Chance to Lead Global Innovation May Lie with 5G Mobile Technology Development," *South China Morning Post*, October 1, 2017; LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," May 5, 2016.

109. Stéphane Téral, "Global Mobile Infrastructure Market Down 14 Percent from a Year Ago," *IHS Markit*, March 13, 2018.

110. Stéphane Téral, "Global Mobile Infrastructure Market Down 14 Percent from a Year Ago," *IHS Markit*, March 13, 2018.

111. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

112. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

113. Eric Auchard, "Huawei in Early 5G trials with 30 Telcos; CEO Rejects U.S. Security Fears," *Reuters*, February 26, 2018; Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

114. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

115. IDC, "IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017," March 5, 2018.

116. Stéphane Téral, "Global Mobile Infrastructure Market Down 14 Percent from a Year Ago," *IHS Markit*, March 13, 2018; IDC, "IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017," March 5, 2018; IDC, "Worldwide Enterprise WLAN Market Sees Steady Growth in Full Year and Q4 2017, According to IDC," March 1, 2018; *BusinessWire*, "Strategy Analytics: 2017 Smartphone Apps Processor Market Share: HiSilicon, Qualcomm and Samsung LSI Gain Share."

117. IDC, "IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017," March 5, 2018; IDC, "Worldwide Enterprise WLAN Market Sees Steady Growth in Full Year and Q4 2017, According to IDC," March 1, 2018.

118. IDC, "IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Modest, Continued Growth for Fourth Quarter and Full Year 2017," March 5, 2018.

119. *BusinessWire*, "Strategy Analytics: 2017 Smartphone Apps Processor Market Share: HiSilicon, Qualcomm and Samsung LSI Gain Share."

120. Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, 27; LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," May 5, 2016.

121. Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, 27; LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," May 5, 2016.

122. Dave Burstein, "China: We Lead 3GPP Wireless Standards," *CircleID*, May 26, 2018; Bien Perez, "China's Chance to Lead Global Innovation May Lie with 5G Mobile Technology Development," *South China Morning Post*, October 1, 2017.

123. Josh Chin, Sarah Krouse, and Dan Stumpf, "The 5G Race: China and the U.S. Battle to Control World's Fastest Wireless Internet," *Wall Street Journal*, September 9, 2018; Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 2, 4–5; Analysys Mason and Recon Analytics, "Race to 5G," *CTIA*, April 2018, 6.

124. Stu Woo, "Why Being First in 5G Matters," *Wall Street Journal*, September 12, 2018; Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 4–5; Analysys Mason and Recon Analytics, "Race to 5G," *CTIA*, April 2018; Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT,"

Jefferies Franchise Note, September 14, 2017, 36*;* CTIA, "America Leads World in 4G LTE," March 4, 2016.

125. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 4–5; Analysys Mason and Recon Analytics, "Race to 5G," *CTIA*, April 2018; CTIA, "America Leads World in 4G LTE," March 4, 2016; Craig Wigginton et al., "The Impact of 4G Technology on Commercial Interactions, Economic Growth, and U.S. Competitiveness," *Deloitte*, August 2011.

126. Recon Analytics LLC, "How America's 4G Leadership Propelled the U.S. Economy," *CTIA*, April 2018.

127. AT&T, "AT&T Bringing 5G to More U.S. Cities in 2018," July 20, 2018; Mike Dano, "T-Mobile to Build—But Not Necessarily Sell—5G in 30 Cities This Year," *FierceWireless*, February 27, 2018.

128. Ryan Daws, "China Is Going to Set the Pace for 5G Network Deployments," *Telecoms*, August 2, 2018; Joe Madden, "Industry Voices—Madden: China's 5G Ramp-up Will Start Soon, and It Will Be Huge," *FierceWireless*, June 27, 2018.

129. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 4; Ryan Daws, "China Is Going to Set the Pace For 5G Network Deployments," *Telecoms*, August 2, 2018; Joe Madden, "Industry Voices—Madden: China's 5G Ramp-up Will Start Soon, and It Will Be Huge," *FierceWireless*, June 27, 2018; Analysys Mason and Recon Analytics, "Race to 5G," *CTIA*, April 2018.

130. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 5.

131. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 5.

132. Dan Littmann et al., "5G: The Chance to Lead for a Decade," *Deloitte*, August 7, 2018, 5.

133. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

134. Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," *Reuters*, February 23, 2018.

135. U.S. House Energy and Commerce Committee, *Hearing on Telecommunications, Global Competitiveness, and National Security*, written testimony of Samm Sacks, May 16, 2018, 3.

136. U.S. House Energy and Commerce Committee, *Hearing on Telecommunications, Global Competitiveness, and National Security*, written testimony of Samm Sacks, May 16, 2018, 3.

137. Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *Center for Strategic and International Studies*, August 2018; U.S.-China Economic and Security Review Commission, *Hearing on U.S. Tools to Address Chinese Market Distortions*, written testimony of Graham Webster, June 8, 2018, 6–7; Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018; U.S. House Energy and Commerce Committee, *Hearing on Telecommunications, Global Competitiveness, and National Security*, written testimony of Samm Sacks, May 16, 2018, 3.

138. Stu Woo, Dan Strumpf, and Betsy Morris, "Huawei, Seen as Possible Spy Threat, Boomed despite U.S. Warnings," *Wall Street Journal*, January 8, 2018; Phil Goldstein, "Huawei Exec: We Treat Tier 3 U.S. Carriers Like They're the 'Belle of the Ball,'" *FierceWireless*, March 27, 2015; U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Congress, October 8, 2012; Joann Lublin, "Security Fears Kill Chinese Bid in U.S." *Wall Street Journal*, November 5, 2010.

139. U.S. Federal Communications Commission, *Fact Sheet: Protecting against National Security Threats to the Communications Supply Chain through FCC Programs*, March 27, 2018.

140. U.S. Federal Communications Commission, *FCC Proposes to Protect National Security Through FCC Programs - Statement of Chairman Ajit Pai*, April 18, 2018; U.S. Federal Communications Commission, *Fact Sheet: Protecting against National Security Threats to the Communications Supply Chain through FCC Programs*, March 27, 2018.

141. Scott Mortiz, Mark Gurman, and Todd Shields, "Verizon Drops Plan to Sell Phones from China's Huawei, Sources Say," *Bloomberg*, January 29, 2018; Vlad Savov, "Huawei's CEO Going Off-Script to Rage at US Carriers Was the Best Speech of CES," *The Verge*, January 9, 2018; Stu Woo and Betsy Morris, "AT&T Backs off Deal to Sell Smartphones from China's Huawei," *Wall Street Journal*, January 8, 2018; Roger Cheng, "Nope, AT&T Isn't Selling a Huawei Phone," *CNET*, January 8, 2018.

142. Best Buy, *www.bestbuy.com*; Roger Cheng, "Huawei Dealt a Blow, Loses Best Buy as a Retail Partner," *CNET*, March 22, 2018; Mark Gurman, "Best Buy Severs Ties with Huawei amid Security Concerns," *Bloomberg*, March 21, 2018.

143. Stu Woo and Gordon Lubold, "Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones," *Wall Street Journal*, May 2, 2018.

144. Stu Woo and Gordon Lubold, "Pentagon Orders Stores on Military Bases to Remove Huawei, ZTE Phones," *Wall Street Journal*, May 2, 2018.

145. John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 5515, Pub. L. No. 115–232, 2018; U.S. House of Representatives, *Conference Report to Accompany H.R. 5515—John S. McCain National Defense Authorization Act for Fiscal Year 2019*, 694.

146. John S. McCain National Defense Authorization Act for Fiscal Year 2019 § 5515, Pub. L. No. 115–232, 2018.

147. U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012, 1.

148. U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, 17; U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012.

149. Thilo Hanemann and Daniel H. Rosen, "Chinese Investment in the United States: Recent Trends and the Policy Agenda," *Rhodium Group* (prepared for the U.S.-China Economic and Security Review Commission), December 2016, 7, 66–77.

150. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018; U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012.

151. Australia's Ministers for Communications and Arts, *Government Provides 5G Security Guidance to Australian Carriers*, August 23, 2018; Colin Packham, "Australia Prepares to Ban Huawei from 5G Project over Security Fears," *Reuters*, July 11, 2018; Huawei Cyber Security Evaluation Center Oversight Board, "Annual Report 2018," July 2018; European Union Agency for Network and Information Security, "Signaling Security in Telecom SS7/Diameter/5G," March 2018, 7–8; U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017; Positive Technologies, "Primary Security Threats for SS7 Cellular Networks," 2016; U.S. Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the NIPP 2013*, 2015; United Kingdom Intelligence and Security Committee, *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*, June 2013; U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012.

152. Elsa Kania, "Much Ado About Huawei," *Australian Strategic Policy Institute*, March 27, 2018; United Kingdom Intelligence and Security Committee, *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*, June 2013; U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012.

153. Nathaniel Ahrens, "China's Competitiveness: Myths, Reality, and Lessons for the United States and Japan—Case Study: Huawei," *Center for Strategic and International Studies*, February 2013, 8; Peilei Fan, "Catching up through Developing Innovation Capability: Evidence from China's Telecom-Equipment Industry," *Technovation*, 26 (2006): 364.

154. U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012, vi.

155. Australia's Ministers for Communications and Arts, *Government Provides 5G Security Guidance to Australian Carriers*, August 23, 2018; Tom Westbrook and Byron Kaye, "China's Huawei Slams Australia 5G Mobile Network Ban as 'Politically Motivated,'" *Reuters*, August 22, 2018; Colin Packham, "Australia Prepares to Ban Huawei from 5G Project over Security Fears," *Reuters*, July 11, 2018.

156. Christopher Balding, "ZTE's Ties to China's Military-Industrial Complex Run Deep," *Foreign Policy*, July 19, 2018; U.S. National Telecommunications and Information Administration, *Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s for an International Section 214 Authorization*, File No. ITC2142011090100289, July 2, 2018, 8; U.S.

House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, October 8, 2012; Mark A. Stokes and Dean Cheng, "China's Evolving Space Capabilities: Implications for U.S. Interests," *Project 2049* (prepared for the U.S.-China Economic and Security Review Commission), April 2012.

157. *BBC*, "China's ZTE 'Poses Risk to UK Security,'" April 16, 2018.

158. U.S. National Telecommunications and Information Administration, *Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s for an International Section 214 Authorization*, File No. ITC2142011090100289, July 2, 2018, 1.

159. U.S. National Telecommunications and Information Administration, *Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s for an International Section 214 Authorization*, File No. ITC2142011090100289, July 2, 2018, 3.

160. U.S. National Telecommunications and Information Administration, *Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s for an International Section 214 Authorization,* File No. ITC2142011090100289, July 2, 2018, 8.

161. U.S. National Telecommunications and Information Administration, *Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s for an International Section 214 Authorization*, File No. ITC2142011090100289, July 2, 2018, 1.

162. U.S. Federal Communications Commission, *Opposition to Petition to Deny*, File No. ITC-214-20110901-00289, August 20, 2018.

163. U.S. Federal Communications Commission, *Reply of the National Telecommunications and Information Administration*, File No. ITC2142011090100289, September 19, 2018, 3.

164. U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities; and Modification of Entry on the Entity List," *Federal Register* 83:148, August 1, 2018.

165. U.S. Department of Commerce, Bureau of Industry and Security, "Addition of Certain Entities; and Modification of Entry on the Entity List," *Federal Register* 83:148, August 1, 2018.

166. Imanol Arbulu et al., "Industry 4.0: Reinvigorating ASEAN Manufacturing for the Future," *McKinsey & Company*, February 2018; U.S. Chamber of Commerce, *ASEAN Business Outlook Survey*, September 6, 2017.

167. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Anthony J. Ferrante, March 8, 2018, 2–3.

168. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Anthony J. Ferrante, March 8, 2018, 2–3; James Manyika et al., "The Internet of Things: Mapping the Value beyond the Hype," *McKinsey Global Institute*, June 2015; Mark Purdy and Ladan Davarzani, "The Growth Game-Changer: How Industrial Internet of Things Can Drive Progress and Prosperity," *Accenture and Frontier Economics*, 2015.

169. Office of the U.S. Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, March 22, 2018; Office of the U.S. Trade Representative, *2017 Report to Congress on China's WTO Compliance*, January 2018; Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016.

170. U.S.-China Economic and Security Review Commission, Chapter 4, Section 1, "China's Pursuit of Dominance in Computing, Robotics, and Biotechnology," in *2017 Annual Report to Congress*, November 2017.

171. Office of the U.S. Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, March 22, 2018; Jost Wübbeke et al., "Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries," *Mercator Institute for China Studies*, December 2016; Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016; Chinese Academy of En-

gineering, Expert Commission for the Construction of a Manufacturing Superpower, *Made in China 2025 Key Area Technology Roadmap*, October 29, 2015. Translation. *http://www.cae.cn/cae/html/files/2015-10/29/20151029105822561730637.pdf*.

172. U.S. House of Representatives Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, and Oversight and Management Efficiency, *Hearing on Access Denied: Keeping Adversaries Away from the Homeland Security Supply Chain*, written testimony of Gregory C. Wilshusen, July 12, 2018; Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 19.

173. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 19; Katherine Koleski, "The 13th Five-Year Plan," *U.S.-China Economic and Security Review Commission*, February 14, 2017.

174. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018; U.S. Government Accountability Office, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, July 27, 2017, 3.

175. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 3.

176. Gregory Falco, "Job One for Space Force: Space Asset Cybersecurity," *Harvard Kennedy School, Belfer Center for Science and International Affairs*, July 2018.

177. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Jennifer Bisceglie, March 8, 2018, 74.

178. UAS Vision, "Pentagon Bans Marines from Using COTS Quadcopters," June 21, 2018; U.S. Department of Defense, Inspector General, *Reannouncement of the Audit of the DoD's Implementation of Cybersecurity Controls for Unmanned Aerial Vehicle Systems as the Audit of DoD's Management of Cybersecurity Risks for Purchasing Commercial Items*, D2018-D000CR-0113.000, June 18, 2018; Gary Mortimer, "US—DOD Pulls the Plug on COTS Drones," *sUAS News*, June 7, 2018.

179. U.S. Department of Defense, Inspector General, *Reannouncement of the Audit of the DoD's Implementation of Cybersecurity Controls for Unmanned Aerial Vehicle Systems as the Audit of DoD's Management of Cybersecurity Risks for Purchasing Commercial Items*, D2018-D000CR-0113.000, June 18, 2018.

180. Denise E. Zhang and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military," *Center for Strategic and International Studies*, September 2015, 13–16.

181. Tate Nurkin et al., "China's Advanced Weapons Systems," *Jane's by IHS Markit* (prepared for the U.S.-China Economic and Security Review Commission), May 10, 2018, 150–176.

182. U.S. Department of Commerce and U.S. Department of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats*, May 22, 2018; U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Chuck Benson, March 8, 2018, 1–2, 9–10; U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Anthony J. Ferrante, March 8, 2018, 3–7.

183. U.S. Department of Commerce and U.S. Department of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats*, May 22, 2018, 3.

184. Ponemon Institute LLC, "2017 Study on Mobile and IoT Application Security," *IBM and Arxan*, January 2017.

185. U.S. Department of Commerce and U.S. Department of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats*, May 22, 2018; Andrew Tannenbaum, "Why Do IoT Companies Keep Building Devices with Huge Security Flaws?" *Harvard Business Review*, April 27, 2017.

186. U.S. Senate Select Committee on Intelligence, *Hearing on the Worldwide Threat Assessment of the US Intelligence Community*, written testimony of Daniel R. Coats, May 11, 2017, 2, 4.

187. U.S. Department of Justice, Federal Bureau of Investigation, *Cyber Actors Use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious*

Cyber Activities, August 2, 2018; U.S. Department of Justice, Federal Bureau of Investigation, *Common Internet of Things Devises May Expose Consumers to Cyber Exploitation*, October 17, 2017; Common Vulnerabilities and Exposures, "CVE List"; U.S. Government Accountability Office, *Internet of Things: Status and Implications of an Increasingly Connected World*, May 2017, 16–17.

188. Symantec, *Internet Security Threat Report: Volume 23*, March 2018, 80.

189. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Chuck Benson, March 8, 2018, 60.

190. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Chuck Benson, March 8, 2018, 62.

191. Executive Office of the President, Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018, 5.

192. Executive Office of the President, Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018, 6.

193. Executive Office of the President, Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan*, May 2018, 15, 18; U.S. National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, 203.

194. U.S. Department of Commerce and U.S. Department of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats*, May 22, 2018, 3; U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Chuck Benson, March 8, 2018, 55; U.S. Defense Science Board, *Cyber Supply Chain*, April 2017, 6–11.

195. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, v.

196. Radware, "A Quick History of IoT Botnets," March 1, 2018; Dan Goodin, "New IoT Botnet Offers DDoSes of Once-Unimaginable Sizes for $20," *Ars Technica*, February 1, 2018; Allison Nixon, John Costello, and Zach Wikholm, "An After-Action Analysis of the Mirai Botnet Attacks on Dyn," *Flashpoint*, October 25, 2016.

197. Radware, "A Quick History of IoT Botnets," March 1, 2018; U.S. Government Accountability Office, *Internet of Things: Status and Implications of an Increasingly Connected World*, May 2017, 29; Michael Kan, "Chinese Firm Admits its Hacked Products Were behind Friday's DDOS Attack," *Computer World*, October 23, 2016; Lorenzo Franceschi-Bicchierai, "How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet," *Motherboard*, September 29, 2016.

198. Ashley Carman, "Hacked Webcams that Helped Shut Down the Internet Last Week are Being Recalled," *The Verge*, October 24, 2016; Jon Gold, "DNS Provider Dyn Hit by DDoS Attack that Takes out Major Sites," *Computer World*, October 21, 2016.

199. Ashley Carman, "Hacked Webcams that Helped Shut Down the Internet Last Week are Being Recalled," *The Verge*, October 24, 2016; Jon Gold, "DNS Provider Dyn Hit by DDoS Attack that Takes out Major Sites," *Computer World*, October 21, 2016.

200. Sara Boddy and Justin Shattuck, "Cyber Attacks Spike in Finland before Trump-Putin Meeting," *F5*, July 19, 2018.

201. Giulio Coraggio, "Global: Large Number of Internet of Things Devices Are Not Privacy Compliant," *DLA Piper*, October 4, 2016; International Commissioner's Office, "Privacy Regulators Study Finds Internet of Things Shortfalls," September 22, 2016.

202. Beatric Perez, Micro Musolesi, and Gianluca Stringhini, "You Are Your Metadata: Identification and Obfuscation of Social Media Users Using Metadata Information," *Association for the Advancement of Artificial Intelligence,* May 14, 2018; U.S.-China Economic and Security Review Commission, *Hearing on China's Pursuit of Next Frontier Tech: Computing, Robotics, and Biotechnology*, written testimony of Edward H. You, March 16, 2017, 2–3; Peter Pitts, "The Privacy Delusions of Genetic Testing," *Forbes*, February 15, 2017 Erika Check Hayden, "Privacy Protections: The Genome Hacker," *Nature*, May 8, 2013.

203. Supreme Court of the United States, "United States v. Jones," October Term 2011, 3.

204. Jeremy Hsu, "The Strava Heat Map and the End of Secrets," *Wired*, January 29, 2018.

205. U.S. Department of Defense, *Use of Geolocation-Capable Devices, Applications, and Services*, August 3, 2018.

206. U.S. Department of Defense, *Use of Geolocation-Capable Devices, Applications, and Services*, August 3, 2018.

207. U.S. Government Accountability Office, "Personal Information, Private Companies," *Watch Blog*, May 1, 2018; U.S. Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, September 2013.

208. U.S. Government Accountability Office, "Personal Information, Private Companies," *Watch Blog*, May 1, 2018; U.S. Government Accountability Office, "Smartphone Data: Information and Issues Regarding Surreptitious Tracking Apps that Can Facilitate Stalking," May 9, 2016; U.S. Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, September 2013.

209. U.S. Federal Trade Commission, *Federal Trade Commission Act*; U.S. Federal Trade Commission, *Gramm-Leach Bliley Act*; U.S. Federal Trade Commission, *Fair Credit Reporting Act—Revised May 2016*; U.S. Federal Trade Commission, *A Summary of Your Rights under the Fair Credit Reporting Act*; U.S. Department of Health and Human Services, Office of Civil Rights, interview with Commission staff, September 12, 2017; U.S. Department of Health and Human Services, Office of Civil Rights, *Covered Entities and Business Associates*, June 16, 2017; U.S. Federal Trade Commission, *Children's Online Privacy Protection Rule ("COPPA")*.

210. Laura Bliss, "Are Dockless Bikes a Cybersecurity Threat?" *City Lab*, February 15, 2018.

211. Michael LaForgia and Gabriel J.X. Dance, "Facebook Gave Data Access to Chinese Firm Flagged by Intelligence," *New York Times*, June 5, 2018; Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York Times*, June 3, 2018.

212. David Shepardson, "Facebook Confirms Data Sharing with Chinese Companies," *Reuters*, June 5, 2018; Gabriel J.X. Dance, Nicholas Confessore, and Michael LaForgia, "Facebook Gave Device Makers Deep Access to Data on Users and Friends," *New York Times*, June 3, 2018.

213. U.S. Department of Commerce and U.S. Department of Homeland Security, *Enhancing the Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated, Distributed Threats*, May 22, 2018, 3.

214. Ms. Smith, "Critical Hikvision Flaw Could Be Remotely Exploited to Hijack Cameras, DVRs, and Accounts," *CSO*, April 25, 2018; Joel Griffin, "Dahua Patches Cyber Vulnerability in Its Cameras," *Security InfoWatch*, November 16, 2017.

215. Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018, 7–8.

216. Lance Noble, "Marshalls over Markets: China Tightens Cybersecurity," *Gavekal Dragonomics*, June 4, 2018, 7–8; Human Rights Watch, "China: Big Data Fuels Crackdown in Minority Region," February 26, 2018.

217. Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017.

218. Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017.

219. Paul Mozur, "Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say," *New York Times*, November 29, 2017.

220. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Anthony Ferrante, March 8, 2018, 87; Karen Campbell et al., "The 5G Economy: How 5G Technology Will Contribute to the Global Economy," *IHS Economics and IHS Technology*, January 2017; LexInnova, "5G Mobile Network Technology: Patent Landscape Analysis," May 5, 2016.

221. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, written testimony of Doug Brake, March 8, 2018, 7.

222. Recon Analystics LLC, "How America's 4G Leadership Propelled the U.S. Economy," *CTIA*, April 2018; Craig Wigginton et al., "The Impact of 4G Technology on Commercial Interactions, Economic Growth, and U.S. Competitiveness," *Deloitte*, August 2011.

223. Tai Ming Cheung et al., "Planning for Innovation: Understanding China's Plans for Technological, Energy, Industrial, and Defense Development," *University of California Institute on Global Conflict and Cooperation* (prepared for the U.S.-China Economic and Security Review Commission), July 28, 2016, 181–182.

224. Raymond Zhong, "China's Huawei Is at Center of Fight over 5G's Future," *New York Times*, March 7, 2018.

225. T-Mobile, "T-Mobile and Nokia Ink $3.5 Billion, Multi-Year 5G Network Agreement," July 30, 2018; Mike Dano, "Samsung Showing Gains in U.S. Network Equipment Market," *FierceWireless*, March 6, 2018; Mike Dano, "T-Mobile to Build—But

Not Necessarily Sell—5G in 30 Cities This Year," *FierceWireless*, February 27, 2018; AT&T, "AT&T Expanding Fixed Wireless 5G Trials to Additional Markets," August 30, 2017; Ericsson, *Form 20-F*; Nokia, "Nokia Annual Report on Form 20-F 2017"; Samsung, "Consolidated Financial Statements of Samsung Electronics Co., Ltd. and Its Subsidiaries Index to Financial Statement," 2017.

226. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 2–4.

227. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018, 4–5; Richard McGregor, "Xi Jinping's Ideological Ambitions," *Wall Street Journal*, March 1, 2018.

228. Tara Beeny et al., "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology," *Interos* (prepared for the U.S.-China Economic and Security Review Commission), April 19, 2018; U.S. Government Accountability Office, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations*, July 27, 2017, 3.

229. U.S. Senate Select Committee on Intelligence, *Hearing on Worldwide Threats*, February 13, 2018; Sara Salinas, "Six Top US Intelligence Chiefs Caution against Buying Huawei Phones," *CNBC*, February 13, 2018.

230. John S. McCain National Defense Authorization Act for Fiscal Year 2019 §5515, Pub. L. No. 115–232, 2018; U.S. Senate Armed Services Commission, *Hearing on the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program*, written testimony of Admiral Kurt W. Tidd, February 15, 2018, 5–6; Randy Woods and Andrew Mayeda, "Trump Steps up Efforts to Check China Influence in Latin America," *Bloomberg*, January 4, 2018; R. Evan Ellis, "The Strategic Dimension of Chinese Activities in the Latin American Telecommunications Sector," *General José María Córdova*, Bogotá, D.C. (Colombia), 11:11, January-June 2013: 121–140.

231. European Union Agency for Network and Information Security, "Signaling Security in Telecom SS7/Diameter/5G," March 2018, 7–8; U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017; Positive Technologies, "Primary Security Threats for SS7 Cellular Networks," 2016.

232. U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, 112th Congress, October 8, 2012, 29.

233. U.S. Department of Homeland Security and the National Institute of Standards and Technology, *Study on Mobile Device Security*, April 2017, ii.

234. U.S. Federal Communications Commission, *Chairman Pai Statement on Proposal to Help Protect Security of U.S. Communications Networks and Their Supply Chains*, March 26, 2018.

235. European Union Agency for Network and Information Security, "Signaling Security in Telecom SS7/Diameter/5G," March 2018, 7–8; U.S. Department of Homeland Security and the U.S. National Institute of Standards and Technology, *Study on Mobile Device Security*, April 2017, ii, 75–76; Positive Technologies, "Primary Security Threats for SS7 Cellular Networks," 2016.

236. U.S. Department of Homeland Security and the U.S. National Institute of Standards and Technology, *Study on Mobile Device Security*, April 2017, ii, 75–76.

237. European Union Agency for Network and Information Security, "Signaling Security in Telecom SS7/Diameter/5G," March 2018, 21.

238. U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, oral testimony of Anthony Ferrante, March 8, 2018, 87; European Union Agency for Network and Information Security, "Signaling Security in Telecom SS7/Diameter/5G," March 2018, 21.

239. U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, 17.

240. U.S. Department of Defense, Defense Science Board, *Task Force on Cyber Deterrence*, February 2017, 9.