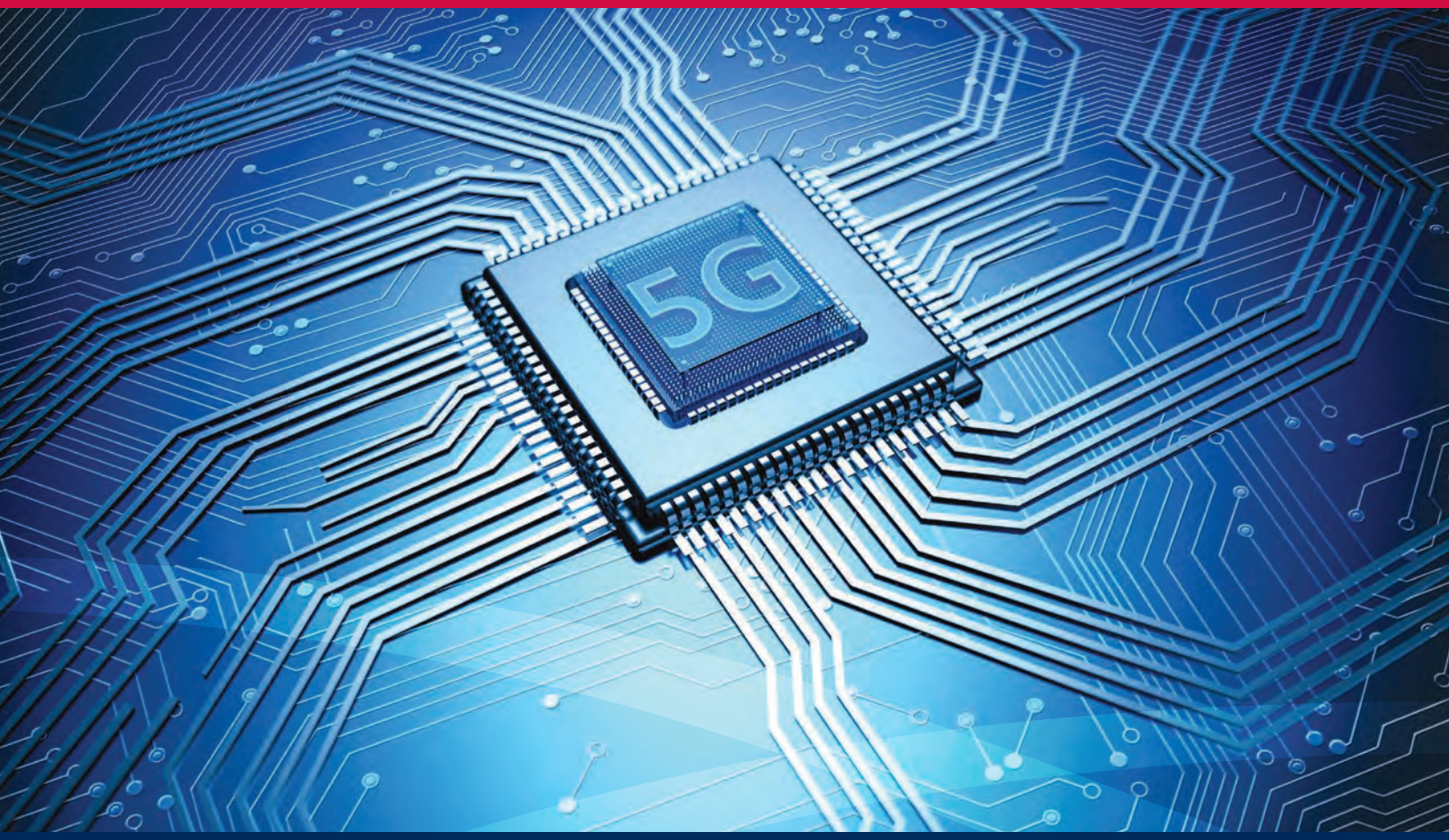


THE NATIONAL SECURITY CHALLENGES OF FIFTH GENERATION (5G) WIRELESS COMMUNICATIONS

Winning the Race to 5G, Securely

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
Cyber Council

June 2019

INSA

ACKNOWLEDGEMENTS

This paper was developed and written by a 5G Working Group operating under the auspices of INSA's Cyber Council. INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to develop this report.

INSA MEMBERS

Kevin Zerrusen, *Goldman Sachs; Cyber Council Chair*

Jim Keffer, *Lockheed Martin; Cyber Council Vice Chair*

George Duchak, *Office of the Secretary of Defense*

Jared Feinberg, *Deloitte*

John Nagengast, *AT&T*

Steve Orrin, *Intel*

Terry Roberts, *WhiteHawk*

Dean Scarlett, *Citi*

Samuel Visner, *MITRE*

INSA STAFF

Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director, Communications and Policy*

Ehrl Alba, *Digital Marketing Manager*

Colin Blowers, *Intern*

EXECUTIVE SUMMARY

The expanded capacity of Fifth Generation (5G) wireless communications will support innovative data-intensive applications, many operating under the rubric of the Internet of Things (IoT), ranging from Smart Cities and autonomous vehicles to advanced medical imaging and the widespread use of virtual reality. Once implemented widely, Americans will come to accept the increased productivity, profitability, and quality of life that 5G enables as the new norm. Whichever country comes to dominate 5G infrastructure – through hardware, software, and technical standards – is likely to have enormous economic and commercial advantages across the global economy.

Manufacturing of wireless telecommunications equipment has gradually shifted overseas due to foreign acquisitions, lower overseas labor costs, and a decline in profitability. The void has been filled by non-U.S. companies – particularly those in China – which have rapidly expanded into manufacturing of semiconductors and 5G technologies. The Executive Order signed by the President on May 15, 2019, Securing the Information and Communications Technology (ICT) and Services Supply Chain, defined a process for assessing risks posed by foreign technology and vendors in the U.S. supply chain, and also expanded authorities for the Administration to mitigate these risks. The following day, the Commerce Department's Bureau of Industry and Security (BIS) added Huawei and 68 of its global affiliates to the "Entity List," stating that "there is reasonable cause to believe that Huawei Technologies Co., Ltd. (Huawei) has been involved in activities determined to be contrary to the national security or foreign policy interests of the United States." The BIS designation prohibits the import of Huawei telecommunications equipment (as well as the export of U.S. technologies to Huawei) in the absence of a specific license. While this effective ban on Chinese telecommunications equipment will help secure U.S. 5G networks, the possibility of waivers, specific licenses, or a future relaxing of the restrictions makes it important that government and industry develop a strategy for the development of a secure 5G network without Chinese equipment.

The dominance of Chinese companies in the wireless technology sector raises significant national security risks, as Chinese-origin 5G equipment could be used to intercept or sabotage information transmitted through it. Risks include the potential theft of U.S. intellectual property and national security information, sabotage of civilian critical infrastructure, and the inability of U.S. military forces and government agencies to communicate and operate securely. In a larger context, Chinese dominance of the equipment that will be used in the 21st century's information backbone challenges the United States' traditional position as the global leader in technology innovation – a dynamic that could undermine U.S. companies' competitiveness and reverberate throughout the U.S. economy.

This paper assesses the state of 5G in the United States and around the world. It discusses the immediate national security challenges inherent in the deployment of 5G wireless technology in the United States, as well as the longer term implications of the push by China to become the world leader in Information and Communications Technology (ICT). Finally, it provides recommendations to government policy makers and private sector technology leaders to address these challenges and reduce the national security risk to U.S. wireless infrastructure, while maintaining long-term technology leadership and competitiveness.

KEY FINDINGS AND RECOMMENDATIONS

Mitigating National Security Risks

- Using Chinese equipment in 5G infrastructure entails significant risks. According to U.S. government authorities, equipment made by Chinese companies, such as Huawei and ZTE, could give China the ability to vacuum up all of the information that passes through it – including sensitive diplomatic, military, and commercial information – and to remotely disrupt U.S. wireless infrastructure in times of conflict. As Americans become increasingly dependent on 5G-capable services, a disruption of 5G networks could cause significant harm to U.S. national security, the U.S. economy, and the health and safety of American citizens.

- Although the leading national carriers in the United States have announced that they will not employ equipment from Chinese companies to provide their 5G capabilities, many smaller regional carriers would prefer to use lower-cost Chinese gear to remain competitive.

- Given the enormous capital costs, 5G equipment, once installed, will be in place for a long time. If Chinese technology companies dominate the global market for 5G equipment, the Chinese government may acquire a "back door" into critical U.S. and allied communications that lasts for decades or more.

  - **RECOMMENDATION #1:** While the Administration, Congress, and private sector groups are looking at such long-term issues as global supply chain security and limits on foreign access to U.S. intellectual property, the imminent deployment of 5G technology in the United States means that government and industry must immediately collaborate on steps to mitigate national security risks.

  - **RECOMMENDATION #2:** The Administration and/or Congress should direct the Intelligence Community to evaluate foreign strategies for influencing U.S. 5G wireless infrastructure and the IoT applications it will support, including the acquisition of U.S. companies and technologies. Building on such analysis, the Committee on Foreign Investment in the United States (CFIUS) should carefully scrutinize proposed acquisitions that could give foreign countries sensitive footholds in 5G technologies, components, networks and IoT applications.

Maintaining Global Mission Capabilities

- Operations by U.S. forces and government agencies will be rendered less secure in countries with Chinese-origin 5G equipment in their telecommunications systems. Some U.S. allies have banned Huawei and ZTE from providing wireless infrastructure due to national security concerns, while others have resisted a ban, as large portions of their infrastructure already use Huawei equipment and as Chinese equipment offers cost savings as they upgrade to 5G.

  - **RECOMMENDATION# 3a:** To eliminate the threat where possible, the United States should continue urging its allies and partners to ban Chinese firms from their 5G networks.

  - **RECOMMENDATION #3b:** To mitigate the threat where necessary, the United States should develop technical solutions that enable U.S. and allied military forces and intelligence agencies to operate securely on telecommunications networks that could be compromised. Solutions may include the use of improved encryption or segregation of communications over multiple networks.

Regaining U.S. Leadership in Wireless Technology

- The United States has no comprehensive strategy or policy to regain global leadership in wireless technology, nor does it have a strategy to deal with the consequences of the expanding Chinese dominance in the Information and Communications Technology (ICT) and 5G markets. Wireless technology manufacturing has largely moved offshore due to lower labor and manufacturing costs, foreign governments' subsidies to vendors, and U.S. companies' decisions not to compete in a low-profit marketplace in which products have largely been commoditized. Some of the few U.S. companies that remain in the market rely largely on offshore fabrication and packaging.

- Given the right incentives, American industry can and will expand investment in wireless technology, including network architecture and virtualization, open source software development, and international standards. Greater involvement of U.S. technology companies in 5G wireless and IoT applications will engender innovation in the technology itself, which will in turn promote security and resilience in the U.S. telecommunications backbone and the other critical infrastructure sectors it supports.

  – RECOMMENDATION #4: The White House should form a public/private Working Group on defining U.S. Trade Policy and Strategy with respect to wireless technology and innovation, including 5G and IoT applications deployment in the United States, with representation from DOD, the IC, the FCC, USTR, the leading wireless carriers, the larger U.S. technology industry, the venture capital community, and academia. Such a forum would assure that key policymakers and private sector technology leaders have a common understanding of the national security risks and challenges associated with the deployment of 5G wireless infrastructure in the United States, as well as the ways in which ongoing trade negotiations affect wireless technology and infrastructure. The Working Group's priorities should be to:

    a. Develop a long-term strategy to enhance U.S. technology leadership in the global wireless marketplace.

    b. Establish a public-private mechanism to continuously "red team" 5G infrastructure and the IoT applications it supports.

    c. Develop common strategies to reduce the overall security risk to the U.S. 5G infrastructure, such as wider use of open source software, zero-trust networking concepts, virtualization and containerization of key security functions and applications, and the employment of artificial intelligence techniques for advanced threat detection.

  – RECOMMENDATION #5: The Administration should continue to assess and implement regulatory and policy changes that would remove barriers to rapid deployment of 5G and make more radio spectrum available for 5G.

  – RECOMMENDATION #6: With significant input from technology leaders in the U.S. telecommunications sector, Congress should develop legislation to expand U.S. private sector investment in ICT and wireless innovation.

INTRODUCTION

Fifth Generation (5G) wireless communications promises a dramatic increase in capabilities over earlier generations, particularly in its ability to support Internet of Things (IoT) applications requiring almost instantaneous data flows at very high data bandwidths. The resulting infrastructure will revolutionize American society by making possible smart cities, autonomous vehicles, wider access to healthcare, and a range of capabilities that will make public services and businesses more effective and efficient.

Whichever country comes to dominate 5G infrastructure – through hardware, software, and technical standards – is likely to have enormous economic and commercial advantages across the global economy. Such advantages are likely to reshape global geopolitics. As the Eurasia Group noted in a November 2018 report, "The decisions governments and industry players will make about how and when to build their 5G networks will have significant consequences, both for how the next phase of the digital revolution unfolds in the US, China, and beyond, and, potentially, for the long-term balance of global power."[1]

New capabilities – particularly ones shaped by U.S. adversaries – come with new challenges. Over time, much of the United States' critical infrastructure will become highly reliant on the security and reliability of our wireless infrastructure. The rapid pace in the advancement of technology is perhaps only matched or exceeded by the advance of ever more sophisticated cyber threats to that technology. Further, the United States' longstanding leadership role in the technology sector has been threatened by the globalization of the wireless industry, with international players now dominating the supply of wireless equipment and other aspects of the technology. This has raised broad concerns about the risks of adopting these new technologies, particularly from a national-security perspective, and how to manage these risks.

This paper describes the national security challenges inherent in the deployment of 5G wireless technology in the United States. It also provides recommendations to government policy makers and private sector technology leaders to deal with these challenges and reduce the national security risk to our wireless infrastructure.

[1] *Eurasia Group, The Geopolitics of 5G, November 15, 2018, p. 3. At https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf. All URLs cited are valid as of April 24, 2019.*

The Administration, Congress, and various private sector groups are looking at such long-term issues as global supply chain security and the risks of foreign investment in critical companies and economic sectors. However, the imminent deployment of 5G technology in the U.S. requires policymakers to take immediate steps to mitigate the national security risks to the Information and Communications Technology (ICT) critical infrastructure sector. U.S. policy makers and industrial leaders must develop a long-term strategy that minimizes the national security risk to the U.S. wireless infrastructure while assuring continued U.S. technology leadership in the global wireless environment. Development of this strategy should include input from the major wireless carriers and other relevant technology innovators and providers (such as chip makers, device manufacturers, cloud service providers, application developers, and venture capitalists).

Early deployment of 5G wireless communications in the United States began in the latter half of 2018, with many other countries launching 5G around the same time or shortly thereafter.[2] A November 2018 report by Ericsson projected that by the end of 2024, an estimated 40% of global mobile subscribers will be 5G, with about 1.5 billion subscriptions. North America will be leading in deployment, with 55% of all mobile broadband subscriptions in North America on 5G.

The move to 5G is more of a tectonic shift than an evolution of current technology. 5G promises numerous improvements over the currently deployed 3G and 4G cellular/wireless services, with significantly higher bandwidths and lower latency (delay). These capabilities will support expanded applications ranging from HD video streaming to telemedicine to self-driving cars and smart cities under the "Internet of Things" rubric. Data bandwidths of up to 20Gbit/sec are possible, using millimeter wave frequency bands (at 28 GHz and up to 60GHz) and MIMO (Multiple Input Multiple Output) beam-forming antennae techniques in the middle bands (3.5-4.2G HZ), and reliable propagation in the 600 MHz band. Many carriers are planning deployment of 5G technology for both fixed and mobile applications, essentially replacing local fiber and Wi-Fi. Given the recapitalization of both wireless and wired infrastructure, many see 5G as the new Internet.

Because Chinese 5G equipment is extremely competitive in the marketplace, there is great concern that deployment of globally-sourced 5G technology in the United States will impose national security risks. Specifically, Chinese-origin equipment in 5G networks could provide China with access to U.S. and allied national security information and valuable intellectual property. Such equipment could also enable an adversary to remotely disrupt the U.S. wireless infrastructure in times of conflict, with severe consequences to critical infrastructure such as the power grid, transportation systems, and healthcare systems.

[2] *Tim Fisher, "5G Availability Around the World," Lifewire.com, April 17, 2019. At https://www.lifewire.com/5g-availability-world-4156244.*

THE NATIONAL SECURITY ISSUES WITHIN 5G WIRELESS COMMUNICATIONS

The hardware and software needed for 5G networks is made by a small number of companies in the United States, Europe, and, increasingly, China. The "race" to dominate 5G is frequently portrayed as one component of U.S.-Chinese economic competition, which also encompasses tariffs, trade, intellectual property theft, and allegations that some Chinese companies – including telecommunications giants Huawei and ZTE – give the Chinese government improper access to information and equipment. Critics argue such access could give China the ability to vacuum up all of the information that passes through 5G equipment – including sensitive diplomatic, military, and commercial information[3] – and to remotely disrupt the U.S. wireless infrastructure in times of conflict. (It should be noted that other countries' activities in cyberspace potentially threaten the United States – most notably those of Russia, Iran, and North Korea – but technology companies from these nations manufacture little or no advanced telecommunications equipment used in 5G networks.)

The recapitalization of both wireless and wired infrastructure will require hundreds of billions of dollars in investment around the world.[4] Given the enormous capital costs, 5G equipment, once installed, will be in place for a long time. There is great concern that, were Chinese technology companies to enter the market for 5G equipment, the Chinese government could acquire a "back door" into critical U.S. and allied communications that lasts for decades or more.

U.S. officials have therefore asserted that Chinese 5G equipment must be excluded from U.S. and allied ICT networks to ensure their security and resiliency and thus protect U.S. national and economic security. In the 2018 National Defense Authorization Act, Congress barred the sale of Huawei and ZTE equipment to government agencies and contractors.[5] The Executive

[4] Some U.S. experts believe that Chinese law would require Chinese telecommunications firms, upon request, to provide the government data to which they have access. See Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have A Choice," MSNBC.com, March 4, 2019. At : https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html. See also written testimony of James Mulvenon, "China, the United States, and Next Generation Connectivity," hearing of the U.S.-China Economic and Security Review Commission, March 8, 2018, p. 4. At https://www.uscc.gov/sites/default/files/James%20Mulvenon_Written%20Testimony.pdf.

[5] Accenture Strategies, Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities, 2017, p. 3. At https://api.ctia.org/docs/default-source/default-document-library/how-5g-can-help-municipalities-become-vibrant-smart-cities-accenture.pdf. See also Bien Perez, "Why China is Set to Spend US$411 Billion on 5G Mobile Networks," South China Morning Post, June 19, 2017. At http://www.scmp.com/tech/china-tech/article/2098948/china-plans-28-trillion-yuan-capital-expenditure-create-worlds.

Order signed by the President on May 15, 2019, Securing the Information and Communications Technology (ICT) and Services Supply Chain, defined a process for assessing risks posed by foreign technology and vendors in the US supply chain, and also expanded authorities for the Administration to mitigate these risks. Specifically the E.O. authorized the Secretary of Commerce, acting in concert with other senior administration officials, to prohibit or modify transactions involving ICT products and services posing undue risks to U.S. national security.

The next day, the Department of Commerce published a notice that the Bureau of Industry and Security (BIS) had announced that Huawei Technologies Company Ltd. and its affiliates were being added to the Entity List, which requires that any sale or transfer of American technology to Huawei and its affiliates would require a BIS license.[6] Because a license may be denied if the sale or transfer would harm U.S. national security or foreign policy interests, the E.O. will effectively ban Chinese technology companies from the 5G market in the United States.[7] However, the E.O. alone does not secure U.S. 5G networks from foreign influence, as BIS could grant licenses to technology incorporating Chinese components or the E.O. could be changed by the current or a future administration in response to political or commercial pressures.

While the Administration, Congress, and private sector groups are assessing such long-term issues as global supply chain security and new limits on foreign access to U.S. intellectual property, the imminent deployment of 5G technology in the United States means that government and industry must immediately collaborate on steps to mitigate the national security risks.

National security concerns to the United States and its allies fall into three broad categories:

- **Wireless Infrastructure Security.** Given the large and expanding presence of Chinese companies in the global ICT marketplace and the well-documented concerns that these companies enable Chinese intelligence activities, 5G wireless infrastructure in the United States and allied countries must be made secure against deliberate disruption, the theft of sensitive personal information, trade secrets and/or intellectual property, and the physical tracking of individuals of interest.

- **Maintaining Technology Leadership.** To promote U.S. global economic interests and sustain a vibrant U.S. ICT sector, the United States must be able to maintain and expand its traditional ICT technology leadership in the face of expanding competition from China. Chinese firms are also made more competitive by state subsidies and by the Chinese government's methodical strategy of stealing advanced U.S. technology and intellectual property, which accelerates Chinese companies' work by years and saves billions of dollars in research and development investments.[8] U.S. economic interests must be protected from a growing global footprint of Chinese information technology products, which is being accelerated by the deployment of 5G wireless.

- **U.S. Global Mission Capability.** As U.S. military operations continue globally, a global information technology infrastructure comprised of Chinese 5G technology – and possibly operated by a Chinese company on behalf of a host nation telecommunications operator – could affect the security of U.S. and allied military and intelligence operations. U.S. and Allied forces may not be able to communicate securely on global IT infrastructures when the entity that controls the relevant portion of the infrastructure may not be friendly to U.S. interests or welcome U.S. involvement in their affairs.

[6] *Addition of Entities to the Entity List, 84 FR 22961 (May 21, 2019). At https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.*

[7] *David Welna, "Defense Budget Shifts Military's Focus From Terrorism to China and Russia," NPR, August 5, 2018. At https://www.npr.org/2018/08/05/635380840/defense-budget-shifts-militarys-focus-from-terrorism-to-china-and-russia.*

[8] *See, for example, National Counterintelligence and Security Center, Foreign Economic Espionage in Cyberspace, 2018, pp. 5-7. At https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf. See also Del Quentin Wilber, "China Has 'Taken the Gloves Off' in Its Thefts of U.S. Technology Secrets," Los Angeles Times, November 16, 2018. At https://www.latimes.com/politics/la-na-pol-china-economic-espionage-20181116-story.html.*

The following sections provide a more in-depth look at each of these three areas:

A. WIRELESS INFRASTRUCTURE SECURITY

The principal concern about 5G network security and resiliency is that the Chinese Government will be able to access and even control or interrupt data that passes through Chinese-made telecommunications equipment. In response to a question about ZTE and Huawei in a Senate Hearing in early 2018, FBI Director Christopher Wray summed up the threat:

> 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 telecommunication 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.[9]

Due to extreme concerns about the security risks of Chinese telecommunications equipment, the federal government has taken steps to prevent Chinese companies from selling 5G equipment in the United States. The National Defense Authorization Act of 2019 imposed restrictions on certain Chinese technology companies' access to the U.S. telecommunications market, and the May 2019 executive order effectively bans Chinese 5G equipment from U.S. 5G networks by prohibiting the use of telecommunications equipment that "poses an unacceptable risk to the national security of the United States."[10]

In considering the inherent security of the emerging 5G wireless infrastructure, the discussion usually begins (and frequently ends) with "who is supplying the hardware and software?" The four major U.S. wireless carriers had announced they would not purchase their 5G wireless infrastructure from either Huawei or ZTE, but many small local and regional carriers, which have a history of using Chinese gear due to their significantly lower price structure and attractive financing options, had made no such commitment. Nevertheless, equipment from Huawei and other Chinese companies is already present in the U.S. wireless and wired infrastructure. The existence of this equipment, upon which 5G technologies will be layered, must be dealt with as an element of a larger strategy.

Although the E.O. seems to prevent Huawei, ZTE, and other Chinese companies from ever selling its gear for use in U.S. 5G networks, it may not be the final word; not only does the E.O. offer the possibility of waivers, but either the current or a future U.S. administration could modify the order in response to changing political or commercial dynamics. Four months after the United States prohibited U.S. exports to ZTE in April 2018 (due to its export of goods with U.S.-made components to Iran and North Korea in violation of U.S. sanctions), the Commerce Department waived the ban – due in no small part to the impact that the ban would have on U.S. chip manufacturers that supplied ZTE. More than 200 American companies – including Qualcomm, Intel, and Texas Instruments – had sold more than $2 billion of components to ZTE in 2017.[11] Qualcomm alone stood to lose $500 million in sales from the ban.[12] Similarly, just five days after the May 2019 executive order, the Commerce Department granted a license for sales to continue for 90 days to mitigate the impact on U.S. technology companies.[13]

[9] Testimony of Christopher Wray, Director of the Federal Bureau of Investigation, before the Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community," S. HRG. 115–278, February 13, 2018, pp. 64-65. Transcript at https://www.govinfo.gov/content/pkg/CHRG-115shrg28947/pdf/CHRG-115shrg28947.pdf.

[10] Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019, Section 1(ii)(C). At https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[11] "China's ZTE paid over $2.3 billion to U.S. exporters last year, ZTE source says," Reuters, May 11, 2018. At https://www.reuters.com/article/us-usa-china-zte/chinas-zte-paid-over-2-3-billion-to-u-s-exporters-last-year-zte-source-says-idUSKBN1ID020.

[12] Zacks Equity Research, "Qualcomm's Revenues Might be Hit by Ban on Sales to ZTE," Nasdaq.com, April 17, 2018. At https://www.nasdaq.com/article/qualcomms-revenues-might-be-hit-by-ban-on-sales-to-zte-cm949022.

[13] Bobby Allyn and Matthew S. Schwartz, "Trump Administration Eases Ban on Huawei After Technology Stocks Tumble," NPR, May 20, 2019. At https://www.npr.org/2019/05/20/724910121/after-trump-ban-huawei-phones-will-lose-access-to-google-software.

The United States has urged allies and other Western countries to ban Chinese firms from their networks as well, but with mixed success.[14] U.S. allies such as Australia, New Zealand, and Japan have banned Huawei and ZTE from providing wireless infrastructure within their countries due to national security concerns.[15] The UK and Germany are pushing back on a ban, insisting the risk is manageable,[16] despite the fact that the UK's National Cyber Security Center Laboratory – jointly operated by Government Communications Headquarters and Huawei since 2010 – found numerous security flaws in the company's equipment.[17] Many European countries and the wireless carriers that serve them have resisted a ban on Chinese 5G hardware and software, since they already rely upon Huawei technology for large portions of their existing wireless infrastructure and are looking to reduce the costs of upgrading to 5G.

Going beyond the simple "county of origin" question, a serious look at the state of 5G infrastructure security is actually encouraging, at least within the leading U.S. carriers. Driven by the desire to make their 5G infrastructure "secure by design," the carriers have adopted a pragmatic approach that emphasizes open standards and software and embeds security at all layers of their infrastructure. Rather than rely on proprietary hardware and software from the individual providers with unknown provenance, the major carriers have coalesced on an approach for 5G that employs open standards, open source software, virtualization, white box hardware, containerized applications for edge-based computing services, and artificial intelligence-based security monitoring of all transaction and functions within the infrastructure. This significantly reduces security risk in the core of the infrastructure by providing transparency throughout the 5G wireless architecture, exposing all the components of the architecture to broad security scrutiny, and continuously monitoring the behavior of the infrastructure and applications it supports. While there is no such thing as perfect security, this approach provides confidence that the risks are appropriately managed and mitigated within the security state of the art. It also helps create opportunities for technological innovation and diversity in the supply chain, since a wireless carrier is no longer locked in to purchasing its entire wireless infrastructure from a single proprietary source to ensure that it all works together.

> Many European countries and the wireless carriers that serve them have resisted a ban on Chinese 5G hardware and software, since they already rely upon Huawei technology for large portions of their existing wireless infrastructure and are looking to reduce the costs of upgrading to 5G.

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

[15] *See "Huawei and ZTE Handed 5G Network Ban in Australia," BBC News, August 23, 2018. At https://www.bbc.com/news/technology-45281495. See also Charlotte Greenfield, "New Zealand Rejects Huawei's First 5G Bid Citing National Security Risk," Reuters, November 27, 2018. At https://www.reuters.com/article/us-spark-nz-huawei-tech/new-zealand-rejects-huaweis-first-5g-bid-citing-national-security-risk-idUSKCN1NX08U. See also Li Tao, "Japan Latest Country to Exclude Huawei, ZTE from 5G Roll-Out Over Security Concerns," Associated Press, December 10, 2018. At https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.*

[16] *Jethro Mullen, "UK Spies Think They Can Handle Huawei In 5G Networks. The US Doesn't Agree," CNN.com, February 18, 2019. At https://www.cnn.com/2019/02/18/tech/huawei-uk-5g-cybersecurity/index.html. Guy Chazan, "US Setback as Germany Fails to Ban Huawei in 5G Guidelines," Financial Times, March 7, 2019. At https://www.ft.com/content/3dae0df4-40eb-11e9-9bee-efab61506f44.*

[17] *Stu Woo, "Huawei Equipment Has Major Security Flaws, U.K. Says," Wall Street Journal, March 28, 2019. At https://www.wsj.com/articles/u-k-says-huawei-gear-has-major-security-flaws-11553765403.*

Residual security concerns in the 5G space carry over from current security issues in the wireless devices and services. The origin of the chip set and other components in a modern wireless device can be rather obscure; while U.S. vendors lead in the global chipset marketplace, that situation is changing as Chinese companies push into that marketplace, and many U.S. vendors employ offshore foundries to fabricate and package their components. Also, the operating systems used in mobile devices and commonly used applications (like web browsers, texting, e-mail, and social media services) can have inherent vulnerabilities which can open up attack surface in the wireless infrastructure. The advent of 5G services does not change this situation.

The evolution of the 5G wireless infrastructure will raise more significant national security risks, especially as more capabilities are added to support complex applications. This is particularly true in the IoT space, with complex services such as smart cities, autonomous vehicles, and virtual reality gaming and entertainment opening up attack surface within the 5G wireless infrastructure. We can expect that Chinese companies and those of other potential adversaries will be actively involved in development of many of these applications. China has already introduced city-wide AI-enabled applications, which will become larger and more data-rich as 5G connectivity expands. As Chinese companies "productize" and export these applications, they are likely to share data from other countries with China's government. Chinese companies will also be able to affect the configuration and operation of these infrastructures, including at the behest of Beijing.

"Beijing's 2015 "Made in China 2025" plan strives to make China mostly self-sufficient in semiconductor production by 2025, aided in part by $31.5 billion in state spending to establish a National Integrated Circuit Industry Investment Fund.

B. REGAINING TECHNOLOGY LEADERSHIP

Perhaps the only aspect of 5G wireless that is more important than the security of U.S. wireless infrastructure is the ability to continue and expand U.S. technical and innovation leadership in the global ICT marketplace. U.S. national security is inextricably linked to the economic influence created by American leadership in technology and innovation.

China has adopted a publicly-announced strategy to dominate the ICT marketplace in design, development, and manufacturing. Beijing's 2015 "Made in China 2025" plan strives to make China mostly self-sufficient in semiconductor production by 2025,[18] aided in part by $31.5 billion in state spending to establish a National Integrated Circuit Industry Investment Fund.[19]

[18] *McKinsey and Company, "A New World Under Construction: China and Semiconductors," November 2015. At https://www.mckinsey.com/featured-insights/asia-pacific/a-new-world-under-construction-china-and-semiconductors.*

[19] *Alex Capri, "Semiconductors – Beijing Versus the West," Nikkei Asian Review, October 12, 2018. At https://asia.nikkei.com/Opinion/Semiconductors-Beijing-versus-the-West.*

For most of the last 75 years or so, the United States took its leadership in ICT technology and innovation for granted. For a variety of reasons, however, U.S. leadership has eroded. Manufacturers lost their edge as most ICT hardware became commoditized in the marketplace and as other countries gained cost advantages in fabrication and packaging due to lower labor costs. Indeed, many U.S. technology leaders opened research and development laboratories in China to access the lower-cost technical talent available there, while companies in the U.S. met their staffing needs by hiring foreign technology workers on H1-B visas or by hiring foreign graduate students. These workers frequently return to their homelands and use the knowledge they gained in the United States to accelerate their native countries' ICT capabilities.

While U.S. manufacturing capability in the ICT space has declined, particularly in wireless infrastructure, the United States still contributes significantly to the establishment of global standards at bodies such as the 3rd Generation Partnership Project (3GPP), and to the development of the open source software for the wireless infrastructure Radio Access Network and Core. U.S. companies like Qualcomm and Intel also shape the wireless semiconductor space. China has also played an active role in 3GPP, likely in an effort to promote Chinese technologies' specifications as the basis for international 5G standards.[20]

C. U.S. GLOBAL MISSION CAPABILITY

Just as 5G networks' data capacity will enable a vast array of commercial and civilian applications, so too will it open the door for enhanced military capabilities. As described by the Defense Innovation Board (DIB), a federal advisory committee established to provide independent advice to the Secretary of Defense:

> 5G has the capability to combine DoD's current fragmented networks into a single network to promote improved situational awareness and decision-making. This expanded reach will enable new technologies like hypersonic weapons and hypersonic defenses to be deployed, and has the potential to strengthen existing missions like nuclear C3. At an enterprise level, 5G can vastly improve day-to-day tasks such as logistics and maintenance, elevating the efficiency and speed of work across DoD.[21]

[20] *Jill C. Gallagher and Michael E. DeVine, Fifth-Generation (5G) Communications Technologies: Issues for Congress, Congressional Research Service, Report R45485, January 30, 2019. At https://crsreports.congress.gov/product/pdf/R/R45485.*

[21] *Defense Innovation Board, The 5G Ecosystem: Risks & Opportunities for DoD, April 3, 2019, p. 21. At https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF.*

> The dependence of U.S. deployed assets – both military and civilian – on foreign networks makes U.S. dominance of 5G technologies a national security imperative as well as an economic and commercial priority.

U.S. national security requires that such military communications – as well as communications relating to diplomatic, intelligence, law-enforcement, peacekeeping, and humanitarian activities around the globe, some of them integrated with allies or coalition partners – be secure and reliable. These activities frequently rely on the global ICT infrastructure, as well as the infrastructures of our allies and partners, for all or part of their communications. The potential penetration by China of these infrastructures creates significant risks to U.S. mobilization, sustainment, and mission continuity. The use of Chinese equipment in developing countries' telecommunications networks will create a global operational environment in which the U.S. forces may be compelled to operate on systems subject to hostile influence or control.[22] Even though U.S. forces often deploy with U.S.-origin computing and communications systems that can operate independent of indigenous infrastructure, secure 5G technology can enhance deployed capability.

To examine and mitigate threats posed by "dirty" networks, the Department of Defense is evaluating 5G's suitability and desirability to support military operations despite the risks posed by Chinese equipment.[23] In doing this analysis, the DoD needs to consider its domestic employment of 5G communications (for such things as Smart Bases and training), as well as the use of 5G in foreign countries where the host nation may employ Chinese technology and telecommunications workers in its infrastructure. Other elements of the U.S. Government with overseas operations, such as the State Department and the Intelligence Community, need to address similar considerations in the use of 5G capabilities, perhaps joining with the DoD in their efforts.

The dependence of U.S. deployed assets – both military and civilian – on foreign networks makes U.S. dominance of 5G technologies a national security imperative as well as an economic and commercial priority. The United States should therefore assess counterintelligence and security risks country-by-country and develop the ability to deploy ICT capabilities that can independently support global deployments.

[22] Ellen Nakashima and Souad Mekhennet, "U.S. Officials Planning for a Future in Which Huawei Has a Major Share of 5G Global Networks," Washington Post, April 1, 2019. At https://www.washingtonpost.com/world/national-security/us-officials-planning-for-a-future-in-which-huawei-has-a-major-share-of-5g-global-networks/2019/04/01/2bb60446-523c-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.69cf840845cc.

[23] Marcus Weisgerber, "Pentagon to Explore Potential of 5G – and Its Made-in-China Hazards," DefenseOne, March 25, 2019. At https://www.defenseone.com/technology/2019/03/pentagon-explore-5gs-potential-and-its-made-china-hazards/155812/.

THE GLOBAL WIRELESS TECHNOLOGY LANDSCAPE

U.S. leadership in 5G technology faces challenges in four principal areas: the scope and scale of wireless infrastructure development in China versus other regions, which provides an economy of scale to Chinese equipment makers; limited U.S. funding for research and development; the decline of U.S. leadership in semiconductor manufacturing; and the departure of many U.S. manufacturers from the ICT market.

A. WIRELESS INFRASTRUCTURE

A significant shift in the global supply chain for wireless technology is underway. U.S. and Western dominance in design, development and standards in ICT has eroded, as Chinese companies have become increasingly aggressive in expanding their market share. Not everyone agrees on the root causes of this shift.

To some degree, it is a matter of spending and scale of effort. Since 2015, China outspent the United States by approximately $24 billion in wireless communications infrastructure and built 350,000 new sites, while the United States built fewer than 30,000. Looking forward, China's five-year economic plan specifies $400 billion in 5G-related investment. Consequently, China and other countries may be creating a 5G tsunami, making it nearly impossible to catch up.[24]

However, larger wireless market size, greater national investment in 5G deployment (and the sources of funding), and more wireless sites do not equate to wireless technology leadership. In fact, deploying a large and expensive physical infrastructure diverts available funding away from investment in innovation. A deeper analysis is required.

[24] *Deloitte Consulting LLP, 5G: The Chance to Lead for a Decade, 2018. At https://www2.deloitte.com/us/en/pages/consulting/articles/5G-deployment-for-us.html.*

It is well-known that Chinese firms and the Chinese government enjoy a special symbiotic relationship. China has adopted a publicly-announced strategy to dominate the ICT marketplace in design, development, and manufacturing by the 2025 time frame. It is well on its way to achieving that objective, with Huawei becoming the world's largest manufacturer of telecommunications equipment. The growing dominance of Chinese-owned or China-based companies in the telecommunications marketplace affords the Chinese government the opportunity to deliberately insert vulnerabilities into telecommunications equipment. Such "back doors" – which have been uncovered in cell phones, cameras, and other devices that were either made in China or customized for the Chinese market[25] – could allow the Chinese government to exploit communications or interrupt critical wireless services remotely at a time of its choosing.

Software and hardware pedigree are a paramount security concern as our telecommunications infrastructure evolves. U.S. national security depends on having secure reliable command, control and communications with warfighting assets, and much of the U.S. military's communications uses commercial telecommunications infrastructure.[26] Increasingly, much of the U.S. telecommunications infrastructure is becoming software-defined. The trend is towards virtualization in the wireless infrastructure, as Radio Access Network (RAN) and associated functions move to an approach based on Software Defined Network/ Network Function Virtualization (SDM/NFV). While this shift is not directly connected to 5G deployment, the cost savings and performance advantages of SDN/NFV are moving the entire communications/networking industry in that direction.

By Chinese law, 70 percent of the 1.5 billion-person Chinese telecommunications market is restricted to Chinese-owned firms. This enormous captive market potentially gives Chinese firms an immediate 5G production cost advantage due to scale. As noted earlier, however, the performance of Chinese companies in the global marketplace is distorted by their leverage of PRC government subsidies and low-cost loans, and market size may not prove to be a strategic advantage in reality. The effect of continued selling of 5G infrastructure at "loss leader" pricing, along with the global trend away from dedicated hardware and software to open source software running on generic "white box" hardware may in fact actually hurt Chinese vendors.

In response to concerns from the Administration and Congress, the largest national wireless carriers in the United States have announced that they will not employ Huawei or ZTE equipment as part of their 5G infrastructure.[27] However, many smaller regional telecommunications and wireless service providers would like to use Chinese firms as technology suppliers and operators due to their significant cost advantage.[28]

Further, the Chinese wireless carriers and technology vendors are partnered in the development of many broad IoT applications, including Smart Cities and autonomous vehicles, and are integrating these applications with sophisticated AI capabilities. Over time, these applications could spread into the global marketplace through various partnerships with U.S. and Western technology providers and wireless operators, thereby imperiling user privacy and security through a path that does not exploit the 5G wireless infrastructure itself. The United States and other Western countries must also focus their resources and innovation initiatives in the IoT space as well, particularly those with broad potential impact.

[25] Defense Innovation Board, pp. 25-26.

[26] Defense Innovation Board, p. 23.

[27] See Todd Shields and Bloomberg, "T-Mobile CEO to Congress: We Won't Use Huawei Equipment After Sprint Acquisition," Fortune, February 13, 2019. At http://fortune.com/2019/02/12/t-mobile-congress-testimony-huawei-equipment-sprint-acquisition/. See also Paul Mozer, "AT&T Drops Huawei's New Smartphone Amid Security Worries," New York Times, January 9, 2018. At https://www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html.

[28] John D. MacKinnon and Stu Woo, "Rural U.S. Carriers Resist Proposed Chinese Telecom Ban Aimed at Huawei," Wall Street Journal, February 11, 2019. At https://www.wsj.com/articles/rural-u-s-carriers-resist-proposed-chinese-telecom-ban-11549886402.

B. RESEARCH AND DEVELOPMENT

In recent decades, many leading U.S. technology companies have moved away from doing pure research to focus on developing capabilities that can bring more immediate return on investment. For example, the Bell Laboratories famous for landmark technology breakthroughs such as the transistor, laser, and maser has effectively ceased to exist.

At the same time, research in U.S. academic institutions has flattened in the ICT space, while foreign institutions increase their investments. According to Bloomberg:

> The U.S. is still out in front of global rivals when it comes to innovation, but American universities – where new ideas often percolate – have reason to look over their shoulder.
>
> That's especially true for technologies like 5G phone networks and artificial intelligence. They're exactly the fields where President Donald Trump recently insisted the U.S. has to lead – and also the ones where Asia, especially China has caught up.
>
> Universities in China, Korea, and Taiwan get more patents than their U.S. peers in wireless communications…. In AI, 17 of the top 20 universities and public research organizations are in China.[29]

While the reasons for the above are complex, U.S. federal funding for core ICT research has been flat (thus shrinking in real dollars) for at least the last ten years, according to the *Wall Street Journal*. To top it off, a significant share of ICT researchers in U.S. academia are foreign graduate students, many of whom go to work at a U.S. technology company after graduation and eventually return to their homeland with their knowledge of American technology.

C. SEMICONDUCTORS

Over the years, foreign governments – particularly Japan, South Korea, Taiwan, and China – have made several serious attempts to dominate semiconductor technology through government-financed R&D. In response, the United States established consortia such as the SEMATECH, a partnership formed in 1987 between the Department of Defense and 14 U.S. semiconductor manufacturers. SEMATECH achieved its original purpose of restoring U.S. leadership over Japan in semiconductor design and manufacturing, and it continues today, independent of U.S. government funding, as an international consortium of semiconductor companies working to advance state of the art semiconductor manufacturing.

Foreign acquisition of U.S. companies, particularly by China, has also eroded U.S. technical leadership and bolstered foreign competition. As one notable example, the then-U.S.-headquartered Broadcom was acquired in 2015 by Avago Technologies, a Singapore-based holding company which was once a part of Agilent Technologies, which itself had spun off from Hewlett-Packard in 1999. In 2018, the now Singapore-based Broadcom sought to acquire Qualcomm, a leading U.S. vendor of semiconductor chips to the global wireless device and infrastructure suppliers. This acquisition was blocked by the Committee on Foreign Investment in the United States (CFIUS), which reviews foreign investments to determine their effect on U.S. national security, on national security grounds. This history – a formerly American electronics manufacturer trying to acquire a current American manufacturer and bring its know-how under foreign control – encapsulates the ways in which foreign acquisitions have undermined the U.S. semiconductor industry.

[29] *Susan Decker, Alex Tanzi, and Bloomberg, "In Tech Race with China, U.S. Universities May Lose a Vital Edge," Fortune, March 2, 2019. At http://fortune.com/2019/03/02/us-tech-race-china/.*

In July of 2018, the Administration hosted a panel discussion at the SEMICON West conference to announce the development of a National Strategy for Semiconductor and Microelectronics Innovation. A press advisory for this discussion stated that the multi-agency initiative would "outline activities and new policies under development to ensure U.S. strategic leadership in microelectronics, including focused investment in innovations key to the next generation of devices for commercial and government use. The initiative also includes public-private partnerships to accelerate the capabilities of advanced semiconductors for critical applications such as artificial intelligence (AI), cyber, secure communications, the internet of things (IoT) and big data analytics."[30] The Administration should complete and publish this report as soon as possible, in collaboration with the U.S. semiconductor industry, so it can launch R&D, investment, and acquisition efforts to advance U.S. semiconductor manufacturing leadership.

D. MANUFACTURING

Although non-Chinese companies such as Ericsson, Nokia, and Samsung are developing 5G capabilities, China has been successfully executing its strategy to become the dominant supplier of ICT technology, particularly with respect to the manufacturing of 5G infrastructure and devices.

The U.S. telecommunications industry has gradually globalized, and wireless technology manufacturing has largely moved offshore due to lower costs and the availability of cheaper labor, frequently coupled with national financial subsidies to vendors. Some of the few U.S. companies that remain in the market, such as Apple (which makes wireless devices) and Qualcomm and Intel (which make semiconductor devices for the wireless market), have come to rely largely on offshore fabrication and packaging. Any U.S. strategy must deal with the reality that offshore manufacturing of hardware along with fabrication and packaging of semiconductor devices is a reality for the foreseeable future.

[30] *"Strategy for U.S. Semiconductor Leadership to be Previewed at SEMICON West," HPCwire, July 6, 2018. At https://www.hpcwire.com/off-the-wire/strategy-for-u-s-semiconductor-leadership-to-be-previewed-at-semicon-west/.*

> Any U.S. strategy must deal with the reality that offshore manufacturing of hardware along with fabrication and packaging of semiconductor devices is a reality for the foreseeable future.

These trends have been exacerbated by U.S. companies choosing not to compete in the marketplace for pennies on the dollar where products have largely been commoditized. Qualcomm, for example, withdrew from the cellular phone manufacturing business, preferring to invest in wireless chip innovation and design (which offer higher profit margins). Hong Kong-headquartered Lenovo Group purchased IBM's personal computer, laptop, and low-end server business, as IBM preferred to focus its innovation investments in platforms with higher profit margins. Lenovo also purchased Motorola Mobility, the last significant vestige of a U.S. manufacturing capability for wireless devices, from Google in 2014. Motorola was once the global leader in the development of cellular technology and the manufacture of advanced cellular devices.

The shift in importance from hardware to software also helped drive U.S. manufacturers out of the wireless business. Although Motorola Mobility excelled in wireless handset technology, it struggled with its software. Google purchased it in 2012 to manufacture devices for its own mobile operating system, but sales lagged and manufacturing was offshored to reduce cost. In 2014, Google sold Motorola to Lenovo, which saw the renowned brand name as an opportunity to enhance its presence in the United States.[31] Cisco, one of the last American companies active in this space, still participates in the RAN software market, and in fact has an agreement with Ericsson to provide its 5G RAN software.

Even as few U.S. providers of wireless infrastructure capability remain, Chinese companies have rapidly expanded into semiconductor manufacturing and 5G technologies.

- Huawei has become the world's largest provider of communications and network technology, and it is arguably the leading global player in manufacturing and deployment of 5G wireless infrastructure.
- In early 2018, ZTE raised $2.1 billion to support its development of 5G network infrastructure.[32] In January 2019, ZTE asserted it completed the first 5G phone call and successfully tested 5G video streaming and web browsing, using its own 5G prototype handset.[33]

[31] *"Motorola Brought Us the Mobile Phone, But Ended Up Merged Out of Existence," The Conversation, January 13, 2016. At https://theconversation.com/motorola-brought-us-the-mobile-phone-but-ended-up-merged-out-of-existence-33967.*

[32] *Sijia Jiang, "China's ZTE Corp to Raise $2 Billion in Share Placement for 5G Plans," Reuters, January 31, 2018. At https://www.reuters.com/article/us-zte-5g-placement/chinas-zte-corp-to-raise-2-billion-in-share-placement-for-5g-plans-idUSKBN1FK1NQ.*

[33] *Juan Pedro Tomás, "ZTE Completes 5G Test with China Unicom," RCR Wireless News, January 18, 2019. At https://www.rcrwireless.com/20190118/5g/zte-completes-5g-test-china-unicom.*

A number of companies that are neither American nor Chinese offer more reliable alternatives to Chinese 5G equipment that could be installed in the United States.

- Samsung, a South Korean company that is currently the leading provider of wireless handsets, has announced its entry into the 5G wireless infrastructure market, intending to compete with Huawei, ZTE, Ericsson, and Nokia. The firm announced it would invest $22 billion in 5G in an attempt to capture 20 percent of the global wireless market.[34] If successful, Samsung would open up a non-Chinese based wireless infrastructure in the U.S. marketplace.
- A Taiwan-headquartered company, Foxconn (officially known as Hon Hai Precision Industries Co. Ltd.), is the world's largest contract manufacturer of electronic devices and the world's fourth largest information technology company by revenue. Foxconn has manufacturing plants in at least nine countries (including China), employing more than 800,000 workers.
- The Swedish company Ericsson has successfully pursued 5G deals in many Western countries concerned about the security of Chinese technologies. In February 2019, Ericsson announced signed or pending 5G deals with more than 50 service providers, and it has already deployed 5G networks in the United States, Europe, Australia, and Asia.[35] Ericsson is estimated to have captured 13 percent of the global 5G market.[36]
- Nokia, a Finnish company, has invested $851 million for R&D in Europe alone as of December 2018, and the company pledged to prioritize future spending on 5G over legacy technologies. The company announced it would reorganize and cut costs by $800 million expressly to be more competitive in the global 5G market,[37] of which it has already captured roughly 17 percent.[38]

Equipment from Huawei and other Chinese companies is already present in the U.S. wireless and wired infrastructure. The existence of this equipment, upon which 5G technologies will be layered, must be dealt with as an element of a larger strategy.

[34] Niclas Rolander and Sam Kim, "Samsung's 5G Network Grab Gets Boost with Huawei, ZTE Under Fire," Bloomberg, December 19, 2018. At https://www.bloomberg.com/news/articles/2018-12-19/samsung-s-5g-network-grab-gets-boost-with-huawei-zte-under-fire.

[35] Börje Ekholm, "The World is Talking About 5G. We Are Deploying It," Ericsson Blog, February 15, 2019. At https://www.ericsson.com/en/blog/2019/2/Ekholm-5G-deployment-Europe-security.

[36] Elias Groll, "Who Benefits from the U.S. Crackdown on Huawei?" Foreign Policy, January 31, 2019. At https://foreignpolicy.com/2019/01/31/who-benefits-from-the-u-s-crackdown-on-huawei/.

[37] Anne Morris, "Nokia Bolsters 5G R&D Coffers with $283 Million Loan," SDxCentral.com, December 3, 2018. At https://www.sdxcentral.com/articles/news/nokia-bolsters-5g-rd-coffers-with-283-million-loan/2018/12/.

[38] Groll, January 31, 2019.

E. WIRELESS SPECTRUM

Yet another consideration in 5G deployment in the United States and elsewhere around the globe is the availability of sufficient wireless spectrum to support the huge amounts of bandwidth needed to transport all the expected data. Wireless spectrum is a precious commodity, and despite the many innovations in 5G to increase available bandwidth, the propagation and capacity of a given frequency is still subject to the laws of physics. Higher frequencies provide more bandwidth, but don't propagate as well as lower frequencies. Thus, for successful 5G deployment nationwide, wireless carriers will require a wide range of frequency choices appropriate for varied local physical conditions. In urban areas, wireless service providers will typically employ the higher frequencies of the Millimeter Wave bands of 30 GHZ and above, along with small cells mounted short distances apart on buildings and telephone poles, along with techniques as beam shaping, to optimize their capabilities. In these scenarios, many of the wireless carriers are planning to provide 5G services to fixed locations (replacing local fiber optics) as well as to mobile users and devices. In less populated regions, the wireless providers will implement more conventional wireless frequencies, such as the 700MHz and 1900MHz bands, to provide connectivity over greater distances, albeit with lower bandwidths.

In the United States, the Federal Communications Commission (FCC) has stepped forward aggressively to assure that the spectrum required for the success of 5G is available, as well as to facilitate the installation permitting process for new cell towers and small cells. But other players like the Commerce Department's National Telecommunications and Information Administration (NTIA) and the Department of Defense, which are responsible for management of wireless spectrum for U.S. government use, must work collaboratively with the FCC and the wireless industry to assure the optimum utilization of available spectrum for the benefit of all and to promote the timely deployment of 5G.

Proposals have been floated to take the deployment of 5G wireless technology out of the hands of the wireless carriers and replace it with a centralized "national wholesale" network that would sell capacity to private carriers. However, senior government officials, including FCC Chairman Ajit Pai, have emphasized that a free market, private sector-led approach to developing 5G would lead to greater innovation and faster rollout,[39] and a bipartisan group of senators has introduced legislation that would block the "nationalization" of 5G infrastructure.[40] Given the considerable progress and momentum already established by the leading wireless carriers in the U.S. and around the world – which will be accelerating in the coming years – a nationalized 5G network would do little, if anything, to accelerate 5G deployment or enhance U.S. innovation and competitiveness.

[39] *Dean DiChiaro, "Nationalization Question Hangs Over White House's 5G Announcement," Roll Call, April. 15, 2019. At https://www.rollcall.com/news/policy/nationalization-question-hangs-white-houses-5g-announcement.*

[40] *"Senate Bill Would Block Move to 'Nationalize' 5G Tech," MeriTalk, March 28, 2019. At https://www.meritalk.com/articles/senate-bill-would-block-move-to-nationalize-5g-tech/. See also "Secure 5G and Beyond Act of 2019," S. 893, 116th Cong. (2019).*

SOME EXAMPLES OF 5G/IoT APPLICATIONS

5G wireless provides a uniquely capable communications and computation platform, but the largest part of the anticipated value is the innovative applications it can support, under the rubric of the Internet of Things (IoT). Many companies around the world are already developing a wide variety of applications, which could drive broad societal change in the way we work and live.

While the companies capable of providing scalable 5G wireless infrastructure are limited, virtually anyone can develop an IoT application based on 5G capabilities. Some application developers are working independently of the wireless providers, and some are partnering closely with providers to ensure that the wireless network capabilities their application requires will be available to them. One of the features of 5G is referred to as network slicing, which furnishes on-demand network capabilities and cloud-based computing resources at the network edge and in the infrastructure itself to optimize the performance of a particular application.

The IoT application space includes capabilities ranging from the very complex to the simple and straight-forward. To list just a few:

- Sophisticated industrial control systems with embedded sensors for smart manufacturing, robotics control, smart power generation and optimized distribution, smart shipping and delivery systems, smart fleet and industrial maintenance systems.
- Smart cities, including smart homes and buildings for energy efficiency, smart traffic control and public transportation systems, intelligent appliances.
- Virtual reality systems, including sophisticated entertainment and gaming, industrial simulation and training, medical treatment, first responder, police, fire, and rescue operations, and military training and operations.

- Autonomous vehicles, including self-driving cars and trucks.
- Drone control for safety, rescue, and surveillance operations and for automated delivery applications.
- Smart healthcare, including advanced imaging and diagnostics, robotic surgery, genetic engineering of drugs and treatment protocols.

In other words, IoT applications will only be limited by the imaginations of application developers. Many applications will be paired with artificial intelligence, and in the future perhaps with quantum computing as that field advances. Many of the applications listed above will be integrated together over time, such as autonomous vehicles with smart traffic controls.

While these potential applications provide great promise, they certainly also provide a significant risk from a national security perspective if not managed properly. For many years the United States has been concerned about the security of its power grid and other critical infrastructure from foreign interruption. The United States must be able to address this problem both nationally and globally, working with our foreign allies; state, local, and tribal governments; private infrastructure operators; and application developers and vendors.

SPECIFIC RECOMMENDATIONS

No one set of steps by one set of actors can, by itself, promote 5G network security and resiliency. Any solution will require collaboration between U.S. government agencies and U.S. technology companies, as well as their counterparts in allied countries. In addition to recommending actions by U.S. intelligence agencies to understand foreign threats and steps by regulatory agencies to promote U.S., competitiveness, INSA recommends a collaborative public/private initiative to mitigate security vulnerabilities and incentivize U.S. technology leadership.

MITIGATING NATIONAL SECURITY RISKS

1. **The imminent deployment of 5G technology in the United States means that the White House must drive government-industry collaboration on steps to mitigate the national security risks.** Given the enormous capital costs of modernizing telecommunications networks, 5G equipment, once installed, will be in place for a long time. While the May 16, 2019, BIS decision to add Huawei to the Entity List effectively prohibits the use of Chinese equipment in U.S. 5G networks, the restrictions could be waived or removed in the future. If Chinese technology does become incorporated into U.S. 5G networks, there is great concern that the Chinese government will acquire a "back door" into critical U.S. and allied communications that lasts for decades or more.

   While the Executive Order was a step in the right direction, its provisions were developed in the narrow context of limiting immediate risk, as well as part of the ongoing saga of larger trade and tariff negotiations with the Chinese government, which has been a difficult road at best. A continuing, in-depth dialogue between the Administration and the key technology leaders in the U.S. private sector is needed to develop and implement a comprehensive strategy for maintaining and expanding U.S. leadership in technology innovation in the years to come. This strategy must be framed as part of our global trade and tariff interests and the negotiations with China and other major trading partners.

2. **The Intelligence Community should evaluate foreign strategies for acquiring U.S. innovation and technologies,** and possibly for influencing U.S. 5G wireless infrastructure and the IoT applications it will support, to their advantage. In conjunction with this effort, the Administration and Congress should review and expand existing mechanisms for preventing foreign-owned companies from gaining sensitive footholds in 5G networks and IoT applications, such as the CFIUS, and identify 5G technologies, components, or intellectual property whose potential acquisition by foreign companies should be reviewed.

MAINTAINING GLOBAL MISSION CAPABILITIES

3. **The United States must work with allies and partners to eliminate or mitigate security risks from foreign 5G networks incorporating Chinese technology.**

    a. To eliminate the threat where possible, the United States should continue urging its allies and partners to ban Chinese firms from their 5G networks.

    b. To mitigate the threat where necessary, the United States should develop technical solutions that enable U.S. and allied military forces and intelligence agencies to operate securely on telecommunications networks that could be compromised. Solutions may include the use of improved encryption or segregation of communications over multiple networks.

REGAINING U.S. LEADERSHIP IN WIRELESS TECHNOLOGY

4. **The White House should form a public/private sector Working Group on defining U.S. Trade Policy and Strategy** with respect to wireless technology **and innovation,** including 5G and IoT applications deployment in the United States. Participants should be senior officials from relevant agencies – including the FCC, the Office of the U.S. Trade Representative, and the Departments of Commerce and Treasury – as well as from wireless carriers, the U.S. technology industry, venture capital community, and academia. This Working Group should ensure that key U.S. government policy makers and private sector technology leaders have a common understanding of the national security risks and challenges in the deployment of 5G wireless infrastructure in the United States.

    The priorities of the working group should be to:

    A. **Develop a common strategy for strengthening current areas of U.S. technology leadership in 5G, IoT, and future wireless generations,** along with specific recommendations to achieve this goal through U.S. trade policy, incentives for private sector investment in future technologies, and increased U.S. government investments in advanced research by organizations such as the National Science Foundation (NSF), the Defense Advanced Research Projects Agency (DARPA), the Department of Energy's National Laboratories, and other appropriate research entities.

    B. **Establish a public-private mechanism to continuously "red team" 5G infrastructure** and the IoT applications it supports as it's deployed throughout the United States. Participants should include U.S. government agencies with expertise in cybersecurity and foreign cyber threat vectors, such as the FBI, USCYBERCOM, NSA, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, as well as leading wireless carriers and 5G equipment manufacturers.

    C. **Develop common strategies to reduce the overall security risk to U.S. 5G infrastructure,** such as wider use of open source software, zero-trust networking concepts, virtualization and containerization of key security functions and applications, and the employment of artificial intelligence techniques for advanced threat detection.

5. The FCC and the NTIA should continue to implement regulatory and policy changes that would **remove barriers to rapid deployment of 5G and make more radio spectrum available for 5G.**

6. With significant input from technology leaders in the U.S. telecommunications sector, **Congress should develop legislation to expand U.S. private sector investment in ICT and wireless innovation.** In undertaking this effort, Congress should draw on private sector entities, such as the Business Roundtable, U.S. Chamber of Commerce, or the Cellular Telephone Industry Association that have interested membership and in-depth expertise.

CONCLUSION

The United States must develop a comprehensive strategy to regain global leadership in wireless technology, as well as a strategy to deal with the consequences of the expanding Chinese dominance in the ICT and 5G market. While the U.S. government is engaged in an on-going trade dialogue with China, it has not established a vehicle for consistent, comprehensive dialogue with industry leaders and investors to discuss the challenges, solutions, and strategies for reestablishing U.S. leadership in wireless technology, or to address ways to maintain security of U.S. and allied 5G networks.

Given the right incentives, American industry can and will expand investment in wireless technology to regain U.S. leadership over time, including network architecture and virtualization, open source software development, and international standards. Greater involvement by U.S. technology companies in 5G wireless and IoT applications will engender innovation in the technology itself and will promote security and resilience in the U.S. telecommunications infrastructure and in the other critical infrastructure sectors it supports.

If implemented effectively, the above recommendations will reduce the considerable supply chain risk posed by the Chinese government and by Chinese companies to the U.S. 5G infrastructure, minimizing the chance of deliberate disruption of U.S. communications infrastructure, preventing the theft of U.S. companies' intellectual property, and securing sensitive information carried over the wireless infrastructure. Further, they would put the United States on a path towards regaining U.S. technology leadership in wireless communications.

RECOMMENDED READING ON 5G WIRELESS

Accenture Strategy, *Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities,* 2017. At https://www.accenture.com/us-en/insight-smart-cities.

Australian Strategic Policy Institute, Huawei and Australia's 5G Network: Views from ASPI, Report No. 8/2018, October 2018. At https://www.aspi.org.au/report/huawei-and-australias-5g-network.

Chertoff Group, "Are We Leading the 5G Race?" *Intelligence & Insights, Episode 36.* Podcast audio. April 22, 2019. At https://www.chertoffgroup.com/podcasts.

Center for Strategic and International Studies, "Mitigating Security Risks to Emerging 5G Networks," discussion transcript, February 6, 2019. At https://www.csis.org/analysis/mitigating-security-risks-emerging-5g-networks.

CTIA, *The Global Race to 5G,* April 2018. At https://www.ctia.org/the-wireless-industry/the-race-to-5g.

Deloitte Consulting LLP, *5G: The Chance to Lead for a Decade,* 2018. At https://www2.deloitte.com/us/en/pages/consulting/articles/5G-deployment-for-us.html.

Ericsson, *Ericsson Mobility Report,* November 2018. At https://www.ericsson.com/en/mobility-report/reports/november-2018.

Eurasia Group, *The Geopolitics of 5G,* November 15, 2018. At https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g.

Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board, *2019 Annual Report: A report to the National Security Advisor of the United Kingdom,* March 2019. At https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

Jones, James L., "Recommendations on 5G and National Security," Atlantic Council Scowcroft Center for Strategy and Security, Strategic Insights Memo No. 3, February 11, 2019. At https://www.atlanticcouncil.org/images/acevents/BrentScowcroftCenter/Strategic_Insights_Memo_vF_2.11.pdf.

Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik, *Huawei, 5G and China as a Security Threat,* NATO Cooperative Cyber Defence Centre of Excellence, 2019. At https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/.

Kennedy, Scott, *The Fat Tech Dragon, Benchmarking China's Innovation Drive,* Center for Strategic and International Studies, August 2017. At https://www.csis.org/analysis/fat-tech-dragon.

Lewis, James A., *How Will 5G Shape Innovation and Security: A Primer,* Center for Strategic and International Studies, December 2018. At https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security.

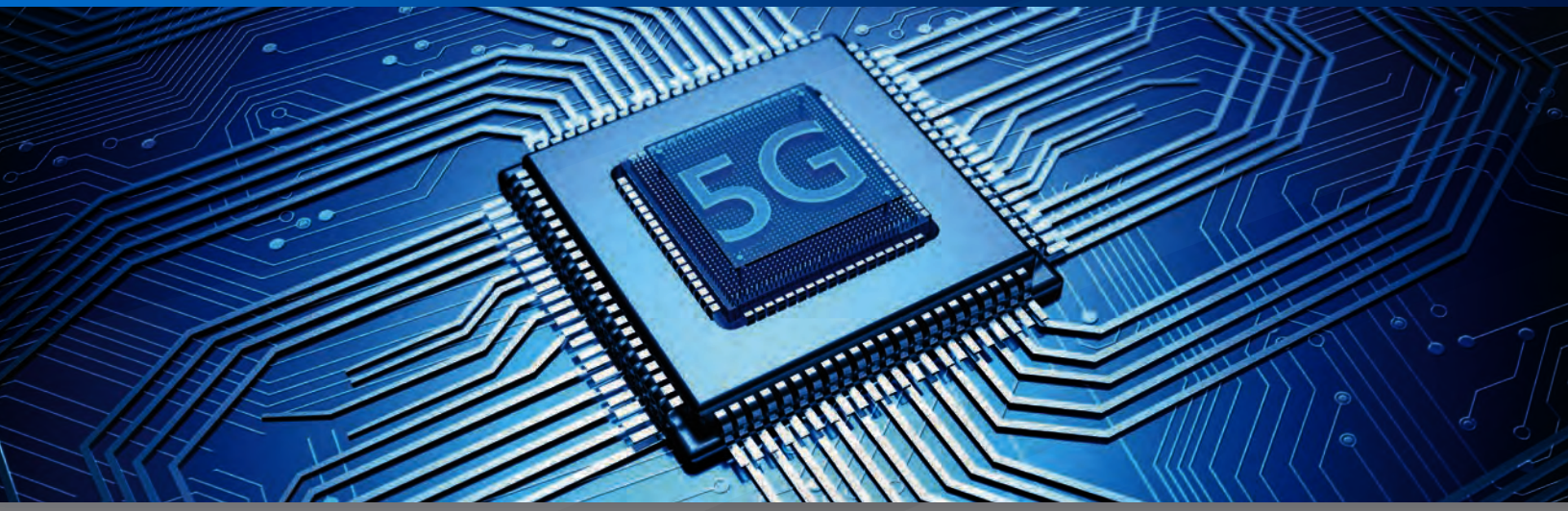
Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* October 8, 2012. At https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT INSA'S CYBER COUNCIL

The Cyber Council fuses the knowledge of industry, government, and academic experts to provide authoritative and influential insights regarding national security challenges in the cyber domain. Council members works to promote a greater understanding of the cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.



INSA
INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org