DECEMBER 2018

How Will 5G Shape Innovation and Security: A Primer

AUTHOR
James A. Lewis

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Report of the
CSIS TECHNOLOGY POLICY PROGRAM

DECEMBER 2018

How 5G Will Shape Innovation and Security

A Primer

AUTHOR
James A. Lewis

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

We would like to thank William Crumpler, Manyi Kathy Li, and Jordan Miller for their contributions to this report. This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, D.C. 20036
202-887-0200 | www.csis.org

Executive Summary

How 5G Will Shape Innovation and Security

- The fifth generation of mobile network technologies, known as "5G," promises greater speed, security, and capacity. 5G will underpin the internet economy and provide the backbone for the next generation of digital technologies. So, it is unsurprising that there is intense competition among companies and countries for 5G leadership.
- 5G will determine the direction the internet will take and where nations will face new risks and vulnerabilities. Who makes 5G technologies will affect security and innovation in an increasingly competitive technological environment. Decisions made today about 5G will affect national security and economic performance for decades to come.
- This is a competition among companies and groups of companies but also a competition between market-based and state-directed decisionmaking. The United States has relied on the former, China on the latter, and Europe falls somewhere in between.
- American technology remains essential for 5G mobile telecommunications. American companies have been strong performers in developing 5G technologies, but the United States and its allies face a fundamental challenge from China. The focus of competition is over 5G's intellectual property, standards, and patents. Huawei, for example, has research programs to develop alternatives to American suppliers, and U.S. trade restrictions have accelerated China's efforts to develop its own 5G industry.
- While American companies lead in making essential 5G technologies, there are no longer any U.S. manufacturers of core telecommunications network equipment. Four companies dominate the market for the core network technologies needed for 5G networks. None of these companies are American.[1] The choices are between European security partners (Ericsson and Nokia) and China (Huawei and ZTE).
- Telecom is a strategic industry and having two companies with close ties to a hostile power creates risk for the United States and its allies. A secure supply chain for 5G closes off dangerous areas of risk for national security in terms of espionage and the potential

1. Samsung has significant network and chip-making capabilities but still has a relatively small share of the 5G market.

disruption to critical infrastructures. China's aggressive global campaign of cyber espionage makes it certain that it will exploit the opportunities it gains as a 5G supplier.

- One way to envision this is to imagine that the person who built your house decides to burgle it. They know the layout, the power system, the access points, may have kept a key, and perhaps even built in a way to gain surreptitious entry. Major telecom "backbone" equipment connects to the manufacturer over a dedicated channel, reporting back on equipment status and receiving updates and software patches as needed, usually without the operator's knowledge. Equipment could be sold and installed in perfectly secure condition, and a month later, the manufacture could send a software update to create vulnerabilities or disrupt service. The operator and its customers would have no knowledge of this change.

- The United States can manage 5G risk using two sets of policies. The first is to ensure that American companies can continue to innovate and produce advanced technologies and face fair competition overseas. American and "like-minded" companies routinely outspend their Chinese competitors in 5G R&D and hold 10 times as many 5G patents. Chinese companies still depend on the western companies for the most advanced 5G components.

- The second is to work with like-minded nations to develop a common approach to 5G security. The United States cannot meet the 5G challenge on its own. When the United States successfully challenged Chinese industrial policy in the past, it has been done in concert with allies.

- Another task will be to find ways to encourage undecided countries to spend on 5G security. Huawei's telecom networks cost between 20 to 30 percent less than competing products. Huawei also offers foreign customers generous terms for leasing or loans. It can do this because of its access to government funds. Beijing supports Huawei for both strategic and commercial reasons. Many countries will be tempted by the steep discount. Not buying Huawei means paying a "premium" for security to which economic ministries are likely to object. The United States will need to encourage others to pay this security premium while at the same time preparing for a world where the United States unavoidably connects to Huawei-supplied networks and determine how to securely connect and communicate over telecom networks in countries using Chinese network equipment.

- The United States does not need to copy China's government-centric model for 5G, but it does need to invest in research and adopt a comprehensive approach to combatting non-tariff barriers to trade. 5G leadership requires a broader technology competition policy in the United States that builds the engineering and tech workforce and supports both private and public R&D. The United States also needs to ensure that U.S. companies do not face obstacles from antitrust or patent infringement investigations undertaken by other countries to obtain competitive advantage.

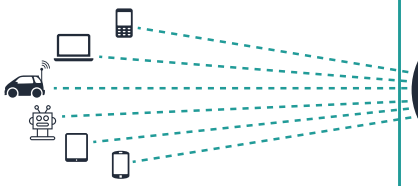
- In the twentieth century, steel, coal, automobiles, aircraft, ships, and the ability to produce things in mass quantity were the sources of national power. The foundations of security and power are different today. The ability to create and use new

technologies is the source of economic strength and military security. Technology, and the capacity to create new technologies, are the basis of information age power. 5G as the cornerstone of a new digital environment is the focal point for the new competition, where the United States is well-positioned to lead but neither success nor security are guaranteed without action.

5G Networking Diagram

Company Countries **US** U.S. **EU** European **CH** Chinese **SK** South Korean

User Equipment

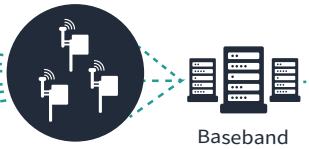


Smartphones, laptops, tablets, autonomous vehicles, VR/AR equipment, and consumer and industrial IoT devices

Industrial IoT Hardware
Market Leaders (2018)[1]
1. **US** Cisco
2. **CH** Huawei
3. **EU** Ericsson
4. **EU** TE Connectivity
5. **US** Qualcomm

Smartphone
Market Leaders (2Q18)[2]
1. **SK** Samsung (21%)
2. **CH** Huawei (16%)
3. **US** Apple (12%)
4. **CH** Xiaomi (10%)
5. **CH** OPPO (9%)

Radio Access Network (RAN)



Small Cell Radio Units

Baseband Unit Pool

RAN Equipment
Market Leaders (1Q18)[3]
1. **CH** Huawei (31%)
2. **EU** Ericsson (29%)
3. **EU** Nokia (23%)
4. **CH** ZTE (9%)
5. **SK** Samsung (4%)

Core Network

Core Network Infrastucture

Evolved Packet Core (LTE)
Market Leaders (1Q18)[4]
1. **EU** Ericsson
2. **CH** Huawei
3. **EU** Nokia
4. **US** Cisco
5. **CH** ZTE

Top two vendors account for over 60% of the market.

Service Provider Router and Ethernet Switch
Market Leaders (1Q18)[5]
1. **US** Cisco
2. **CH** Huawei
3. **EU** Nokia
4. **US** Juniper

Top four vendors account for over 90% of the market.

Select Mobile Network Equipment Components

Small Cell Antenna Array
Market Leaders (US - 2017)[6]
1. **EU** Alpha Wireless
2. **EU** Ericsson
3. **US** Galtronics

Data Converter Chip
Market Leaders (2017)[8]
US Texas Instruments
US Analog Devices

Small Cell Chipset
Market Leaders (2017)[10]
US Qualcomm
US Intel
CH HiSilicon
EU NXP Semiconductor
EU Ericsson
US Cavium

Ethernet Switch Chips
Market Leaders (2015)[12]
US Broadcomm (94.5%)

Small Cell Power Amplifier
Market Leaders (2017)[7]
US Texas Instruments
EU NXP Semiconductor
US Qorvo
US Broadcom
US Anadigics

Network Processor
Market Leaders (2016)[11]
1. **US** Intel
2. **US** Broadcom
3. **CH** HiSilicon
4. **US** Qualcomm
5. **US** Texas Instruments

FPGA
Market Leaders (2017)[9]
US Intel
US Xilinx

Server
Market Leaders (2Q18)[13]
1. **US** Dell (28.8%)
2. **US** HPE
3. **US** IBM (7.3%)
4. **CH** Lenovo (6.9%)
5. **CH** Inspur (4.8%)

1: "IoT ONE Connectivity Hardware 10 (2018)," IOT One, https://www.iotone.com/top10-2018/connectivity-hardware
2: "Smartphone Vendor Market Share," IDC, https://www.idc.com/promo/smartphone-market-share/vendor
3: Baburajan K, "RAN market: How Huawei, Ericsson, Nokia, ZTE, Samsung performed," Telecomlead, July 31, 2018, https://www.telecomlead.com/telecom-equipment/ran-market-how-huawei-ericsson-nokia-zte-samsung-performed-85605
4: Mike Robuck, "Report: EPC is pushing network functions virtualization to new heights," Fierce Telecom, June 5, 2018, https://www.fiercetelecom.com/telecom/report-epc-pushing-network-functions-virtualization-to-new-heights
5: "Service Provider Router and Switch Market Falls to a Five-Year Low in 1Q18 According to Dell'Oro Group," June 7, 2018, http://www.delloro.com/news/service-provider-router-and-switch-market-falls-to-a-five-year-low-in-1a18-according-to-delloro-group
6: "EJL Wireless Research Reports U.S. Outdoor Small Cell Antenna Shipments Up 84% in 2017," EJL Wireless, September 21, 2018, http://ejlwireless.com/news/2018/09/22/ejl-wireless-research-reports-u-s-outdoor-small-cell-antenna-shipments-up-84-in-2017/
7: "Small Cell Power Amplifier Market 2018 Global Overview, Business Growth, Development Status, Opportunities, Future Plans, Competitive Landscape, Emerging Trends and Potential of Industry Till 2022," Market Research Future, December, 2018, http://www.crossroadstoday.com/story/39185696/small-cell-power-amplifier-market-2018-global-overview-business-growth-development-status-opportunities-future-plans-competitive-landscape-emerging
8: Joe Madden, "Industry Voices—Madden: The impact of the ban on exports to ZTE," Fierce Wireless, April 24, 2018, https://www.fiercewireless.com/tech/industry-voices-madden-impact-ban-exports-to-zte
9: Joe Madden, "Industry Voices—Madden: The impact of the ban on exports to ZTE," Fierce Wireless, April 24, 2018, https://www.fiercewireless.com/tech/industry-voices-madden-impact-ban-exports-to-zte
10: David Chambers, "Broadcom downsize small cell chipset operations," Think Small Cell, October 4, 2016, https://www.thinksmallcell.com/Chipsets/broadcom-downsize-small-cell-chipset-operations.html; Martha DeGrasse, "Small cell chip vendor update," RCR Wireless News, January 30, 2017, https://www.rcrwireless.com/20170130/chips/small-cell-chip-vendor-update-tag4-tag99
11: Ashraf Eassa, "Intel Corporation Breaks Down its Networking Business," The Motley Fool, February 13, 2017, https://www.fool.com/investing/2017/02/13/intel-corporation-breaks-down-its-networking-busin.aspx
12: Craig Matsumoto, "Broadcom Ups Its Game in Ethernet Switching," Light Reading, December 19, 2017, https://www.lightreading.com/white-box/white-box-systems/broadcom-ups-its-game-in-ethernet-switching/d/d-id/739182
13: "Top five server vendors in Q2 2018," Telecomlead, September 6, 2018, https://www.telecomlead.com/telecom-statistics/top-five-server-vendors-in-q2-2018-86180

How 5G Will Shape Innovation and Security

A Primer

The fifth generation of mobile network technologies, known as "5G," promises greater speed, security, and capacity. 5G will underpin the digital economy and will provide the backbone for the next generation of digital technologies. So, it is unsurprising that there is intense demand for 5G networks and intense competition among companies and countries to meet that demand.

The 5G contest is about networks, data, the direction the internet will take, how economies will grow, and where nations will face new risks and vulnerabilities. Part of this involves investing in and deploying 5G networks. But who makes 5G technologies, who sets the standards, and who owns the intellectual property (IP) has implications for security, innovation, and employment in an increasingly competitive technological environment. Decisions made today about 5G will affect national security and economic performance for decades.

American companies have been strong performers in developing and preparing to deploy 5G technologies, but the United States and its allies face a fundamental challenge from China. There are no longer any U.S. manufacturers for core telecommunications network equipment. Four companies dominate the market for the core network technologies needed for 5G networks. None of these companies are American. The choices for core network equipment are between European security partners (Ericsson and Nokia) and China (Huawei and ZTE). Samsung, with its substantial chipmaking and equipment-making capabilities, has also entered the 5G race but still has a relatively small share of the market. Telecoms are a strategic industry and having two companies with close ties to a hostile power creates risk for the United States and its allies.

The outcomes in the 5G race will help determine national competitiveness and technological capabilities. 5G will affect the many industries that will be built on top of it, just like the app economy was built on top of 4G. Countries and companies that do better in making and deploying 5G will be richer and have an inside track in building a world where computing and connectivity are embedded in every device.

5G Reshapes the Digital World

5G networks will be among the most complex systems ever designed. 5G uses radio spectrum to transmit vast amount of data at higher speed and with greater reliability than previous technologies. It is this combination of speed and reliability that will lead to new, advanced services in health care, automobiles, robotics, entertainment, and to innovations we have not yet envisioned. By allowing more devices to connect to each other more securely and at higher speeds, a 5G environment will essentially create a new digital environment.

Looking at the last generation of telecom technology—4G—provides perspective. 4G is the smartphone in your pocket. It is more powerful and can access more information than the "supercomputers" the United States used in the Cold War to design nuclear weapons. This in itself is a triumph, but what is more important is the economic growth that 4G enabled. 4G is the basis for the "app economy," the outburst of innovation and investment largely centered in Silicon Valley that changed the way people use the internet. 4G created new economic opportunities and industries, and the internet economy grew four times as fast as overall U.S. GDP.

We can think of 5G as a chain of technologies, starting with devices at the edge of the network (such as a phone, robot, or car) which connect via specialized antenna to modems in advanced base stations and ultimately link to routers that form larger networks, allowing fast, reliable connections to other devices or to data and processes stored in the "cloud."[2]

Semiconductors are the most important components of 5G technologies and American companies are still the major suppliers. China's efforts to become self-reliant in semiconductors are not advanced enough to support 5G, and despite massive spending, this will not change in the foreseeable future.

Opening the hood of the 5G supply chain reveals complex interconnections. Chinese products cannot work without crucial American components. These American components use Chinese parts. There are complex commercial relationships and partnerships among American, Japanese, Taiwanese, Chinese, and Korean companies. Only two companies—Huawei and Samsung—intend be self-reliant, an alternative business strategy that offers greater market share if it succeeds, but most companies rely on a broad global supply chain to ensure access to innovations in technology and production.

The technologies that 5G will enable also have significant military value. These include robots, artificial intelligence, and a number of advanced sensing devices. As entrepreneurs rush to exploit the opportunities for new services and products that 5G offers, there will be spillovers to the defense technology base. 5G will be a foundational technology for new military capabilities.

A New Kind of Great Power Competition

Technological innovation has become a major part of the competition among states, but this competition sits uneasily atop an intermeshed global innovation environment where

2. The cloud also provides the computing resources that allow for "software defined networks."

international research and business partnerships are the norm. Science has become international, as scientists are more productive using research conducted by multinational teams of specialists. Commercial partnerships are the rule—and essential—for producing advanced technology. This is a much more difficult environment to establish national "leadership," and policies that emphasize building and maintaining strong competitive companies work best in this situation.

5G is a technological competition on many levels. It is a contest between economic models. It is a competition among companies and groups of companies but also between market-based and state-directed decisionmaking. The United States has relied on the former, China on the latter, and Europe falls somewhere in between. It is worth noting that the market-based model (with supportive government policies) has been the most innovative and productive, a point that sometimes gets lost in the general anxiety over China's rise.

Standards, Patents, Revenue

The focal points for this new technological competition are investment, innovation, intellectual property creation, defining standards, and patents. These have been "politicized," with some governments using investments, non-tariff trade barriers, and (in China) espionage to build national champions and hamper foreign competitors.

Standards describe performance requirements and technologies that will define 5G networks. They outline how the technology should work and set levels of performance and compatibility among technologies made by different companies. 5G will require hundreds of standards to be developed. In the context of 5G and its implications for espionage and innovation, standards have become a national security issue.

Defining global 5G standards will produce immense economic advantage. 5G standards are developed by international groups. The most important group is 3GPP (3rd Generation Partnership Project), but the ITU and 5GPPP also play important roles. These groups use open processes where companies and government agencies involved in telecommunications can participate.

China has politicized the standards-making process. Beijing expects Chinese companies to vote for Chinese standards whether or not they are the best. When Lenovo, a leading Chinese IT company, voted for a proposed standard from Qualcomm in 3GPP instead of one proposed by Huawei, it faced intense criticism in China.

In June 2018, 3GPP announced the first tranche of agreed 5G standards. Chinese companies are attempting to dominate standards development (to mandate the use of Chinese technologies), but in the June 2018 agreement, collaboration among Western companies ultimately determined the outcomes in the standards-making process. China "lost" the first rounds of the standards battle, in that 3GPP remains an international process not dominated by China that selects standards on the basis of quality and not national origin. But China will have more opportunities to try to capture 5G standards.

Patents implement standards. Patents provide ownership of the intellectual property required to make or use a technology based on a standard and create a revenue stream

(through licensing). For 5G, this revenue stream will be measured in the billions of dollars. The companies that patent technologies that meet 5G standards will gain larger shares of revenue and have an important advantage in further innovation.

Maintaining Technological Leadership

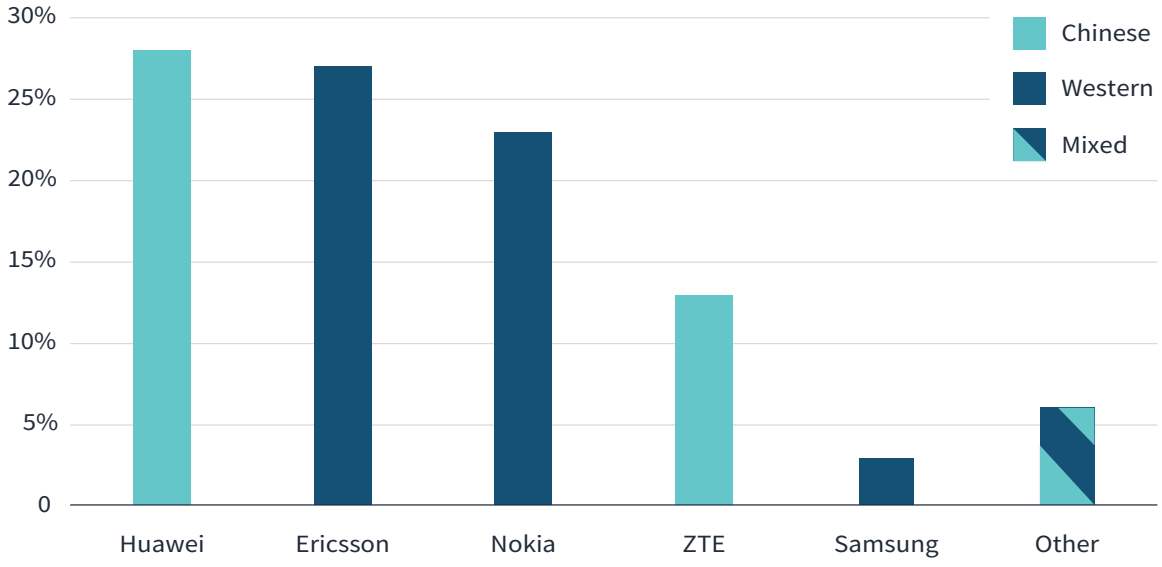
American companies are global leaders in 4G technology, helped to set the standards, and own many of the patents needed to build 4G equipment and networks. American technology is essential for 4G mobile telecommunications and an important source of income and exports.

Partially in reaction to this American success, 5G is a focus of intense international competition over standards and patents. Chinese officials and executives already complain about their dependence on U.S. technology. Huawei, for example, has research programs to develop alternatives to American suppliers. When the United States imposed sanctions on Chinese telecom manufacturer ZTE, crippling the company by denying it U.S. technology, China accelerated efforts to develop its own 5G semiconductor industry.

Despite this, American companies retain a leading market share for most advanced component 5G technologies. Only one of the major network manufacturers—Huawei—attempts to make the majority of components by itself, and even Huawei has a close partnership with many leading American tech companies.

5G Network Equipment Market Share

2017 Market Share for Mobile Network Equipment



Source: Stéphane Téral, "Global mobile infrastructure market down 14 percent from a year ago," HIS Markit, March 13, 2018, https://technology.ihs.com/600864/global-mobile-infrastructure-market-down-14-percent-from-a-year-ago.

5G networks depend on specialized semiconductors, and American companies dominate this market. Semiconductors are a strategic industry, essential to security and growth in the twenty-first century. Since the 1950s, the United States has been the leader in design and innovation in semiconductors, but the industry is now centered along the Pacific Rim with important participants in Japan, Taiwan, and Korea. China's policy is to displace U.S. companies, but even with immense investment and rampant espionage, American semiconductors remain indispensable for 5G. Chinese companies are strong in simpler microelectronics, but these pose a lower risk to security.

5G competition is part of a larger competition for influence and power based on different national approaches to investment and innovation. Innovation and new technologies have been a source of strength for the American economy for more than a century. New technologies gave the U.S. military advantage over its opponents. More importantly, technological innovation drives economic growth in ways that no other activity can match.

China has spent years trying to end its dependence on Western technology. It sees this as a way to restore China's global position and reduce the risk of American espionage. Building national champions in many different industry sectors (aerospace, telecom, IT, cars, railroads, solar energy) is an important part of China's state-directed economic policy and fits the narrative of China's "return to the center of the world's stage."

5G and Risk

Who makes 5G technologies, who sets the standards, and who controls the intellectual property (IP) can create risk and vulnerabilities for national security when a hostile power is involved. Making 5G would build a strong technological base capable of rapid innovation and having a secure supply chain closes off a dangerous area of risk, for both espionage and disruptions to critical infrastructures.

The state that builds 5G networks can gain immense espionage advantage if it has hostile intent. 5G leadership will provide the foundation for technological innovations that will drive military capability and economic growth. This is an economic contest with significant implications for security.

An easy way to envision this advantage is to imagine that the person who built your house decides to burgle it. They know the layout, the power system, the access points, may have kept a key, and perhaps even built in a way to gain surreptitious entry. Building and maintaining core network equipment provides a similar advantage.

Major telecom "backbone" equipment is usually directly connected to the manufacturer over a dedicated channel, reporting back on equipment status and receiving updates and software patches as needed, usually without the operator's knowledge. Equipment could be sold and installed in perfectly secure condition, and a month later, the manufacture could send a software update to gain access to information or to disrupt service. The operator and its customers would have no knowledge of this access and control.

The Chinese fear that this is what others do to them. The 2013 Snowden leaks exposed the degree of their vulnerability and helped accelerate the Chinese drive to achieve a dominant position in network and information technologies. Snowden's leaks may have

receded from American awareness, but they are still very real for China. But the Snowden leaks did not reveal U.S. government control of its technology companies nor a "special relationship" with them. NSA hacked communications and related equipment without any American manufacturers' knowledge or assistance. It does not subvert the supply chain. The same cannot be said for China.

In a normal environment, China as a supplier would not be a problem. Chinese companies would compete in the global market on the basis of their technology, like any other company, and chances are they would do quite well. Left to their own devices, these companies might prefer to slip Beijing's leash and operate like Western companies. This is not an option for them, however.

China is the most active espionage power when it comes to industrial espionage, theft of IP, and actions against groups or countries that the regime perceives as threatening. Its targets go well beyond the United States and include any country where China has interests and access. There are credible reports of China taking advantage of network equipment supplied by its companies for intelligence advantage that date back almost two decades.[3] In the last year, China has ignored agreements between China, the United States, and others not to engage in commercial espionage, and efforts to acquire American, European, and Asian technology have reached an unprecedented level.[4]

Two Chinese companies, Huawei and ZTE, are subject to control by the Chinese government. Huawei and ZTE have been heavily subsidized by the Chinese government both to obtain market dominance and to gain intelligence advantage. Huawei, after a murky start involving industrial espionage and extensive government financial support, makes competitive equipment that it can offer at discounted prices. Huawei's leadership has connections to the PLA and the Chinese intelligence service.

Huawei, and ZTE, are in no position to refuse a request from the Chinese government, and a good indicator of Chinese government intentions for foreign customers can be found in the treatment of its own population, which is subject to pervasive surveillance. There has been extensive reporting on the dangers of relying on Chinese telecommunications equipment. Data from countries that have purchased Chinese telecommunications equipment suggest that the espionage risk is real and cannot be mitigated effectively.

This is why five countries have put in place explicit or de facto bans on Huawei equipment. Two other countries are considering such bans. The United Kingdom, which bought Huawei technology over the objections of its security services, has had mixed results from the security center it created to screen Huawei software updates and services. Huawei's combination of good technology and subsidized prices is tempting for many countries, and it is the leading telecom equipment supplier in the world, but it comes with a significantly heightened risk of Chinese espionage.

---

3. U.S. Congress, 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*, 112 Cong., 2012, H. Rep. ii-60, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.
4. Nick McKenzie, Angus Grigg, and Chris Uhlmann, "China uses the cloud to step up spying on Australian business," *The Sydney Morning Herald*, November 20, 2018, https://www.smh.com.au/business/companies/china-uses-the-cloud-to-step-up-spying-on-australian-business-20181119-p50gze.html.

Several factors complicate this competition and increase risk. A discussion of the dangers of Chinese industrial policy lies outside the scope of this paper, but there is a high degree of unfair competition by China that has harmed other advanced economies. The current Chinese government is hostile to the United States and its allies. China has been clear in its intent to displace the United States globally and dislodge it from Asia.

Chinese industrial policies could slow the pace of global innovation. The market distorting effects of government-subsidized Chinese companies reduce market share and revenues for other Western firms. One result is that these firms are unable to afford the same investment in research and development. While China's innovation capabilities improved under Hu Jintao, they are not up to world standards in many areas, so shifting R&D investment away from Western firms will reduce the overall "output" of the global innovation system.

Reduced technological innovation in the United States creates national security risks since our military depends on its technological advantage rather than its size to obtain superiority. While the United States is poised to do well in expanding the "app economy"[5] with 5G and in developing industrial applications that use 5G to take advantage of connectivity, sensors, and automation, some U.S. policies on workforce, education, and research work against its market-driven innovation model.

Managing 5G Risk and Opportunity

The problem may seem enormous, but the United States can manage risk using two sets of policies. The first is to ensure that American companies continue to innovate and produce advanced technologies and face fair competition overseas. The second is to work with like-minded states to develop a common approach to the 5G security and supply problem.

A few years ago, no Western company was ready to challenge Huawei and ZTE, but this has changed. Western companies routinely outspend their Chinese competitors in 5G R&D and hold 10 times as many 5G patents. Chinese companies still depend on the Western companies for the most advanced 5G component technologies, such as radio frequency processing or FGPAs (a specialized semiconductor essential for software defined networks).[6] The issue is not who leads, but how to maintain that lead.

The United States cannot meet the 5G challenge on its own. When the United States has overcome against Chinese industrial policy in the past, it has been done in concert with U.S. allies. The United States will need a unified approach among like-minded companies and states who are willing to invest in 5G. Part of creating this approach may be to define voluntary agreements on security standards for secure 5G networks.

Another part will be to find ways to encourage undecided countries to spend on secure 5G. Since Huawei is subsidized, the Chinese government can give Huawei an edge in pricing. Secure equipment costs more. Determining how to persuade countries that they should pay a premium is one problem; determining how to securely connect and communicate over telecom networks in other countries using vulnerable equipment is another.

---

5. Mobile applications that provide a wide range of new internet-based services.
6. Field Programmable Gate Arrays.

The United States also needs to act to ensure that American companies do not face unfair obstacles from antitrust or patent infringement investigations undertaken by any country to obtain competitive advantage. Fair competition is essential for innovation because it incentivizes companies to build better products and offer better services.

The United States does not need to copy China's government-centric model for 5G (and for technology in general), but it does need to invest in research and adopt a comprehensive approach to combatting non-tariff barriers to trade. 5G leadership has to be part of a larger technology competition policy in the United States that builds the engineering and tech workforce and supports both private and public R&D. Government action can provide the public goods needed for American companies to flourish in the market.

In the twentieth century, what made a state powerful was the strength of its industries—steel, coal, automobiles, aircraft, and ships. These industries, and the ability to produce things in mass quantity, were the sources of industrial age power. The foundations of security and power are different today. The ability to create and use new technologies is the source of economic strength and military security. Technology, and the capacity to create new technologies, are the basis of information age power. 5G as the cornerstone of a new digital environment is the focal point for the new competition.

About the Author

James Andrew Lewis is a senior vice president at CSIS. Before joining CSIS, he worked at the Departments of State and Commerce as a Foreign Service officer and as a member of the Senior Executive Service. His government experience includes a broad range of political-military, negotiating, and intelligence assignments. He was an adviser to the U.S. Southern Command for Operation Just Cause, the U.S. Central Command for Operation Desert Shield, and the U.S. Central American Task Force. He led the U.S. delegation to the Wassenaar Arrangement Experts Group on advanced civilian and military technologies. He worked on presidential policies for arms transfers, on commercial space remote sensing, on policies to secure and commercialize the Internet, and on encryption and lawful access to communications. He was the Commerce Department lead for national security and espionage concerns related to high-technology trade with China.

Lewis was the rapporteur for the UN Group of Government Experts on Information Security for the successful 2010, 2013, and 2015 sessions. He has led long-running Track 1.5 discussions on cybersecurity with the China Institutes of Contemporary International Relations. He has served on several Federal Advisory Committees, including as chair of the Committee on Commercial Remote Sensing, as well as member of the Committees on Spectrum Management and International Communications Policy and the State Department's Advisory Committee on International Communications and Information Policy, and as an adviser on the security implications of foreign investment in the United States. Lewis has authored numerous publications since coming to CSIS on a broad array of topics, including innovation, space, information technology, globalization, deterrence, and surveillance. He was the director for CSIS's Commission on Cybersecurity for the 44th Presidency and is an internationally recognized expert on cybersecurity who is frequently quoted in the media. He has testified numerous times before Congress. Lewis's current research examines the effect of technology on warfare and how the internet has changed politics. He received his PhD from the University of Chicago.

Appendix A

The Complex, Interconnected 5G Supply Chain

The outer edge of a 5G network begins with devices**,** where phones, IoT devices, autonomous vehicles, and other equipment connect to a 5G network to send and receive data. An enormous variety of manufacturers will be responsible for creating 5G devices, ranging from producers of smartphones to automobiles. Common features of all 5G devices, however, will include 5G-compatible modems for translating data into a form that can be sent via radio waves; 5G radio frequency front end systems (RFFEs) for processing signals transmitted over 5G frequencies; and 5G-compatible antennas for sending and receiving those radio signals.

5G networks are composed of cell sites (or base stations) that provide network coverage to devices. These base stations now use cell towers that can provide coverage over a few miles. 5G uses higher frequency radio waves that have shorter effective ranges than before. Network equipment providers have developed a new generation of "small cells" that will be the first link for most 5G devices trying to connect to telecoms networks.

Mobile networks require antenna units to capture signals from user devices as well as a host of electrical processing components to clean, amplify, modulate, and route incoming and outgoing RF signals. With 4G, this process was done by "baseband processing units" (BBUs) co-located with the cell towers. For 5G networks, however, network processing activities are predicted to move away from cell site towards centralized, cloud-based BBUs.

Significant components include antenna arrays and data converters **(**semiconductors that convert analog radio signals into digital values). China has attempted to build its own data converters without success. Power transistors for low noise and power amplifiers are another critical component, serving to amplify the signal received by the small cell's antenna. Small cells also require "field programmable gate arrays" (FPGAs) to connect baseband units and the transport network. The only major suppliers of FPGAs are American. Many of these components can be combined into a single "chipset." Producers of small cell chipsets include Samsung, Ericsson, and Huawei, as well as external chipset manufacturers like Intel, Qualcomm, Cavium, and NXP. U.S., European, and Japanese firms are dominant in the provision of components that go into these chipsets.

The signals travel through a transport network—known as the backhaul—before reaching

the telecom's core network. The backhaul comprises routers, switches, fiber-optic cables, optical transceivers, and microwave transmission equipment. There are many different ways to accomplish backhaul networking, and there are a broad range of offerings from U.S., European, Chinese, and other Asian suppliers. After being sent via the backhaul transport network, the signals arrive at the carrier's core network, which is responsible for providing services to customers and routing traffic to other devices or networks.

For 4G LTE, telecoms' core networks are based on the Evolved Packet Core architecture. For 5G, telecom companies will eventually have to change to new hardware and software infrastructures defined by the emerging standards for 5G Core (5GC). Currently, the market leaders are Ericsson and Huawei (with 60 percent of the market), followed by Nokia, Cisco, and ZTE.

The router and switch market is currently led by Cisco, Huawei, Nokia, and Juniper, which together account for 90 percent of the market share. Cisco, Juniper, and Nokia have all announced plans to deploy 5G routers for next generation core networks. Huawei and Samsung have also announced 5G compatible edge routers for fixed 5G customers. Other routing market participants include Ericsson, HPE, Brocade, Coriant, Fujitsu, NEC, and ZTE.[7] Routers and switches depend on network processors. In 2016, Intel and Broadcom led the market in network silicon, with other participants including HiSilicon (owned by Huawei), Qualcomm, TI, Global Foundry, Xilinx, Cavium, Cisco, Ericsson, and Marvell. Manufacturing for network silicon primarily takes place in Taiwan (48.67 percent in 2016) and China (17.11 percent).

Ethernet switches are the most common type of network switches, and Cisco has 50 percent of the market, followed by Huawei (10 percent), Arista (6.6 percent), HPE (6.5 percent), and Juniper (3.8 percent). However, the market for ethernet switches may be overtaken by "white box" routers—generic, low-cost hardware using cloud-based software. Many tech companies already use white box switches in their data centers, and Amazon is rumored to be considering selling its own white box switches to outside customers.

Actions by the U.S. government have effectively ensured that no U.S. company will rely on Chinese equipment manufacturers for their 5G infrastructure. However, the global 5G equipment supply chain is extraordinarily complex, and interlinkages with Chinese suppliers are inescapable. Both Nokia and Ericsson have established joint ventures with Chinese-based subsidiaries, joint-venture partners, and Chinese companies (many with links to the government) to develop and manufacture 5G equipment and compete for network deployment contracts with Chinese telecoms. Many American manufacturers have design and manufacturing centers in China or are partnered with Chinese firms who provide components or software for their 5G equipment. The same is true for Chinese companies: Huawei has worked with over 270 international partners to develop its 5G applications.

7. Ray Sharma, "Juniper, Cisco, Huawei and Nokia Form Top Tier of Service Provider Router and CES, says IHS," The Fast Mode, https://www.thefastmode.com/technology-and-solution-trends/11896-juniper-cisco-huawei-and-nokia-form-top-tier-of-service-provider-router-and-ces-says-ihs.

Appendix B
Selected Publications on Chinese Espionage

1. Adam Segal, "An Update on U.S.-China Cybersecurity Relations," Council on Foreign Relations, November 17, 2017, https://www.cfr.org/blog/update-us-china-cybersecurity-relations.

2. Jon R. Lindsay et al., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford University Press, April 2015).

3. James A. Lewis, "China's Economic Espionage: Why It Worked in the Past But It Won't in the Future," *Foreign Affairs*, November 13, 2012, https://www.foreignaffairs.com/articles/china/2012-11-13/chinas-economic-espionage.

4. Gabriel Dominguez, "Chinese cyber-attacks 'not a parallel with NSA spying'," Deutsche Welle, Interview with James A. Lewis, May 21, 2014, https://www.dw.com/en/chinese-cyber-attacks-not-a-parallel-with-nsa-spying/a-17651036.

5. Derek Scissors and Steven Bucci, *China Cyber Threat: Huawei and American Policy Toward Chinese Companies* (Washington, DC: The Heritage Foundation, October 2012).

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

7. James A. Lewis, "Cyber Security and US-China Relations," China-US Focus, July 6, 2011, https://www.chinausfocus.com/peace-security/cyber-security-and-us-china-relations.

8. James A. Lewis, "Cyber Tensions: Putting the Indictments for Cyber Espionage in Context," American Chamber of Commerce, Shanghai, July 2014, https://www.csis.org/blogs/technology-policy-blog/cyber-tensions-putting-indictments-cyber-espionage-context.

9. James A. Lewis, "Economic Warfare and Cyberspace," *China's cyberpower: International and domestic priorities Australian,* Strategic Policy Institute, November 2014, http://sdsc.bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-03/sr74_china_cyberpower.pdf.

10. Tobias Freakin, *Enter the Cyber Dragon Understanding Chinese intelligence agencies' cyber capabilities* (Australian Strategic Policy Institute, June 2013), https://www.aspi.org.au/report/special-report-enter-cyber-dragon-understanding-chinese-intelligence-agencies-cyber.

11. James A. Lewis, "Expanding International Norms after the U.S.-China Cyber Theft Agreement," World Political Review, January 13, 2016, https://www.worldpoliticsreview.com/articles/17653/expanding-international-norms-after-the-u-s-china-cybertheft-agreement.

12. James A. Lewis, "Five Myths About Chinese Hackers," *Washington Post*, March 22, 2013, https://www.washingtonpost.com/opinions/five-myths-about-chinese-hackers/2013/03/22/4aa07a7e-7f95-11e2-8074-b26a871b165a_story.html?utm_term=.5a61d8c5238f.

13. James A. Lewis, "How the Internet Became a Focal Point for Espionage," Fletcher Forum of World Affairs, August 6, 2016, http://www.fletcherforum.org/home/2016/9/6/how-the-internet-became-a-focal-point-for-espionage.

14. Danielle Cave et al., *Huawei and Australia's 5G Network: Views from ASPI* (Australian Strategic Policy Institute, October 2018), https://www.aspi.org.au/report/huawei-and-australias-5g-network.

15. Richard McGregor, "Huawei Has Ended a National Illusion," *Financial Review*, June 22, 2018, https://www.afr.com/opinion/columnists/huawei-has-ended-a-national-illusion-20180622-h11q3y.

16. Danielle Cave, "Huawei highlights China's expansion dilemma: espionage or profit?" Australian Strategic Policy Institute, June 15, 2018, https://www.aspistrategist.org.au/huawei-highlights-chinas-expansion-dilemma-espionage-or-profit/.

17. U.S. Congress, 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*, 112 Cong., 2012, H. Rep. ii-60, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf. Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman, March 7, 2012, https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-066.pdf.

18. Alex Joske, "Picking flowers, making honey: The Chinese military's collaboration with foreign universities," Australian Strategic Policy Institute Policy Brief, no. 10, October 2018, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2018-10/Picking%20flowers%2C%20making%20honey_0.pdf?H5sGNaWXqMgTG_2F2yZTQwDw6OyNfH.u.

19. James A. Lewis, "Put China's IP Theft in a Larger Context," *Commentary*, CSIS, August 15, 2017, https://www.csis.org/analysis/put-chinas-intellectual-property-theft-larger-context.

20. Adam Segal, "The code not taken: China, the United States, and the future of cyber espionage," *Bulletin of the Atomic Scientists* 69, no. 5 (October 2013), https://www.tandfonline.com/doi/abs/10.1177/0096340213501344.

21. James A. Lewis, "There Is More to the Trade War than Trade," *Commentary*, CSIS, April 6, 2018, https://www.csis.org/analysis/there-more-trade-war-trade.

22. James A. Lewis, *U.S. Policy on Economic Espionage* (Washington, DC: CSIS, December 2011), https://www.csis.org/analysis/us-policy-economic-espionage.

23. James A. Lewis, "Understanding ANT, Big Data, and CFIUS," *Commentary*, CSIS, January 9, 2018, https://www.csis.org/analysis/understanding-ant-big-data-and-cfius.

24. James A. Lewis, "We Wuz Robbed," *Commentary*, CSIS, July 2, 2015, https://www.csis.org/analysis/we-wuz-robbed.

25. James A. Lewis, *ZTE, the Telecom Wars, and Cyber Spies* (Washington, DC: CSIS, June 2018), https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**