Open Future

The Way Forward on 5G

Martijn Rasser
Ainikki Riikonen

Center for a
New American
Security

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Acknowledgements

Thank you very much, Paul Scharre and Loren DeJonge Schulman, for your valuable feedback and suggestions on the draft. We are grateful for the insight of the attendees of the workshops convened through the "Securing Our 5G Future" project at the Center for a New American Security (CNAS) in 2019 and 2020. The input of industry experts on the technical aspects of this report was invaluable.

Melody Cook, you outdid yourself with fantastic designs for the cover and the graphics. Thank you, Maura McCarthy, for your role in the review and production of this report. Finally, thank you to Monika Bochert for your assistance in reviewing and finalizing the report. Any errors that remain are the responsibility of the authors alone.

About the Authors

Martijn Rasser is a Senior Fellow in the Technology and National Security Program at CNAS. Mr. Rasser served as a senior intelligence officer and analyst at the Central Intelligence Agency. Upon leaving government service, Mr. Rasser was Chief of Staff at Muddy Waters Capital, an investment research firm. More recently, he was Director of Analysis at Kyndi, a venture-backed artificial intelligence (AI) start-up. Mr. Rasser received his BA in anthropology from Bates College and his MA in security studies from Georgetown University.

Ainikki Riikonen is a Research Assistant for the Technology and National Security Program at CNAS. Before joining CNAS, Ms. Riikonen worked at the Department of Defense's Near East South Asia Center for Strategic Studies, where she supported security cooperation programs on regional security issues for participants from North Africa, the Middle East, Central Asia, and South Asia. Ms. Riikonen holds a degree in international relations from the University of St Andrews and is currently studying for an MA in security studies at Georgetown University.

About This Report

This report is produced as part of the CNAS project "Securing Our 5G Future," which explores the opportunities and challenges of 5G in a world of highly globalized and competitive innovation. This project is made possible through support from AT&T, Cisco, and Qualcomm, and other general funding, which helped sponsor a series of workshops in the fall of 2019 and winter of 2020 that contributed to informing this report. The workshops included a diverse set of stakeholders from the policy community, industry, and academia. The authors also thank NEC Corporation for their participation in these workshops.

Prior Report in This Series

"Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy" by Elsa B. Kania (November 2019)

This report and other analysis and commentary are available online at https://www.cnas.org/5G.

Table of Contents

Executive Summary

Communication networks are the central nervous system of the 21st century economy. The fifth generation of wireless—5G—will be essential to and inseparable from all we do. In many ways, we are already there. What for most was an abstract concept became all too real during the COVID-19 crisis.

The coronavirus pandemic has underscored the critical importance of communication networks: They are integral to our daily lives and our ability to function economically and as a society. Shutdowns of offices, schools, and stores have meant turning to apps to work, learn, and buy. Frontline medical workers and vaccine researchers have consulted colleagues via teleconference to get the latest insight and advice on combating the virus. Being connected means resilience, coping, surviving.

Getting 5G right is all the more urgent. Next-generation 5G networks will enable telemedicine, self-driving cars, and a proliferation of Internet of Things devices to fuel the future digital economy. Secure, reliable 5G networks will be essential elements of national infrastructure. Policymakers in Australia, Japan, and Vietnam understood this early on and took decisive action to secure their 5G networks. U.S. officials, slower out of the gates, are now the loudest voice on the risks of having equipment from untrusted vendors in 5G networks. The spotlight is brightest on the risks that Huawei poses to national security, including the threat of espionage or disruption. Given the Chinese Communist Party's ability to exercise control over Huawei, there is justifiable concern over data integrity on networks that deploy Huawei equipment. More serious is the potential to use 5G equipment as a vector to cripple critical infrastructure. Such risk is not only about communications—5G will be the backbone of controls needed for power grids, water supplies, and transportation infrastructure. Despite this, the United States has had only limited success convincing its allies to join it in banning Huawei.

The United States has the opportunity to regain momentum by taking a fresh approach to 5G in the aftermath of the pandemic. In addition to the broader appreciation for the criticality of reliable communication networks, Beijing's coronavirus cover-up and clunky attempts at soft power have hardened public opinion toward China around the world. The economic fallout of the pandemic will likely slow 5G deployments globally, curtailing the urgency with which many operators approached the issue. At the same time, the first commercial projects centered on technological alternatives to the predominant 5G approach are being deployed. This confluence of events presents the United States and like-minded countries an opening to promote an alternative approach that could lead to a paradigm shift in the industry: wireless infrastructure built on a modular architecture with open interfaces.

A modular architecture allows an operator to choose multiple vendors for a range of offerings, rather than being locked in with a single large integrated vendor. Open interfaces—the ability of equipment from any vendor to work with that of another—make that possible. Such a shift means upending the industry status quo that is dominated by four telecommunications equipment providers: China's Huawei, Finland's Nokia, Sweden's Ericsson, and South Korea's Samsung. Whereas other proposed responses to the Huawei dilemma and the problematic current state of competition in the telecommunications industry fiddle at the margins, switching to an industry centered on open interfaces would change the game altogether.

A restructured industry based on open interfaces would directly address the prevailing concerns over untrusted vendors such as Huawei and the broader inefficiencies of the industry. There are distinct advantages to be gained in security and interoperability, supply chain resiliency, probable cost savings, and the opportunity to stimulate much-needed competition in the sector. Taken together, these advantages do much to blunt Beijing's industrial policies that have enabled Huawei's predatory anti-competitive practices.

There are three distinct but related lines of effort the U.S. executive and legislative branches should take to promote open standards for 5G as a viable alternative to the status quo, and as a foundation for a secure 5G future:

1. **Signal U.S. government (congressional and executive) support for modular 5G equipment with open interfaces.**
   - Encourage industry-led efforts to promote telecommunications infrastructure that is modular and based on open interfaces with congressional messaging, such as a nonbinding resolution.
   - Publicly highlight the technical merits and the economic opportunities of open interface technologies with a series of expert-led congressional hearings.
   - Condition the subsidy of telecommunication deployments with the use of U.S. modular products and open interfaces.
   - Make modular products with open interfaces the cornerstone of an updated White House national strategy for 5G.
2. **Promote development and deployment of modular telecommunications infrastructure based on open interfaces.**
   - Provide tax breaks and other incentives for the manufacture of equipment and the development of software in the United States.
   - Increase the research and development (R&D) incentives for relevant technologies to at least $2 billion over 10 years, from the $750 million over 10 years proposed in the USA Telecommunications Act.
   - Promote adoption of open modular systems in rural areas to address the digital divide.
   - Use the purchasing power of the U.S. government to stimulate open modular architecture development and deployment.
3. **Collaborate with allies and partners.**
   - Pursue joint R&D with like-minded countries to build a multilateral technology base that promotes the development and deployment of open interface 5G equipment.
   - Initiate multilateral 5G policies to build a viable environment for a restructured telecommunications sector.

Introduction

5G will enable a transformation of global infrastructure. Transcending the boundaries of our physical and digital worlds, 5G technologies will serve as a conduit that transmits the firing synapses of our everyday and our essential: an adjustment of the thermostat, a check-in with a personal virtual assistant, automated grocery purchases delivered by an autonomous van, power plants supplying electricity to cities and towns, purification of our drinking water, brain surgery by a doctor a thousand miles away, a call for air support and reinforcements on a distant battlefield.

Confidence in the security, resilience, and robustness of 5G networks is paramount. The U.S. government has concluded that the presence of untrusted vendors on these networks poses unacceptable risk and is placing pressure on allies and partners to join it in banning Chinese telecommunications firm Huawei from their 5G networks. This effort has failed, however, to gain traction in the capitals of many allied countries. Part of the reason is that U.S. government messaging on China and 5G has been inconsistent, and sometimes outright contradictory. Another important factor is hesitance in many countries to endanger important economic ties to China. China is a major trade partner for many European countries; at the same time, many also receive considerable Chinese foreign direct investment.[1] In this light, a limited deployment of Huawei kit is rationalized as a risk to be accepted.

The broader problem is that the telecommunications equipment industry of today is an oligopoly of proprietary equipment vendors increasingly dominated by Huawei. The dearth of suppliers for essential telecommunications equipment poses supply chain risks. Beijing's industrial policies, which often enable Huawei to undercut the competition on price, worsen this situation.

There is an opportunity to address this situation head-on with emerging technology alternatives. The United States can help to forge a new, more secure 5G future by embracing and promoting a shift to telecommunications infrastructure based on open interfaces. At stake is renewed opportunity for American technology leadership, greater competitiveness, better economic security for the world's tech-leading democracies, greater resiliency to supply chain disruptions, and improved ability to protect the privacy and data of its citizens.

This report comprises eight sections. They explain the basic concepts and technologies behind 5G and open interfaces, make the case for why the 5G status quo is risky, and weigh the merits of different ways to address this status quo. The report surveys current deployments of telecommunications infrastructure based on modular equipment using open interfaces and closes with actionable policy recommendations that the United States should take to help usher in a new era in telecommunications. An analysis of the common arguments against a ban on Huawei is included in an appendix.

5G, Core-Edge, and Open Interfaces: A Primer

A brief overview of important technical concepts is necessary to inform the reader's understanding of the assessments and recommendations in this report. These concern the basic components of a 5G network, the distinction between the core and edges of those networks, and what is meant by "modular with open interfaces."

5G refers to the fifth generation of wireless telecommunications networks. As depicted in Figure 1, these networks consist of two functional areas: the radio access network (RAN) and the core network (5GC).

- *Radio access network:* The RAN is "the part of a telecommunications system that connects individual wireless devices to other parts of a network through radio connections."[2] While the interfaces to do so are open and standardized, the equipment needed—base stations, radio amplifiers, management systems—are closed (not interoperable with other vendors) and do not completely abide by these standards.[3] RAN equipment is vendor-proprietary, and the global market is dominated by just a handful of manufacturers: Huawei, Nokia, Ericsson, and to a lesser extent Samsung and ZTE. In 4G, the fourth generation of wireless telecommunications, this part of the network is called "the edge."

- *Core network:* The core network forms the bridge between the RAN and the internet, the wired telephone system, and internet protocol-based (IP-based) services.[4] The core network controls RAN functions on the entire network: All data (e.g., voice, video, text) on a network traverse the core, and it determines how those data are routed.

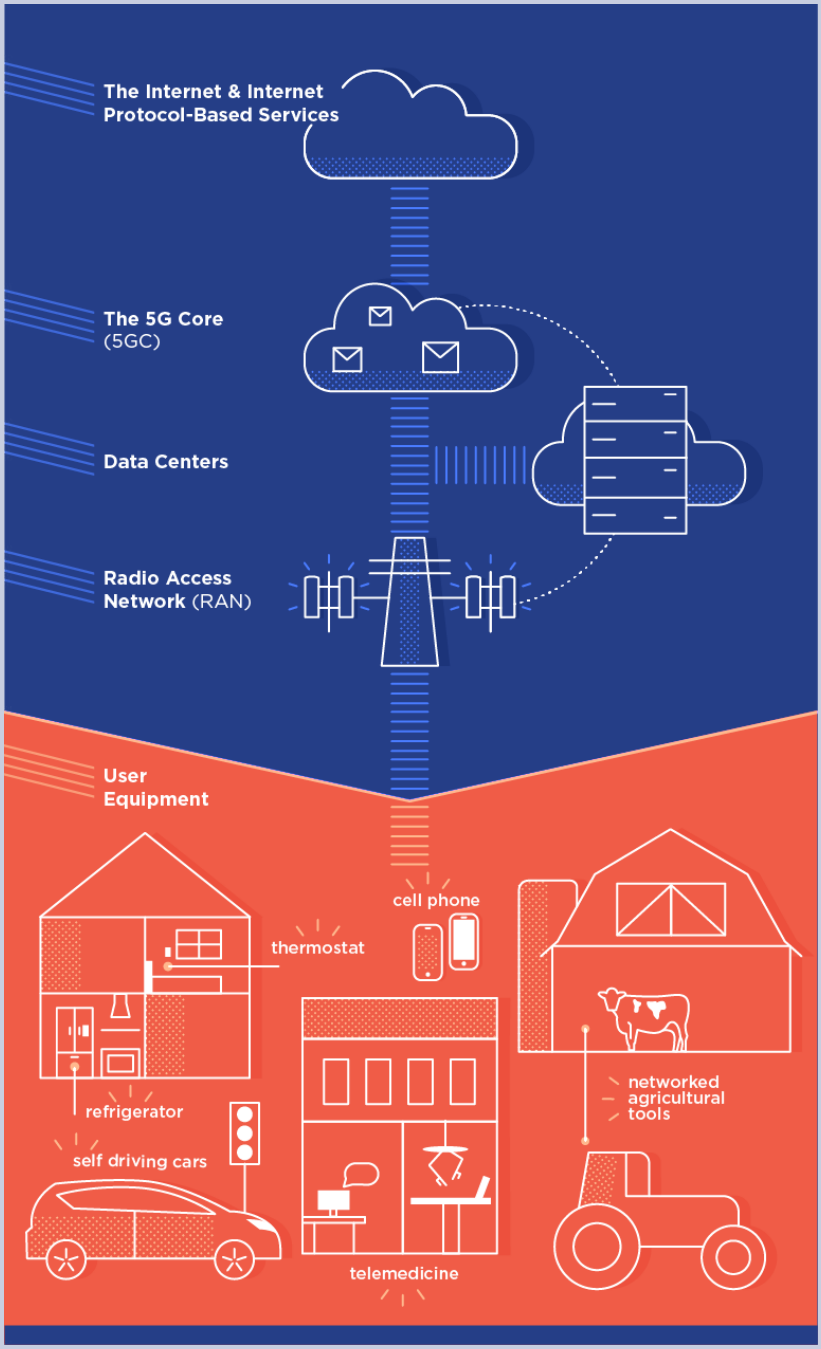
The core-edge distinction is the demarcation between the core network and the RAN. In 4G networks there is a clear line between their functionality. This makes it possible, with appropriate risk mitigation measures, to operate equipment from less-trusted vendors on the edge while still protecting the sensitive and critical functions of the core. This is a suitable approach for geographical areas where the potential for permanent loss of connectivity from sabotage and the potential for eavesdropping are acceptable. A secure core-edge separation can help mitigate the spread of a cyberattack in the RAN so that it does not extend to geographical areas served by equipment from trusted vendors. The United Kingdom took this approach for its 4G networks.[5]

Specific attributes of how 5G networks will function blur the core-edge distinction.[6] Much of the core's traditional functions will increasingly be pushed to the edge to reduce latency: speeding up communication to enable new functionality such as autonomous vehicles and telemedicine, where a millisecond lag can be a matter of life or death. One of the key arguments raised by the governments of Australia and the United States is that a complete ban of untrusted vendors on 5G networks is needed because the core-edge risk mitigation tactics for 4G networks simply will not work on 5G networks as the core and edge in essence are intermingled.

"Modular with open interfaces" refers to a system composed of subcomponents that connect and communicate with one another using published protocols and interface specifications (see Figure 2). The premise of the resulting open architecture is that vendors can focus on parts of the RAN, and not have to provide a complete solution to be a viable vendor as is the case today. Some of the required software and hardware could also be open source to ease integration and certification, while improving security. There are three concepts to remember:

- *Interoperability:* Each RAN hardware manufacturer developed its own solution to the complexities of real-time digitizing of radio signals. Because vendors take different approaches, their equipment is not readily interoperable with that of another. One reason is that the manufacturers do not want to disclose their designs to each other—a lack of visibility into the inner workings that creates a "black box." Another is that proprietary solutions facilitate "vendor lock-in." Once a vendor supplies noninteroperable RAN equipment, it becomes the sole source for servicing, replacement parts, software updates, and upgrades. Furthermore, it becomes difficult and expensive for an operator to have other vendors on the same RAN. Switching vendors to upgrade a network to the next generation of wireless technology in most cases would require a complex overhaul to be able to offer 4G and 5G services at the same time. This means that once a vendor wins a customer, it will derive significant recurrent revenues for the next 10 years and has a good chance to retain that customer when equipment upgrades are needed.

Figure 1: Main Components of a 5G Network



The internet and internet protocol-based (IP-based) services—Internet protocol-based services direct data traffic according to rules called the internet protocol suite, or TCP/IP. Data traffic is divided into small units called packets that are like envelopes; they contain a header, written in internet protocol language that indicates how and where the packet will travel, and the data payload. The internet, one type of IP-based service, is a network of networks that operates on TCP/IP.

5G core (5GC)—The "core" manages data transmission across the network and to other networks and services. In recent generations, the core transitioned to "packet-switched" designs rather than "circuit-switched," where the network created dedicated physical connections between users. In 5GC, the core is "cloud native," which further decreases the use of specialized physical hardware; it is a virtual system that runs on distributed data centers. The cloud architecture increases the flexibility of the system and paves the way for innovation in network management by expanding the capacity for software-driven network functions.

Data centers—Central data centers house networking and computing equipment to store, distribute, and provide access to large amounts of data. Most data centers comprise cloud computing resources, providing access to many internet users. Edge data centers are smaller facilities with the same function. They are located as close as possible to users and user equipment to reduce latency.

Radio access network (RAN)—A combination of remote radio units, which send and receive signals to user equipment such as phones, and baseband units that backhaul data to the 5GC and manage the radio units. In 5G networks, one baseband unit can manage multiple radio units. Pools of baseband units have the potential to deliver cloud-based RAN.

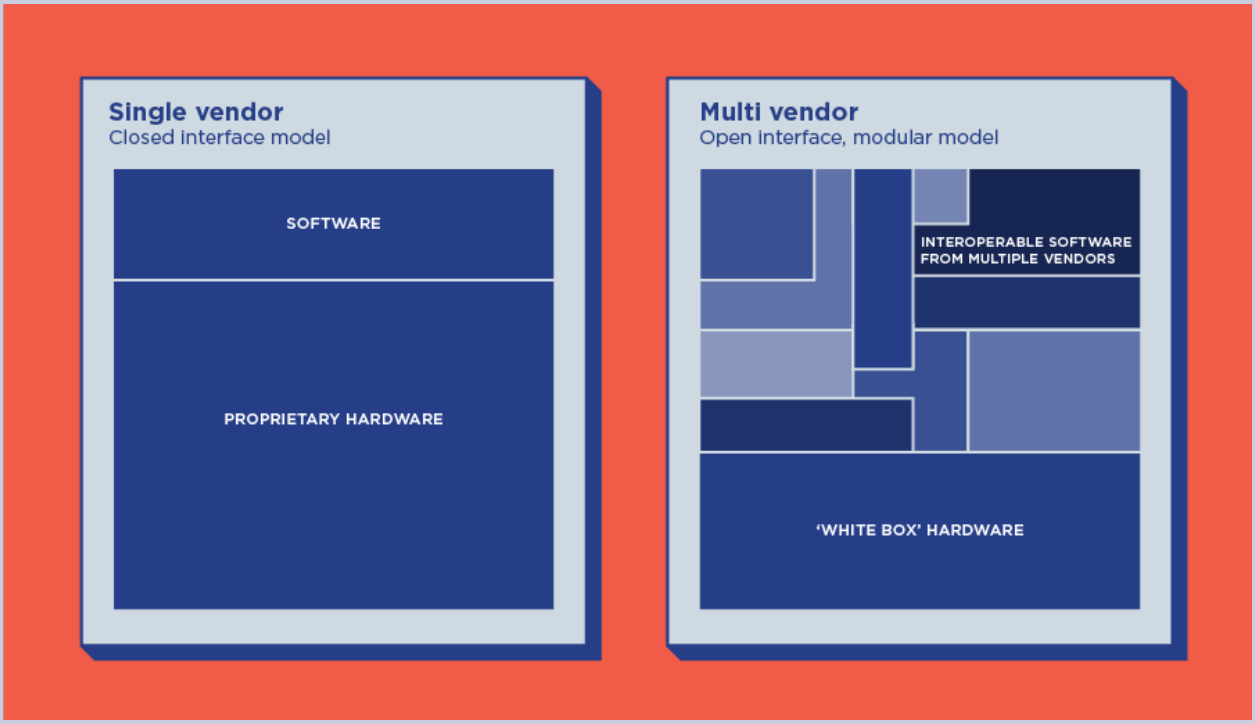
User equipment—Devices such as phones or the Internet of Things (IoT) that connect via 5G networks. The high throughput and low latency of 5G will empower a high volume of user equipment with complex data needs. Examples include self-driving cars, networked agricultural tools and other industrial IoT, and telemedicine where doctors can remotely operate on patients in faraway places in near-real time.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

- *Open architecture:* A solution to this "black box" proprietary hardware issue is to build telecommunication networks—network architecture—based on open interfaces, which allow for interoperability across multiple vendors. Under an open architecture principle, the benefits of a vertically integrated product are lessened, and the vendor lock-in business model is significantly weakened—in particular as more vendors emerge that offer substitute parts. With this approach, the existing technical and economic barriers of entry are greatly reduced, opening up the opportunity for new companies to enter the market.

- *Network virtualization:* The ability of software to simulate the functions of hardware appliances such as switches, routers, and firewalls. In doing so, it is feasible to disaggregate hardware from software and reduce the amount of specialized hardware needed to create a telecommunications network. Network virtualization technology enables new entrants with small research and development (R&D) budgets by allowing them to leverage preexisting cutting-edge IT software and hardware. Advocates for open, virtualized networks point out that hardware then can become less expensive, generic commodities ("white box"), not the proprietary vendor-specific items they are today. In the United States, Verizon and AT&T are building 5G networks increasingly incorporating virtualization.[7]

Figure 2: A Shift to Open Interfaces



The current model (left) is based on a single vendor supplying RAN "black box" hardware with some network virtualization via software. An open interfaces approach (right) enables a modular architecture, with multiple vendors providing expanded software solutions that run on off-the-shelf "white box" hardware such as servers and network switches.

The 5G Status Quo Poses Risks

The promise of 5G is alluring. New capabilities—autonomous vehicles, telemedicine, a true Internet of Things that connects millions of devices, machines, objects, and people—enabled by much greater bandwidth at higher speeds and lower latency than is possible today are expected to transform the U.S. economy and society. 5G also has important national security applications, such as improved military communication and situational awareness. There are also likely to be innovations and use cases we have yet to conceive of. 5G means advances across a spectrum of industries, with novel foundational technology serving as the backbone for critical infrastructure. A common refrain is that 5G could be one of the most consequential technological innovations in human history, ushering in a fourth industrial revolution in a few years' time.[8]

5G networks will form the backbone of critical infrastructure such as power grids. (Andy A. Widmer/EyeEm)

While such exuberance should be tempered by the fact that this transformation will almost certainly need longer to take hold, the fact remains that 5G will be the backbone of the global internet economy.[9] It is essential, then, that 5G networks are secure, reliable, robust, and resilient.

There is ample reason to be worried this will not be the case. U.S. officials have significant concerns about the integrity of global 5G networks. These concerns are valid due to the prominent role that Huawei—a large Chinese telecommunications firm—plays in the international telecommunications sector and the nascent 5G rollout. Huawei seeks to capitalize on its outsize market share (29 percent) for telecom equipment by quickly securing new 5G contracts around the world.[10]

The concerns over Huawei are not new—publicly known examples date at least as far back as 2001—nor are they exclusively American ones.[11] The governments of Australia and the Czech Republic have been early leaders in articulating the risks associated with having Huawei equipment on a country's 5G networks.[12] A risk assessment published by the European Union in October 2019 on the cybersecurity of 5G networks makes note of the same vulnerabilities and risk scenarios that U.S. officials have cited, although the EU report does not refer to China or Huawei by name.[13]

There are three broad categories of concern associated with 5G generally and Huawei specifically: security, critical infrastructure integrity, and supply chain diversity. Security concerns primarily include cybersecurity and espionage. Poor software development poses undue risk and Huawei is shown to have exceedingly insecure practices.[14] This unease is especially acute with 5G because it will be fully intertwined with the digital economy, with potential life or death consequences.

There are also traditional espionage concerns. While many actors could use 5G networks for spying, Huawei's murky relationship with the Chinese Communist Party, China's intelligence law that requires companies to cooperate with the country's security agencies, and the lack of legal recourse to resist doing Beijing's bidding make Huawei an undesirable partner.[15]

More serious than safeguarding data is the potential for critical infrastructure disruptions. 5G will be the backbone of communications needed for power grids, water supplies, and transportation infrastructure. A cyberattack here would be crippling.[16] Catastrophic effects could also result from less dramatic action, such as a "delay" in providing essential maintenance or supplying needed replacement equipment for 5G networks. Beijing has threatened to withhold critical medical equipment and engaged in economic coercion against multiple countries during the pandemic in response to actions that displeased it.[17] Chinese leaders have also threatened economic pain for countries contemplating limiting or banning Huawei from their 5G networks.[18] It is no stretch to consider Beijing's willingness to hold foreign critical infrastructure at risk to achieve its geopolitical goals.

Finally, the supply chain for 5G kit is worryingly limited because the industry is an entrenched oligopoly. There are only two major non-Chinese suppliers of RAN equipment: Nokia of Finland and Ericsson of Sweden. Samsung of South Korea is a distant third. Given the importance of RAN to future critical digital infrastructure, the industry is too consolidated to ensure sufficient supply chain diversity and security.

Huawei has a sprawling research and development (R&D) campus in Dongguan, China. Together with Nokia, Ericsson, and Samsung, the company dominates the global market for radio access network equipment. (Kevin Frayer/Getty Images)

What makes the supply chain issue particularly vexing is that Chinese industrial policy all but ensures the oligopoly will persist, and likely worsen, as Nokia, Ericsson, and Samsung face growing hurdles to compete. Beijing supplied Huawei with as much as $75 billion in subsidies, enabling the company to spend billions on R&D it could otherwise not afford and undercut the competition on price to gain and protect market share.[19] Huawei has also held out on paying licensing fees to Western technology companies, depriving firms of significant revenue streams.[20]

The 5G Dilemma: Potential Solutions

Much ink has been spilled outlining solutions to the 5G dilemma. Leaders in government and industry, pundits, and analysts have proposed an array of options ranging from state intervention to industry-driven efforts to revamp 5G networks. Most proposals focus on tackling the issue in the current paradigm. The most promising one—open 5G network architecture—is hobbled by what has been to date a lack of essential top-down governmental support.

CREATE A NATIONAL 5G CHAMPION

One of the more obvious reactions to the 5G dilemma is to fight fire with fire. Broadly, this approach would entail creating a new U.S. large infrastructure vendor akin to what Motorola was in the 1980s and 1990s, when the company was a dominant force in telecommunications equipment and semiconductors. Trump administration officials have tried to persuade U.S. firms Oracle and Cisco to reenter the RAN equipment market, with no success.[21] In an ironic twist, Huawei even offered to license its intellectual property to create such a national champion.[22]

Why does the United States not have its own Huawei? Much of it has to do with the industry consolidation of the 1990s and early 2000s. Foreign firms acquired U.S. infrastructure vendors such as Lucent and Motorola. Simply stated, the United States let market forces work rather than pursue industrial policy to create a national champion.

Another big factor is that over time U.S. and Western firms faced increasing headwinds in competing with Chinese firms, Huawei in particular, due to rampant IP theft and illegal subsidies.[23] Huawei grew to be a juggernaut by undercutting the competition on price, in part because U.S., Canadian, and European officials did not adequately react to China's unfair and illegal industrial policies.[24] Rather than fight a losing battle, U.S. firms gave up on designing RAN equipment to focus instead on foundational 4G and 5G technologies such as specialized modems and semiconductors.

This last factor is also the primary argument against trying to create a national champion. Any U.S. company propped up in this fashion would still be at a major disadvantage versus Huawei due to Beijing's industrial policies. It would be expensive to create such a company from the ground up and likely cost more than the U.S. government would be willing to bear to maintain it. Creating a national champion is also not necessary, because there are viable options in existing trusted vendors.

PROVIDE SUPPORT TO ERICSSON, NOKIA, AND SAMSUNG

The alternative to creating a new American company to compete with Huawei is to boost the fortunes of its main competitors: Sweden's Ericsson, Finland's Nokia, and South Korea's Samsung. Together, these companies account for about half of global market share for 4G RAN equipment but are projected to lose market share to Huawei in the transition to 5G.

Policymakers and analysts have proposed an array of ways to bolster these companies, from subsidies and technology transfers to ensuring that Samsung has a larger market share in North America and Europe. Of the three, Nokia is the most vulnerable. Its recent financial woes prompted suggestions among some Trump administration officials for the U.S. government to take a large equity stake in the company, an idea that was quickly shot down.[25] Rumors also swirled that Nokia sought to be acquired by Ericsson in a bid to address its difficulties.[26]

While this is a more palatable option than creating a national champion, mostly because it would cost less, it still requires competing with Huawei on an unlevel playing field. Propping up one or more of the three main competitors would also perpetuate a consolidated and inefficient industry.

REQUIRE 5G RAN INTEROPERABILITY BETWEEN VENDORS

Mandatory interoperability between vendors of 5G RAN equipment could mitigate security risks by ensuring greater vendor choice for operators. In a fully interoperable telecommunications network, a specific piece of equipment from one vendor could be replaced—for example, in the event of the discovery of a vulnerability—by that of another vendor with no change in performance or capability. Huawei has so far resisted calls to provide interoperability, citing its right to supply exclusive products to

capitalize on intellectual property and product investments.[27] Huawei's stance also entrenches vendor lock-in. Industry executives note that Huawei 4G equipment can only interface with the company's 5G kit; upgrading to 5G either locks an operator in to staying with Huawei or requires an immediate "rip-and-replace" of legacy 4G equipment.[28] Without Huawei's voluntary compliance, there is no existing mechanism to mandate RAN vendor interoperability.

PROMOTE INTEROPERABILITY: OPEN RAN

Leaders and startups in the industry are organizing to promote interoperability based on open standards. Industry alliances such as the Open RAN (O-RAN) Alliance and Telecom Infra Project (TIP)—Huawei is not a member of either—advocate for an open RAN architecture approach to wireless telecommunications. These groups have achieved some success in establishing multivendor interoperability. In September 2019, Japanese wireless service provider NTT DOCOMO announced it would launch precommercial 5G services based on O-RAN Alliance specifications.[29] Vodafone is conducting trials in the United Kingdom using equipment that complies with O-RAN standards.[30] Nokia, in a nod to its uncertain future in the industry in its current form, often expresses support for a switch to open interfaces.[31]

The open RAN approach is the most promising of all the options because it lays a groundwork for innovative and competitive solutions. There is potential to shift a global industry in a fundamental way. These grassroots industry-led initiatives show that the needed interest and desire are there, even in a risk-averse industry. What are missing are large-scale proof points. This is why national-level governments need to step in with signaling and incentives to nudge these solid ideas on the path toward broad adoption.

A few days after NTT DOCOMO exhibited at the Tokyo Game Show 2019 in September, the company announced it would launch 5G services based on O-RAN Alliance specifications. (Tomohiro Ohsumi/Getty Images)

Changing the 5G Game with Modular Networks Based on Open Interfaces

The appeal of a telecommunications industry centered on modular networks based on open interfaces is that it addresses the main concerns of the status quo. As a highly consolidated industry with big barriers to entry, there is limited vendor choice. Chinese industrial policy exacerbates this more by making it difficult for trusted vendors to compete. Such consolidation further poses supply chain diversity and security concerns.

There are five key anticipated upsides by transforming the industry to being based on open interfaces:

GREATER VENDOR DIVERSITY

The barriers to entry for telecommunications equipment design and manufacturing are great, particularly so when trying to compete with Chinese corporations that receive lavish subsidies from the Chinese

government.[32] The software industry's barriers to entry are lower, however, and the monetary value of the 5G service market is projected to exceed $85 billion by 2024 at 31.9 percent compound annual growth rate.[33]

The combination of these factors is likely to encourage new entrants to the telecommunications market, particularly in the software domain. The United States and its partners and allies have robust software industries that could readily transform the industry. The anticipated vendor diversity would result in secure and robust supply chains, to the benefit of everyone.

COST

Greater competition and lower software development expenses should translate into lower acquisition costs. Rakuten, a Japanese firm deploying an open architecture network in that country, claims to have built its infrastructure at about half the cost of a traditional network.[34] Similarly, U.S. carrier AT&T claims cost savings through its deployment of virtualized core technology.[35] The cost associated with sustaining such a network is not settled, however. In many cases, a systems integrator is likely needed to manage the complexities of the required architecture and its maintenance. This would present an operator with large downstream costs. It is unclear based on current industry experience (Rakuten, whose 5G open RAN project is detailed below, built its own computing platform and is managing its own integration) how much of the expected cost savings of an open, multivendor system would be absorbed by this expense.[36]

INTEROPERABILITY

A major issue with 5G rollouts is that new equipment from vendors often does not work well with the legacy (4G) equipment of other vendors—or in the case of Huawei, not at all. With network virtualization, interoperability becomes vendor-agnostic because every software or hardware product has to be compatible to function on the network. It becomes much easier for an operator to work with multiple vendors if it so chooses. One aspect of interoperability that must be addressed for widespread open RAN deployments to be feasible is ensuring that each node on a network does not just guarantee transfer of data between nodes, but that each node functions as it is supposed to. Standards-setting in this area will be critical.

GREATER SECURITY

Transparency and standardization of security will be necessary because vendor products must be interoperable. End-to-end encryption should be mandated, for example. Marketplace competition incentivizes superior security practices for vendors to differentiate themselves from their competitors. Software security can also be more readily verified and monitored. Cybersecurity firms such as Finite State have demonstrated that it is possible to do this at scale.[37]

OPERATOR GROWTH

Operators of virtualized networks would benefit from new opportunities in scaling and differentiation. With this new approach it would be possible for an operator to introduce enhancements based on software offerings from multiple vendors. One technique for doing so is "network slicing," where portions of a 5G network can be optimized for different use cases.[38] This optimization is easier and more effectively achieved with choice in vendors.

For example, an operator may decide to team up with one vendor to focus part of its network on enabling automation in manufacturing facilities and supporting logistics. Another vendor could have an edge in offerings such as virtual and augmented reality. This flexibility would encourage existing operators to provide tailored services to specific customers and allow for expansion into new business areas,

encourage new operators to enter the market to meet demand for new capabilities, and provide customers with greater choice and better pricing.

Beyond some uncertainty about the extent of cost savings and the need for comprehensive standards-setting, there is one potential risk and one possible downside to consider when promoting a telecommunication sector centered on open architecture:

POTENTIAL RISK: SCALABILITY

Open, virtualized telecommunications RANs thus far have been largely limited to local and regional deployments. At this scale, the load from traffic routing and network functions on data centers, which typically run on off-the-shelf routers, is readily managed. Whether that architecture is scalable as this load increases for larger networks is an open question for many industry experts.

To date, the indicators for ready scalability are encouraging. Japanese e-commerce firm Rakuten has the largest open virtualized network 4G deployment, with 3,700 sites as of May 2020, and is on track to have 7,000 sites deployed by year-end—the equivalent of a medium-sized European country like Austria or Portugal.[39] Scaling the technology to larger and more complex deployments will test the technology and provide valuable feedback to enhance products.

DOWNSIDE: DISRUPTION TO BUSINESS MODELS OF TRUSTED VENDORS

An obvious outcome of upending an industry is that the players benefiting from the old way of doing business face dramatic upheaval. This poses a problem in that three of the affected companies are based in U.S. allied and partner countries: Finland (Nokia), South Korea (Samsung), and Sweden (Ericsson). These firms also have a considerable employee base in the United States. Samsung is likely to survive because it has a diversified range of business activities to keep it solvent. For Nokia and Ericsson, however, an inability to adapt to this new reality would likely result in their dissolution.

This is an unlikely outcome, however. A full transition to open interfaces will take time, allowing the companies to prepare. The companies are already hedging their bets as well: All three are members of the O-RAN Alliance, and Nokia and a Samsung subsidiary are also members of TIP. Combined with growing interest in and awareness of open interfaces as a viable alternative, these companies can anticipate the shifting winds and navigate the new waters ahead by adjusting their business models accordingly.

Current Open RAN and Virtualized Network Developments

Numerous commercial deployments of 5G open architecture networks are underway around the world. American firms are key vendors for these rollouts.

JAPANESE FIRM SEEKS TO DEPLOY NATIONAL 5G NETWORK BASED ON OPEN RAN AND VIRTUALIZED NETWORKS

Rakuten is currently deploying the world's first 5G virtualized network based on open RAN and expects a commercial launch by year-end.[40] The network is planned to contain equipment made by NEC of Japan, and U.S. firms Airspan, Qualcomm, and Intel. The network will run on software from Altiostar and Robin, also American companies.[41] Rakuten currently operates a nationwide 4G LTE virtualized open RAN

network in Japan.[42] Rakuten's efforts mark an important milestone in demonstrating the feasibility and economics of a large-scale 5G deployment based on open interfaces.

U.S. FIRMS LEAD IN DEVELOPING OPEN VIRTUALIZED RAN SOLUTIONS

American technology companies are among the most prominent solutions providers in the open architecture arena. In March 2020, Altiostar announced a partnership with Spanish mobile operator Telefonica to conduct 4G and 5G open RAN trials in Spain, the United Kingdom, Germany, and Brazil.[43] Altiostar already has open RAN network contracts in Alaska, Mexico, Italy, India, and Japan.[44] Deployment of the company's technology is tied closely to the activities of its chief investors: Cisco Systems, Qualcomm, Tech Mahindra, Telefonica, and Rakuten.[45] Texas-based Mavenir cites open RAN projects in New York, Turkey, and Slovakia, among others, while New York-based JMA Wireless conducted a pilot project in Bologna, Italy.[46]

Chinese telecom operators also do not want to be beholden to a market dominated by a small number of vendors, particularly when the Chinese market for RAN is dominated by Huawei. China Mobile, a major mobile operator and charter member of the O-RAN Alliance, partnered in 2019 with U.S. firms Intel and Radisys to demonstrate 5G RAN equipment that complied with open architecture specifications.[47]

Growing U.S. Government Interest in Open RAN

Elements of the U.S. government are signaling growing interest in open RAN and virtualized network technologies as an alternative to the current makeup of the industry. Most significant is the proposed Utilizing Strategic Allied (USA) Telecommunications Act. Introduced by a bipartisan group of senators in January 2020, the bill calls for the Federal Communications Commission to make available at least $750 million from spectrum auction proceeds for R&D of open architecture and software-based wireless technologies. The pending legislation further allocates $500 million to work with foreign partners to accelerate the adoption of secure and trusted equipment around the world.[48] A bipartisan group of lawmakers introduced a similar bill in the House of Representatives in April 2020.[49]

U.S. Sen. Mark Warner, D-Va., a former telecommunications industry executive, is co-sponsor of the USA Telecommunications Act, a bill that would authorize at least $750 million to fund R&D of telecommunications technologies based on open interfaces. (Larry French/Getty Images for Sirius XM)

At the Department of Defense, which would be the single largest U.S. government customer for open RAN and virtualized networks solutions, the official in charge of the department's R&D efforts called on U.S. companies to develop technologies compliant with open architecture specifications.[50] There are also indications that other national security-focused agencies are exploring the potential of open architecture. In-Q-Tel, the Central Intelligence Agency's venture capital arm, invested in Parallel Wireless, a start-up developing technologies that conform with open RAN specifications.[51]

In February 2020, White House officials announced it would hold a 5G summit with tech executives—including from Nokia, Ericsson, and Samsung. Discussions between White House officials and CEOs of technology companies in the run-up to the announcement "helped shape an emerging view that the 5G issue is as much about software as it is about physical infrastructure."[52] Representatives from Altiostar and Mavenir were invited to the event, indefinitely postponed from April 1 due to the pandemic.[53]

Policy Recommendations

There are three broad categories for taking action to promote a healthy telecommunication sector based on open architecture and virtualized networks: signaling support for open architecture by U.S. government elements; taking specific actions to promote adoption, innovation, and manufacturing of open architecture-compliant equipment in the United States; and employing multilateral coordination to ensure that allies and partners can equally benefit and partake from the advantages an alternative open, multivendor system provides.

SIGNAL U.S. GOVERNMENT SUPPORT

Congress should:

- **Affirm commitment.** There are a number of messaging opportunities Congress should consider for signaling support. For example, passing a nonbinding resolution declaring support for efforts like the O-RAN Alliance and the Telecom Infra Project sends a message to industry that U.S. legislators are supportive of 5G alternatives. These international groups of telecom operators and technology companies promote the development of RAN virtualization and open architecture.
- **Organize hearing series.** Congressional hearings of experts on strategies for broad-based network virtualization are an important way to signal interest in and support of alternatives for 5G infrastructure development. Together with speeches by legislators, such actions could spur private equity and venture capital firms to invest in companies developing technology built on open interfaces.
- **Condition industry subsidies.** Universal Service Fund disbursements, which total billions each year, should be mandated to use U.S.-origin modular products and open interfaces for relevant telecommunication infrastructure deployments whenever possible.

The White House should:

- **Update its 5G strategy.** A commitment to open architecture and network virtualization should be a core element of a national strategy to revamp the telecommunication sector and create a competitive alternative to the current proprietary hardware-based market.

PROMOTE DEVELOPMENT AND DEPLOYMENT

Congress should:

- **Incentivize 5G RAN manufacturing in the United States.** Tax incentives should be provided to encourage 5G-related innovation, manufacturing, and production to occur in the United States as part of a broader effort to diversify and secure critical supply chains. Ericsson, for example, already manufactures U.S.-market equipment in the United States.[54]
- **Boost R&D.** The Utilizing Strategic Allied (USA) Telecommunications Act should be updated to provide at least $2 billion in grants to companies developing compliant 5G wireless technology, up from the $750 million currently proposed. Greater funding will help encourage new companies to enter the market and support skilled workers joining the telecommunications sector.
- **Promote adoption of open multivendor systems in rural areas.** To help close the digital divide in the United States, the Secure and Trusted Communications Networks Act (the “rip-and-replace” bill) should be amended to set aside funds for open, multivendor systems. Rural carriers face considerable barriers to deploying 5G networks due to low population density and large geographic areas requiring coverage.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

- **Encourage U.S. government departments and agencies to adopt open RAN.** The purchasing power of the U.S. government, particularly the Department of Defense, would provide critical momentum. The department is already at the forefront of experimental 5G deployments.[55]

COLLABORATE WITH ALLIES AND PARTNERS

The White House should:

- **Encourage joint R&D and deployment of open RAN.** Joining forces with telecommunications technology leaders Japan, South Korea, Finland, and Sweden will harness the knowledge of the world's telecommunications experts. It will also incentivize the relevant companies and governments to promote open RAN as a preferred alternative.
- **Promote multilateral 5G policies.** The world's leading democracies working in concert have the purchasing power to ensure that an alternative to the 5G status quo is viable. Multilateral coordination will help tech-leading democracies regain the competitive edge in global telecommunications and be able to proliferate more secure and robust communications infrastructure to middle powers. Working in concert to help Ericsson, Nokia, and Samsung transition to a revamped industry based on open interfaces will help to cement critical support.

Conclusion

The world's liberal-democratic technology leaders have a unique opportunity to reshape a foundational aspect of the 21st century economy. Concerted action to revamp the telecommunications equipment sector from an oligopoly increasingly dominated by a Chinese firm to a vibrant and competitive ecosystem is necessary. The choice is between a global communications infrastructure that could be held at risk by Beijing at will, or one where democratic states can innovate and compete to build networks that are secure, resilient, robust, and reliable. Promoting open interfaces as the new norm for telecommunications is the way forward on 5G.

Appendix

ASSESSING THE ARGUMENTS AGAINST BANNING HUAWEI

The prevailing reasons given to not exclude Huawei as a vendor are that doing so would delay 5G rollouts, cost more, and deprive consumers of choice—all causing economic harm and stifling innovation. Huawei's chief security officer in the United States, Andy Purdy, frequently states that U.S. policy toward Huawei harms American companies and costs jobs.[56] Industry executives have claimed that a Huawei ban would slow 5G deployments.[57] Journalists often repeat this.[58] Despite the prevalence of these statements, objective empirical data to back them up are scarce.

To date, the main data provided by Huawei are from reports it paid for. One is an assessment by an American economist.[59] This report, which the company presented to the Federal Communications Commission, concludes that excluding Huawei from U.S. networks could cause 5G rollout delays of 18 months, cost up to $241 billion in lost gross domestic product (GDP), and result in over 75,000 jobs lost. The report's author argues that much of this delay would be due to Huawei's technology being superior to alternatives. Reduced competition would also mean higher prices for RAN equipment that would retard deployments. Finally, the author concludes that Ericsson, Nokia, and Samsung would not be able to meet contractual obligations in a timely fashion—a conclusion supported only by citing a single press report of a 90-day rollout delay for a network in South Korea.[60]

Another report commissioned by Huawei was published in December 2019 by consulting firm Oxford Economics. It presented cost scenarios for individual countries should Huawei be excluded from national 5G networks. The middle cost scenario projects that 5G rollouts would add 0.15 percent to annual GDP from 2020 through 2024, doubling to 0.3 percent through 2030, and a 16 percent to 19 percent equipment price increase. For France, this would mean $400 million more in annual investment costs, 4 million people with delayed access to 5G by 2023, and $8.3 billion in permanent GDP loss. For Japan, it would be $1.4 billion, 13.6 million, and $15.6 billion respectively.[61]

These calculations are based on the assumptions that Huawei technology is superior, that only Ericsson and Nokia would be able to compete for market share that Huawei would lose due to a ban, and that equipment prices would rise due to reduced competition.[62]

An assessment of cost and delay issues specific to Europe is a report from June 2019 from GSMA, a mobile communications industry trade group of which Huawei is a member. The authors claim a €55 billion ($62 billion) cost and an 18-month 5G rollout delay if Chinese vendors are excluded from European networks.[63] Almost half of that increase would be due to presumed price increases by other vendors (i.e., Nokia and Ericsson) and the rest of the cost due to the need to replace legacy (4G) Huawei equipment.[64] Europe counted 465 million unique mobile subscribers in late 2017, meaning that the projected cost would be about $133 per subscriber.[65]

Without transparency into the underlying methodology of the GSMA report, however, it is unwise to take these conclusions at face value. The report's authors state anticipated price increases would be due to decreased market competition, with Europe having much higher market concentration than the rest of the world.[66] What is not explained is why Europe is calculated as having a much higher market concentration than the United States, which has already banned Chinese vendors. Also left out of the projection of the replacement cost is a breakdown of what equipment would need to be replaced in the transition to 5G regardless of the origin of the legacy equipment.

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

Another report on the matter receiving considerable attention is by Strand Consult, a Danish firm. The conclusions articulated here offer a marked contrast to the Huawei-funded reports and the GSMA report. Among the key claims is that 70 percent to 80 percent of legacy equipment would need to be replaced in the transition from 4G to 5G no matter the vendor. Replacing equipment specifically from Chinese vendors beyond that would add up to €3.5 billion ($3.8 billion), or €6.5 ($7) per subscriber. The Strand Consult report also disputes that RAN equipment costs would go up, citing Australia as an example, but does not provide hard numbers or sources in support.[67]

Missing from these reports is creative thinking about alternate futures. All go on the assumption that the status quo remains in place. There is no consideration of the potential for other suppliers such as Samsung achieving greater market share, government interventions on industrial policy, or technological alternatives to an industry dominated by four RAN providers. In reality, a range of such ideas has been considered, and facts on the ground are at odds with Huawei's preferred narrative.

Initial real-world data suggest that the cost of excluding Huawei and replacing legacy equipment will be more in line with the conclusions of Strand Consult and not have a meaningful impact on deployment timelines. Vodafone, a British wireless operator, said in March 2020 that it would spend £200 million (approximately $247 million) over five years to replace Huawei equipment in the core of its European networks in response to the recommendations of the EU 5G Toolkit.[68] Vodafone reported 63.2 million mobile contract customers in Europe in 2019, meaning it looks to spend about $4 per subscriber.[69]

BT, another British operator, in early 2020 projected that its cost to replace Huawei 4G equipment would be around £500 million (approximately $620 million), a cost of around $22 for each of its 28 million customers worldwide.[70] The Nordic operator Telenor, which announced in December 2019 it was switching to Ericsson from Huawei for its 5G rollout, is projecting lower capital expenses as a percentage of sales revenue for 2020, even as its 5G buildout accelerates with portions of the network already active as of January 2020.[71]

Center for a New American Security
1152 15th Street NW, Suite 950, Washington, DC 20005
T: 202.457.9400 | F: 202.457.9401 | CNAS.org | @CNASdc

[1] Frank Bickenbach and Wan-Hsin Liu, "Chinese Direct Investment in Europe – challenges for EU FDI Policy," *CESifo Forum*, 19 no. 4 (2018), https://www.econstor.eu/bitstream/10419/199017/1/CESifo-Forum-2018-4-p15-22.pdf; and "Trade in goods by top 5 partners, EU27, 2019" (Eurostat, 2020), https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Extra-EU_trade_in_goods.

[2] Margaret Rouse and Corinne Bernstein, "radio access network (RAN)," SearchNetworking blog on TechTarget.com, October 2018, https://searchnetworking.techtarget.com/definition/radio-access-network-RAN.

[3] Tom Wheeler, "Moving from 'secret sauce' to open standards for 5G," TechTank blog on Brookings.edu, February 18, 2020, https://www.brookings.edu/blog/techtank/2020/02/18/moving-from-secret-sauce-to-open-standards-for-5g.

[4] Curt Schwaderer, "5G Primer Part 1: Basic Architecture," Embedded-Computing.com, February 22, 2019, https://www.embedded-computing.com/articles/5g-primer-part-1-basic-architecture.

[5] "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019" (Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, 2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

[6] Rachael Falk, "Can the 'core' and 'edge' of a 5G network really be separated?" ASPIStrategist.org.au, January 17, 2020, https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated.

[7] "Verizon and AT&T want to virtualize the 5G Network Core and use Mobile Edge Computing," Technology Blog on ComSoc.org, March 15, 2019, https://techblog.comsoc.org/2019/03/15/verizon-and-att-want-to-virtualize-the-5g-network-core-and-use-mobile-edge-computing.

[8] Erik R. Peterson, "5G is the key to future American competitiveness," Kearney.com, https://www.atkearney.com/communications-media-technology/article?/a/5g-is-the-key-to-future-american-competitiveness.

[9] Brian Heater, "The promise of 5G is still years away," TechCrunch.com, March 1, 2017, https://techcrunch.com/2017/03/01/5g-at-mwc.
[10] Brian Fung, "How China's Huawei took the lead over U.S. companies in 5G technology," *The Washington Post*, April 10, 2019; and Rita Liao, "Huawei says two-thirds of 5G networks outside China now use its gear," TechCrunch.com, June 25, 2019, https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts.

[11] Tamlin Magee, "Huawei controversies timeline," Computerworld.com, September 10, 2019, https://www.computerworld.com/article/3427998/huawei-controversies-timeline.html.

[12] Colin Packham, "Australia spy chief says 5G risks high, in nod to China firms' exclusion," Reuters, October 29, 2018, https://www.reuters.com/article/us-australia-china-huawei/australia-spy-chief-says-5g-risks-high-in-nod-to-china-firms-exclusion-idUSKCN1N40AW; and Marc Santora and Hana de Goeij, "Huawei Was a Czech Favorite. Now? It's a National Security Threat," *The New York Times*, February 12, 2019, https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html.

[13] "Member States publish a report on EU coordinated risk assessment of 5G networks security," European Commission and the Finnish Presidency of the Council of the EU, press release, October 9, 2019, https://europa.eu/rapid/press-release_IP-19-6049_en.htm; and Christopher Ashley Ford, "Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications" (U.S. Department of State Loy Henderson Auditorium, Washington, September 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications.

[14] "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd." (Finite State, 2019), https://finitestate.io/finite-state-supply-chain-assessment.

[15] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," LawfareBlog.com, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; and Ford, "Huawei and Its Siblings, the Chinese Tech Giants."

[16] Cassell Bryan-Low, Colin Packham, David Lague, Steve Stecklow, and Jack Stubbs, "Special report - Hobbling Huawei: Inside the U.S. war on China's tech giant," Reuters, May 21, 2019, https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-us-war-on-chinas-tech-giant-idUSKCN1SR1EU.

[17] Keoni Everington, "China threatens to halt medical supplies after Netherlands changes Taiwan rep office name," TaiwanNews.com, April 30, 2020, https://www.taiwannews.com.tw/en/news/3925556; and Matt Apuzzo, "Pressured by China, E.U. Softens Report on Covid-19 Disinformation," *The New York Times*, April 24, 2020, https://www.nytimes.com/2020/04/24/world/europe/disinformation-china-eu-coronavirus.html.

[18] Tony Czuczka and Steven Arons, "China Threatens Retaliation Should Germany Ban Huawei 5G," Bloomberg, December 14, 2019, https://www.bloomberg.com/news/articles/2019-12-14/china-threatens-germany-with-retaliation-if-huawei-5g-is-banned; and Angelina Rascouet, "China Warns France Against Excluding Huawei From 5G Networks," Bloomberg, February 9, 2020, https://www.bloomberg.com/news/articles/2020-02-09/china-warns-france-against-excluding-huawei-from-5g-networks.

[19] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *The Wall Street Journal*, December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[20] Jonathan Stempel, "Huawei, InterDigital enter licensing pact, end patent litigation; InterDigital surges," Reuters, April 28, 2020, https://www.reuters.com/article/us-interdigital-huawei-tech-settlement/huawei-interdigital-enter-licensing-pact-end-patent-litigation-interdigital-surges-idUSKCN22A31B; and Ted Greenwald and Dana Cimilluca, "Qualcomm, Huawei in Talks to Settle Patent-Royalty Dispute," *The Wall Street Journal*, March 6, 2018, https://www.wsj.com/articles/qualcomm-huawei-in-talks-to-settle-patent-royalty-dispute-1520367886.

[21] Kiran Stacey, "US pushes to fund western rivals to Huawei," *Financial Times*, October 7, 2019, https://www.ft.com/content/94795848-e6e3-11e9-b112-9624ec9edc59.

[22] Arjun Kharpal, "Huawei's offer to license 5G tech to US firm to create an American rival is still 'on the table,'" CNBC, February 25, 2020, https://www.cnbc.com/2020/02/26/huawei-reiterates-offer-to-license-5g-tech-to-us-firm-to-create-rival.html.

[23] See, for example, Tom Blackwell, "Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants," *National Post*, February 20, 2020, https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants; and Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha, "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics," *The Wall Street Journal*, May 25, 2019, https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

[24] Elsa B. Kania, "Why Doesn't the U.S. Have Its Own Huawei?" Politico, February 25, 2020, https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-american-innovation-strategy-106378.

[25] Ellen Nakashima and Jeanne Whalen, "Barr suggests U.S. consider investing in Nokia, Ericsson to counter Huawei," *The Washington Post*, February 6, 2020, https://www.washingtonpost.com/national-security/barr-warns-against-chinese-dominance-of-5g-super-fast-networks/2020/02/06/1da26794-48ec-11ea-9164-d3154ad8a5cd_story.html; and David Shepardson, "White House dismisses idea of U.S. buying Nokia, Ericsson to challenge Huawei," Reuters, February 7, 2020, https://www.reuters.com/article/us-usa-china-spying-huawei-tech-idUSKBN2012A5.

[26] Ed Hammond, Dinesh Nair, Myriam Balezou, and Niclas Rolander, "Nokia to Weigh Strategic Options as Profit Pressure Mounts," Bloomberg, February 26, 2020, https://www.bloomberg.com/news/articles/2020-02-26/nokia-said-to-weigh-strategic-options-as-profit-pressure-mounts.

[27] Matt Hamblen, "Cyber experts call for Huawei 5G gear to interoperate with other vendor hardware," FierceElectronics.com, September 24, 2019, https://www.fierceelectronics.com/electronics/cyber-experts-call-for-huawei-gear-to-interoperate-other-vendor-hardware.

[28] David Shepardson, "AT&T CEO says China's Huawei hinders carriers from shifting suppliers for 5G," Reuters, March 20, 2019, https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX.

[29] Linda Hardesty, "NTT DoCoMo achieves multi-vendor base station interoperability," FierceWireless.com, September 18, 2019, https://www.fiercewireless.com/operators/ntt-docomo-achieves-multi-vendor-base-station-interoperability.

[30] Linda Hardesty, "Vodafone leads the early adopter phase of O-RAN," FierceWireless.com, February 25, 2020, https://www.fiercewireless.com/operators/vodafone-leads-early-adopter-phase-o-ran.

[31] Anne Kauranen, Tarmo Virki, and Douglas Busvine, "'We don't have a 5G problem,' says Nokia's head of software," Reuters, November 20, 2019, https://www.reuters.com/article/us-nokia-software-interview/we-dont-have-a-5g-problem-says-nokias-head-of-software-idUSKBN1XU2BB.

[32] Kiran Stacey, "Why is there no US rival to compete with Huawei?" *Financial Times*, April 26, 2019, https://www.ft.com/content/18d3823a-65f2-11e9-9adc-98bf1d35a056.

[33] "5G Service Market to Witness Upsurge by 31.9% CAGR by 2023 | Upsurge in Ultra Latent Connectivity to Foster 5G Service Market Growth," Globe Newswire, July 30, 2019, https://www.globenewswire.com/news-release/2019/07/30/1893828/0/en/5G-Service-Market-to-Witness-Upsurge-by-31-9-CAGR-by-2023-Upsurge-in-Ultra-Latent-Connectivity-to-Foster-5G-Service-Market-Growth.html.

[34] "5Geopolitics," *The Economist*, April 11, 2020, 48.

[35] Tammy Parker, "AT&T's virtualization play makes a star out of Affirmed Networks," FierceWireless.com, February 26, 2014, https://www.fiercewireless.com/tech/at-t-s-virtualization-play-makes-a-star-out-affirmed-networks.

[36] "5Geopolitics," 48.

[37] "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd."

[38] "An Introduction to Network Slicing" (GSM Association, 2017), https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf.

[39] Juan Pedro Tomás, "Rakuten Mobile is deploying 10,000 radio stations: CEO," RCRWireless.com, May 14, 2020, https://www.rcrwireless.com/20200514/asia-pacific/rakuten-mobile-process-deploy-10000-radio-stations-ceo.

[40] Iain Morris, "Rakuten delays 5G launch by three months on COVID-19 disruption," LightReading.com, May 15, 2020, https://www.lightreading.com/asia/rakuten-delays-5g-launch-by-three-months-on-covid-19-disruption/d/d-id/759683?_mc=RSS_LR_EDT.

[41] Iain Morris, "Rakuten turns 5G revolutionary as it nears world's first open RAN launch," LightReading.com, March 19, 2020, https://www.lightreading.com/asia/rakuten-turns-5g-revolutionary-as-it-nears-worlds-first-open-ran-launch/d/d-id/758349; and Linda Hardesty, "Rakuten's 5G network will be built with containers," FierceWireless.com, April 10, 2020, https://www.fiercewireless.com/5g/rakuten-s-5g-network-will-be-built-containers.

[42] Matt Kapko, "Rakuten Mobile Dismisses Open RAN Skeptics," SDXCentral.com, March 3, 2020, https://www.sdxcentral.com/articles/news/rakuten-mobile-dismisses-open-ran-skeptics/2020/03.

[43] "Telefonica joins forces with Altiostar, Gigatera Communications, Intel, Supermicro, and Xilinx for the development and deployment of Open RAN in 4G & 5G," Altiostar, press release, March 18, 2020, https://www.altiostar.com/telefonica-joins-forces-with-altiostar.

[44] "Announcing North America's Most Advanced Radio Access Network Solution by GCI in Collaboration with Altiostar," Altiostar, press release, February 21, 2018, https://www.altiostar.com/announcing-north-americas-most-advanced-radio-access-network-solution-by-gci-in-collaboration-with-altiostar; "Rakuten Mobile and Altiostar To Launch World's First Cloud-Native, Container-Based 5G Radio Access Network Solution," Altiostar, press release, February 27, 2020, https://finance.yahoo.com/news/rakuten-mobile-altiostar-launch-worlds-130000829.html; and "Bharti Airtel deploys Open vRAN with Altiostar," Altiostar, press release, April 29, 2020, https://www.altiostar.com/bharti-airtel-deploys-open-vran-with-altiostar.

[45] "Investors," Who We Are, Altiostar, https://www.altiostar.com/who-we-are/investors.

[46] "Hudson Valley Wireless Deploys Mavenir's Cloud-Native LTE vEPC," Mavenir, press release, March 11, 2020, https://mavenir.com/press-releases/hudson-valley-wireless-deploys-mavenirs-cloud-native-lte-vepc; "T-Mobile CZ and Slovak Telekom Have Selected Mavenir for Their Next-Generation NFV-Based Harmonized IMS," Mavenir, press release, February 4, 2020, https://mavenir.com/press-releases/t-mobile-cz-and-slovak-telekom-have-selected-mavenir-for-their-next-generation-nfv-based-harmonized-ims; "Mavenir and Turkcell Partner on OpenRAN," Mavenir, press release, February 27, 2020, https://mavenir.com/press-releases/mavenir-and-turkcell-partner-on-openran; and "Wind Tre Deploys Live XRAN® Fully Virtualized RAN from JMA Wireless, Expanding the List of Networks Benefiting Downtown Bologna with XRAN® Extreme Efficiencies," JMA Wireless, press release, February 28, 2019, https://jmawireless.com/wind-tre-deploys-live-xran-fully-virtualized-ran-from-jma-wireless-expanding-the-list-of-networks-benefiting-downtown-bologna-with-xran-extreme-efficiencies.

[47] "Radisys, Intel and China Mobile Team Up for 5G Open RAN Architecture," Radisys, press release, June 25, 2019, https://www.businesswire.com/news/home/20190625005974/en/Radisys-Intel-China-Mobile-Team-5G-Open.

[48] U.S. Senate, *A bill to use proceeds from spectrum auctions to support supply chain innovation and multilateral security*, S. 3189, 116th Cong., 2nd sess., https://www.warner.senate.gov/public/_cache/files/2/3/2365fc6a-422c-4df2-837b-f297bb293ad2/E8131EF8149D5D0E1411683ABC3DECCD.oll20034.pdf.

[49] Maggie Miller, "Lawmakers introduce legislation to boost American 5G efforts," TheHill.com, April 24, 2020, https://thehill.com/policy/cybersecurity/494522-lawmakers-introduce-legislation-to-boost-american-5g-efforts.

[50] Kiran Stacey, "Pentagon wants open-source 5G plan in campaign against Huawei," *Financial Times*, December 22, 2019, https://www.ft.com/content/6863a21a-234a-11ea-92da-f0c92e957a96.

[51] Ryan Lovelace, "CIA funnels cash to private company aimed at defeating Huawei," *The Washington Times*, March 8, 2020, https://www.washingtontimes.com/news/2020/mar/8/cia-funnels-cash-q-tel-bid-defeat-huawei.

[52] Eamon Javers, "White House plans 5G summit with global tech leaders as battle with Huawei continues," CNBC, February 21, 2020, https://www.cnbc.com/2020/02/21/trump-plans-5g-summit-with-global-tech-leaders-in-huawei-battle.html.

[53] Monica Alleven, "Altiostar: Open RAN, virtualization 'not pie in the sky,'" FierceWireless.com, March 19, 2020, https://www.fiercewireless.com/tech/altiostar-open-ran-virtualization-not-pie-sky.

[54] Matt Kapko, "Ericsson Expands US Manufacturing With New Factory in Texas," SDXCentral.com, September 23, 2019, https://www.sdxcentral.com/articles/news/ericsson-expands-us-manufacturing-with-new-factory-in-texas/2019/09.

[55] Stacey, "Pentagon wants open-source 5G plan in campaign against Huawei"; and Paul McLeary, "Pentagon Briefs Industry On 5G Experiments," BreakingDefense.com, February 24, 2020, https://breakingdefense.com/2020/02/pentagon-briefs-industry-on-5g-experiments.

[56] Andy Purdy, "Huawei's Chief U.S. Security Officer Downplays The Company's National Security Threat," interview by Mary Louise Kelly, All Things Considered, NPR, February 7, 2020, https://www.npr.org/2020/02/07/803907468/huaweis-chief-u-s-security-officer-downplays-the-companys-national-security-thre; Matt Kapko, "Huawei CSO Slams US Policy," SDXCentral.com, February 28, 2020, https://www.sdxcentral.com/articles/news/huawei-cso-slams-us-policy/2020/02/; and Hope King and Rebecca Heilweil, "Huawei: U.S. Ban Will Hurt American Jobs," Cheddar.com, May 16, 2019, https://cheddar.com/media/huawei-us-ban-american-jobs.

[57] "Huawei ban would delay 5G rollout: Three," BBC News, March 21, 2019, https://www.bbc.com/news/technology-47659380; and Matt Kapko, "Vodafone Australia Blames 5G Delays on Huawei Ban," SDXCentral.com, December 30, 2019, https://www.sdxcentral.com/articles/news/vodafone-australia-blames-5g-delays-on-huawei-ban/2019/12.

[58] Joy Tan, "Huawei exec: The US can't afford to work without us," CNN, February 28, 2020, https://www.cnn.com/2020/02/28/perspectives/huawei-ban-5g-technology/index.html.

[59] "Huawei Facts," Huawei, https://www.huawei.com/us/facts.

[60] Written Ex Parte Submission of Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc., Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Docket No. 18-89 (FCC filed May 10, 2019), https://ecfsapi.fcc.gov/file/1011236282523/Final%20-%20Huawei%20Ex%20Parte%20re%20Economic%20Report%20(10-11-2019).pdf.

[61] "Restricting Competition in 5G Network Equipment: An Economic Impact Study" (Oxford Economics, December 2019), https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V10.pdf.

[62] "Restricting Competition in 5G Network Equipment."

[63] Gwénaëlle Barzic, "Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos," Reuters, June 7, 2019, https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-telcos-idUSKCN1T80Y3.

[64] "Economic impact assessment of 5G supply chain restrictions in the EU" (GSMA Intelligence, April 2019), https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/GSMA-report-Cost-of-ban.pdf.

[65] "The Mobile Economy: Europe 2018" (GSM Association, 2018), https://www.gsma.com/mobileeconomy/europe.

[66] "Economic impact assessment of 5G supply chain restrictions in the EU."

[67] "The real cost to rip and replace Chinese equipment from telecom networks" (Strand Consult) http://www.strandconsult.dk/sw8402.asp.

[68] Paul Sandle, "Vodafone to remove Huawei from core of European network," Reuters, February 5, 2020, https://www.reuters.com/article/us-vodafone-outlook/vodafone-to-remove-huawei-from-core-of-european-network-idUSKBN1ZZ0RB.

[69] "Vodafone Group Plc Annual Report 2019" (Vodafone Group Plc, 2019), http://media.corporate-ir.net/media_files/IROL/77/77862/annual-reports/annual_report19/downloads/Vodafone-full-annual-report-2019.pdf.

[70] Philip Jansen, "BT Group Q3 2019/20 Media Call," https://www.btplc.com/Sharesandperformance/Financialreportingandnews/Quarterlyresults/2019-2020/Q3/Downloads/Webcast/q320-media-transcript.pdf; and "BT Group plc Annual Report 2019," (BT Group plc, 2019), https://www.btplc.com/Sharesandperformance/Financialreportingandnews/Annualreportandreview/pdf/2019_Annual_Report.pdf.

[71] Bevin Fletcher, "Telenor ditches Huawei, taps Ericsson for 5G RAN in Norway," FierceWireless.com, December 13, 2019, https://www.fiercewireless.com/5g/telenor-ditches-huawei-taps-ericsson-for-5g-ran-norway; "Telenor Group Annual Report 2019" (Telenor Group, 2019), 8, https://www.telenor.com/wp-content/uploads/2020/03/2201011-Annual-Report-2019-Q-a97d1b270234873cebe5901dfe14e8c2-1.pdf; and "Telenor Group's results for the 4th quarter 2019," Quarterly Report, Telenor, https://www.telenor.com/investors/reports/2020/telenor-groups-results-for-the-4th-quarter-2019.