Eurasia Group White Paper:
The Geopolitics of 5G

PREPARED BY EURASIA GROUP
15 NOVEMBER 2018

eurasia group politics first

Eurasia Group White Paper:
The Geopolitics of 5G

PREPARED BY EURASIA GROUP
15 NOVEMBER 2018

CONTENTS

CONTACTS

Paul Triolo
Practice Head, Geo-technology
+1 202.903.0006
triolo@eurasiagroup.net

Kevin Allison
Director, Geo-technology
+1 202.552.5399
allison@eurasiagroup.net

Clarise Brown
Researcher, Geo-technology
+1 202.552.5392
cbrown@eurasiagroup.net

Prepared by Eurasia Group

eurasia group politics first

Introduction

The race is underway to deploy next-generation 5G mobile networks. 5G will be both quantitatively different from previous generations of mobile network technology and qualitatively different from anything that has come before, in terms of the innovation that it will enable.

This report, authored by Paul Triolo and Kevin Allison of Eurasia Group's Geo-technology practice, offers an introduction to the geopolitics of 5G. It explains how political forces, including the ongoing technology and trade confrontation between the US and China, will shape the development of next-generation mobile standards, spectrum allocation, and deployment in key markets and regions. It likewise addresses how 5G's development will shape economic, technological, and geopolitical competition between the world's leading technology superpowers.

Much of the public discussion of 5G has centered on its vastly improved data speeds. Next-generation mobile networks will stream data about 100 times faster than today's 4G networks, making the idea of "downloading" even very large files, such as high-definition feature films, largely obsolete. But unlike previous generations of networks, which were built with consumer voice and data services in mind, 5G will also enable high-capacity and ultra-low latency communications.

These capabilities, which will be rolled out for the first time with 5G, will dramatically enhance the performance of mobile data networks by enabling new types of machine-to-machine communication, paving the way for next-generation digital applications that require highly reliable, near-instantaneous access to massive amounts of data. 5G is what will make driverless cars, smart cities, and other large-scale applications of connected devices feasible on a commercial scale.

5G's integral role in these transformational technologies means that to a much greater extent than with 4G, the development and deployment of the next-generation network is being influenced by political concerns, even as information and communications technology companies, firms in affected sectors such as manufacturing and automobiles, and entire national industries jockey for position in the emerging ecosystem.

Specifically, as the trade and technology confrontation between the US and China has steadily escalated over the past year, driven by US economic and national security concerns and by China's ambitious industrial, technological, and economic development goals, every major issue associated with 5G networks has become politicized.

Formerly dry, technical subjects such as standards-setting and spectrum allocation for 5G networks, the location of supply chains, how to protect the next generation of mobile data networks from cyber threats, and which companies build 5G infrastructure and handsets in which countries have acquired new importance.

The decisions governments and industry players make about when and how to build their 5G networks will have significant consequences, both for how the next phase of the digital revolution unfolds in the US, China, and beyond, and, potentially, for the long-term balance of global power. This white paper offers a framework for understanding the underappreciated political dimensions of this critical technology shift.

Paul Triolo
Practice Head, Geo-technology

Key findings

- China will likely gain some first-mover advantage in 5G as it moves toward commercial-scale deployment of its domestic 5G network in 2020. Deployment of standalone 5G in China will mark the culmination of a multi-year whole-of-government effort to establish the country at the forefront of the next generation of mobile networks and related applications through state-led initiatives such as the Internet+ plan (2015) and the 13th Five Year Plan (2016).
- Efforts by the US and like-minded allies to exclude Chinese networking equipment suppliers from Western and allied 5G networks will continue, with the US-China trade and technology confrontation showing little sign of easing and potential national security risks posed by Chinese hardware increasingly dominating policy debates.
- The push for a China-free 5G alternative is likely to delay 5G deployment in some countries, as backup suppliers are forced to invest in new manufacturing capacity and human capital required to introduce next-generation networks cost-effectively and at scale, further cementing China's first-mover advantage.
- A bifurcated 5G ecosystem will increase the risk that the global technology ecosystem gives way to two separate, politically divided and potentially noninteroperable technology spheres of influence—one led by the US and supported by technology developed in Silicon Valley; another led by China and supported by its cadre of highly capable digital platform companies.
- A split into China and non-China camps could lead to some minor interoperability issues, but more likely would result in lower economies of scale and higher transaction costs with second-order effects for the cost of both user and infrastructure equipment.
- Alongside the political fight over the 5G network itself, the US and China are competing to develop innovative technology applications that will run on top of deployed 5G networks. Here the US has an advantage in terms of *innovation capacity*, but China will benefit from its head start in *applications* and *use cases* as it builds out its domestic 5G ecosystem and Chinese companies compete for market share abroad.
- Successful 5G deployments will clear the way for 5G uses cases and applications, and ultimately commercial-scale deployments of next-generation technologies. This is not a winner-take-all game, but there is potential for a virtuous cycle as 5G and related applications attract talent and capital while huge datasets generated by applications running on top of 5G networks spur further innovation.
- In a bifurcated world, third countries wishing to gain access to this virtuous cycle will face difficult choices about whose 5G network technologies and related application ecosystems to adopt. Governments are likely to come under pressure from the US and allies to avoid dependence on China for 5G.
- At the same time, developing countries that are more sensitive to cost will find Chinese technology and related enticements—for example, infrastructure and project financing available through the Belt and Road Initiative—hard to pass up, particularly if China gains an edge in related technology applications. The US/China-exclude camp has no comparable initiative to extend its technology influence globally.

The 5G innovation stack

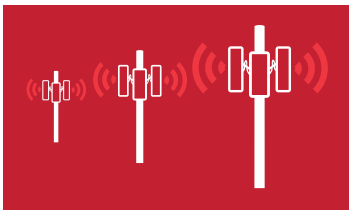
5G-enabled applications

5G networks will enable a new breed of digital applications that depend on ultra-fast, low latency, high-throughput communications, including driverless cars, advanced factory automation, and smart cities.

These applications will be the biggest source of long-term economic and political advantage from 5G, and they will be the subject of intense competition between leading US and Chinese companies.

The US has edge in innovative capacity, but China will gain a head start developing new applications and use cases.

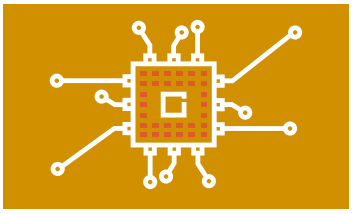
The 5G network



China's first-mover status in 5G may translate into a geopolitical advantage in countries in Africa, Latin America, and the Middle East, where financing and other incentives available through the Belt and Road Initiative will be difficult for governments to pass up, allowing China to extend its digital influence globally.

A parallel US effort to exclude Chinese networking equipment from Western networks will limit China's 5G footprint in more advanced economies.

5G hardware and software



The US retains significant advantages in semiconductors, enterprise software, and other essential hardware and software components of 5G base stations and other underlying technology.

The US and like-minded allies are pushing back against the use of Chinese hardware in 5G networks over concerns about national security.

5G: Foundational technology, political battleground

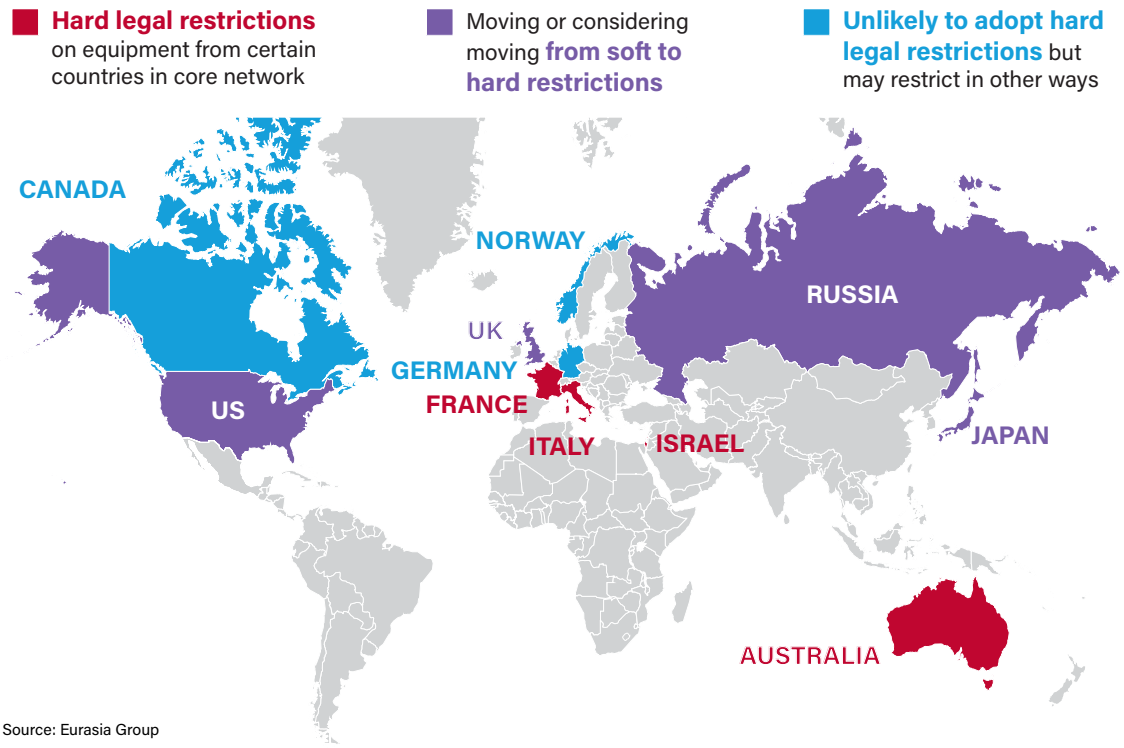
The rollout of 5G networks will take more than a decade and will be one of the most complex and expensive technology projects ever undertaken. The pace of 5G deployment in a given country will depend on an array of factors. These include carrier preferences, government regulatory policies and strategies, infrastructure and handset equipment maker product timelines, costs and scalability of 5G infrastructure, progress in developing compelling uses and applications of 5G networks, and the ability of various players to capture value in a complex technology ecosystem.

To a much greater extent than the deployment of 4G, 5G timelines will also be influenced by political and national security concerns, which will likewise vary from market to market. This is because unlike previous generations of mobile data networks, which were built with consumer voice and data services in mind, 5G will also dramatically expand the capabilities of mobile data networks by enabling new types of machine-to-machine communication.

Although early 5G commercial offerings will target smartphone users who want better video download speeds, the truly revolutionary aspect of 5G networks will be their high-capacity and ultra-low-latency features. These capabilities will for the first time allow industrial-scale deployments of autonomous vehicles, factory automation, and other technologies that require large numbers of devices to remain in near-instantaneous communication across a wide area. By serving as a foundation for the next phase of the digital revolution, 5G will not just offer a quantitative improvement over previous technologies via higher speeds, but it will be qualitatively different from earlier data networks in terms of the innovation that it enables.

That has put 5G at the center of an escalating trade and technology confrontation between the US and China, the world's leading technology superpowers. Both increasingly view control of the next wave of advanced technologies and related applications such as driverless cars, smart cities, and advanced factory automation as an urgent matter of economic and national security.

Number of countries considering restrictions on providers of critical telecommunications infrastructure



Source: Eurasia Group

The consequences are already being felt: Throughout the year, it has become clear the US and some key allies are working to exclude Chinese equipment vendors Huawei and ZTE from their commercial and government 5G networks, owing to national security concerns. Although several countries have effectively restricted the access of these Chinese network equipment suppliers from core government and commercial data networks for some time, 5G has raised the stakes considerably, leading to a concerted push by the US and other members of the so-called Five Eyes intelligence alliance and other like-minded countries to bar Chinese firms from next-generation networks.

This broad camp now includes the US, Australia, and New Zealand. Canada and the UK are likely to take similar steps over time, but their ability to act is complicated by the presence of substantial Chinese equipment in their existing commercial mobile networks. Other countries such as France and Germany are also considering ways to limit Chinese vendor participation in core 5G network deployment, as is Japan. South Korea will not likely follow this path, though it is also concerned about the national security aspects of 5G.

A closer look at 5G can help explain why it has become such an important battleground in the US-China confrontation over the future of advanced technologies.

Understanding 5G networks

The design of 5G networks marks a significant departure from 2G, 3G, and 4G networks, which were built primarily around handset-to-handset voice and data communications. As smartphone cameras and screens became better and afforded much higher resolutions, demand for data applications such as video streaming required equipment makers and operators to adjust the performance of 4G networks. However, the underlying network architecture continued to face limitations in terms of density of devices and achieving very high data rates for applications such as streaming high-definition video.

Enter 5G, which is designed from the ground up to handle massive numbers of devices, high-data rates, and applications that require very fast and reliable communications with minimal latency, or lag, such as connected and autonomous vehicles. To deliver these features, 5G networks are divided into three primary network "slices," each serving a different primary function:

Enhanced mobile broadband (eMBB): This portion of the network, likely to be rolled out first and to use aspects of existing 4G LTE architecture, will enable much higher download speeds for smartphones and other devices, up to ten times faster.

Ultra-reliable low-latency communications (uRLLC): This segment is designed for applications including autonomous vehicles, which require there to be little or no gaps in communication for mission-critical applications such as road obstacle sensing and command and control. This portion of the network will require considerable investments in new equipment to get communications capacity nearer to roads and buildings. It also requires new antenna designs and smaller equipment that will provide dense coverage.

Massive machine-to-machine communications (mMTC): This segment is designed to handle billions of new sensors and other "edge" devices that will communicate among themselves and with other parts of the network, also known as the Internet of Things (IoT).

Standalone vs non-standalone 5G

The unveiling of 5G is typically divided into two phases. First is non-standalone 5G (NSA), which adds eMBB to an existing 4G LTE network and mostly leverages existing pieces of the mobile infrastructure. The second, full or standalone (SA), 5G includes the ultra-reliable low-latency and massive machine-to-machine communications portions, both of which require substantial investments in new infrastructure such as antennas and base stations.

5G networks will rely heavily on artificial intelligence

5G networks' primary functions will be software-based, as opposed to the hardware that drives traditional data networks, making use of concepts such as software defined network and network function virtualization. In industry jargon, 5G will be largely "cloud native."

To control these functions and to ensure that specific applications are allocated the proper network resources, 5G networks will make extensive use of artificial intelligence (AI) to manage network complexity. One practical consequence is that infrastructure equipment manufacturers will design and deploy operating and management systems that use AI, both separately and in collaboration with carriers.

Unique security challenges

5G networks present several security concerns. First, in part because of the role of AI discussed above, equipment integrators will play a much bigger role in the process of operating a network

than in previous generations of mobile technology. This is likely further feeding US and other Western security concerns related to Chinese equipment vendors' role in 5G networks.

The next generation of mobile networks will also blur the traditional distinction between the radio access network (RAN), consisting of base stations and antennas that handle the radio frequency (wireless) portion of the network, and the core portion, including central switching and transport networks that carry large amounts of data traffic.

This is because the architecture of 5G pushes a lot of what would be formerly core functionality out to the "edge" of the network, with big implications for 5G network security:

- The huge growth in the number of connected devices and large bandwidths means that the potential for unsecure or compromised devices to be used for malicious activity such as bot-net-driven denial of service attacks goes way up, as does their size and severity.
- This coupled with software virtualization in the cloud will increase the potential "attack surface" that malicious actors can target by orders of magnitude.
- An exponential expansion of the volume of data flying around will make it more difficult to detect malicious traffic.

Lastly, alongside these technical concerns there is a structural security issue: As the number of connected devices and the amount of data explode, a greater share of total global economic output will come to rely on global data networks. The vulnerability of companies, industries, cities, and even entire countries to disruptive cyberattacks or network outages will grow accordingly, giving malicious cyber actors new leverage and incentives to conduct ransomware attacks and increasing economic vulnerability to destructive—or even merely disruptive—cyberattacks.

This rising economic dependence on 5G will further strengthen the arguments of China hawks in the US advocating for the exclusion of Chinese equipment—or other foreign hardware or software—from Western data networks. Recent allegations that Chinese cyber operators may have taken advantage of supply chains originating in China to compromise a major supplier of server hardware and its clients will only add to concerns over introducing potential security vulnerabilities into a network that will increasingly lie at the heart of the global economy, regardless of the ultimate truth of the allegations.

Geopolitics of 5G standards

Process nearly complete, with European, US, and Chinese firms dominating

One of the first big hurdles to deployment of 5G—both NSA and SA—is nearing completion: the establishment of international standards governing 5G systems.

The standards-setting process has been a long-term, global, and collaborative effort driven by seasoned technical expert groups organized and overseen by the 3rd Generation Partnership Project (3GPP). 3GPP's 500 participating organizations develop standards for mobile networks based on performance and interoperability criteria established by the International Telecommunications Union (ITU).

The standard-setting process is important because it will determine not just how 5G networks are built, but also how money flows between participants in the 5G ecosystem. Companies whose technology becomes the industry standard for 5G will receive royalty payments from other ecosystem participants. Those payments, in turn, will help fund future innovation. In contrast to 3G and 4G, where China was largely relegated to the sidelines in the standards-setting process, China has been heavily involved in the standards process for 5G—a sign of its growing ambitions, capabilities, and global influence.

The 5G standards suite will build on existing 4G LTE standards and provide flexible interoperability for the various flavors of 5G with legacy 4G and 3G systems (which will continue to operate for some time, particularly in developing market countries).

Current planned deployment timelines by country

Country/ region	Trials	Commercial NSA 5G	Commercial SA 5G	Notes
US	2018	2020	2025	AT&T trialling NSA 5G for end 2018, T-Mobile to launch NSA 5G commercially in limited areas probably late 2019; T-Mobile shooting for nationwide by 2020
EU	2019	2020	2025	EC shooting for large-scale commercial use by 2020 for NSA 5G, SA 5G coverage of main urban areas and transportation routes by 2025
China	2018	2019	2020	China Mobile focused on initial rollout of SA 5G, other carriers will gradually introduce SA 5G
Japan	2018	2020	2025	KDDI, Softbank, NTT Docomo all seeking commercial launch of NSA 5G by 2020
South Korea	2018	2019	2025	KT targeting commercial launch of NSA 5G some time in 2019, SK Telecom planning for second half 2019
Canada	2019	2020	2025	Canada will not be auctioning 5G spectrum until 2020, industry pushing for 2019
Australia	2018	2019	2025	Telstra and Optus have committed to roll out NSA 5G in 2019, with Vodafone to follow in 2020

Note: elements of 5G are likely to be rolled out in stages and markets during the period 2020-2025 in markets other than China.
Sources: Eurasia Group, media

In June, 3GPP finalized the list of standards that will form the basis for a subset of standard essential patents (SEP) for the standalone new radio (NR) portion of 5G and for what eventually will be the 5G core, so-called Release 15. This release is focused on the enhanced mobile broadband portion of 5G. If a standard is impossible to implement without using a patented technology, then it is termed a standard essential patent.

Companies participating in 3GPP must agree to the voluntary fair, reasonable, and non-discriminatory terms for SEPs, promising to make their intellectual property associated with the patents available to other firms under specific conditions. Media reports about the process often mischaracterize the role of governments and companies in both the standards-setting process and the determination of SEPs, and they make claims about particular countries, specifically China's, ability to influence standards and patent decisions and use standards as a way to control or influence network operations. The standards process is not public, but it is well established, with multiple companies proposing and contributing technical solutions for a given standard. Standards are agreed based on technical criteria, making it difficult for governments to influence the process.

Nevertheless, politics still plays a role in 5G standards setting. One leading example that observers point to as potentially influenced by political considerations is the selection of a control channel modulation standard championed by China's 5G leader Huawei. While the standard had technical merit, its approval generated controversy, with some industry observers suggesting that China's overall presence at 3GPP and growing global economic clout were decisive factors in the approval.

There is no doubt that Chinese firms, backed by Beijing, are exerting much more influence in the standards-setting process. China has pushed its companies to play a leading role in 5G after it was left largely dependent on foreign 3G technology and played a limited role in 4G standards. Beijing's efforts early on to secure a much bigger role in 5G can also be seen as part of a much broader strategy to reduce China's balance sheet of patent licensing payments, primarily from

major mobile chip technology players such as Qualcomm. Exactly who owns the SEPs for a particular set of standards can be very difficult to estimate—much of the data are not necessarily public, and there are always disputes over ownership. For 4G LTE, one estimate had LG and Qualcomm with 23% and 21%, while ZTE and Huawei own just 6% and 1%, respectively.

Once standards have been set and the subset of standard essential patent licensing defined, companies must build to the agreed standards and pay royalties to patent licensees as required. The patent licensing and royalty payments process is separate from the standards setting and will play out over many years. Once standards are in place, governments and companies cannot manipulate the standards; any company can build equipment and devices based on the standard/SEP suite.

5G standards and security—a red herring

Concerns about 5G security center not on the standards themselves, but on which firms are supplying the equipment and where it is built. 5G standards are like recipes in a cookbook: Any company that takes the recipe and uses it to build networking equipment has the potential to go beyond the standards, including potentially malicious hardware or software implants. This is the primary concern of the US national security community, and it largely accounts for the many legislative and executive measures in place or being considered that would bar Chinese firms from building 5G core infrastructure anywhere in the US.

The large suite of 5G standard essential patents is now coming into clearer focus, and the primary holders of these will be European equipment makers Ericsson and Nokia; Chinese leaders Huawei and ZTE; Japanese and South Korean players such as Fujitsu, Panasonic, Samsung, and LG; and US firms such as Qualcomm, Interdigital, Intel, and Cisco.

No single country's companies will dominate the allocation of SEPs. The goal of the 3GPP is to ensure that the best technology is incorporated into the 5G SEP suite and that no one country or region has a dominant or outsize influence.

Despite this goal, China's influence in the 5G standards-setting process is likely to expand considerably compared to its marginal role in 4G standards. One estimate is that Chinese companies, including Huawei, ZTE, Lenovo, and others, held about 10% of SEP patents in 2017. This may rise substantially, likely to about 40%, once patents have been granted and SEPs are fully clarified. The process is iterative, so as the standards are constantly updated, Chinese firms could contribute more intellectual property as part of future 3GPP 5G releases and increase their overall share.

The geopolitics of 5G spectrum: Big decisions looming, non-interoperability a concern

In addition to standards, spectrum will play an important role in which countries and companies are able to gain a competitive advantage early in the 5G commercial rollout process—and therefore in the geopolitics of 5G.

The ITU will hold a critical World Radio Conference (WRC) in 2019 that will consider spectrum allocation for 5G in light of changes since 2015, and by then the actual experience with deployment of networks, primarily in China and the US. China is already gearing up to make its case at the ITU, while the US does not appear yet to have a coherent government strategy on its preferred spectrum allocations for 5G.

A primary issue is that different countries and companies favor either high frequencies or low frequencies, both of which will be used in 5G, which has a much broader and complex spectrum allocation plan than 4G. This is the result of several factors, primarily the design goals

of 5G that focus on handset voice and data communications, but also on machine-to-machine communications supporting autonomous vehicles and the IoT. The greater density of devices requires more bandwidth capacity and new antenna types to handle the challenge of billions of devices connected to 5G networks.

5G Key Global Vendors

Vendor	Country	Technology sectors primary	Technology sectors secondary	Notes
Ericsson	Sweden	Network equipment, integration	Fiber backhaul	Joint work on end-to-end services with Fujitsu
Nokia	Finland	Network equipment, integration	Fiber backhaul, edge devices	
Huawei	China	Network equipment, integration	Fiber backhaul, edge devices	
ZTE	China	Network equipment, integration	Fiber backhaul, edge devices	
Samsung	South Korea	Network equipment, integration	Edge devices	Joint development of base stations with NEC
LG	South Korea	Edge devices		
Qualcomm	US	Mobile chipsets, modems	Infrastructure semiconductors	
Intel	US	Mobile chipsets, modems		
Broadcom	US	Mobile chipsets, other ICs		
Cisco	US	Data center equipment, routers		
InterDigital	US	IoT devices		
NXP	Netherlands	IoT devices		
Alcatel Lucent	France	Fiber connectivity	Fiber backhaul	
Fujitsu	Japan	Edge devices, systems integration		
NEC	Japan	Network equipment		
NTT	Japan	Edge devices		
Panasonic	Japan	Edge devices		

Source: Eurasia Group

The breakdown of frequency preferences is as follows: China favors using low frequencies for core communications and high frequencies as supplemental, while the US prefers the opposite approach. Some carriers prefer a 28-gigahertz band that is not part of the original ITU allocation at the 2015 WRC. South Korea appears to support the US position and used a limited suite of 5G applications at the 2018 Winter Olympics at high frequencies (28 megahertz). Japanese players are split, with DoCoMo favoring high frequencies and Softbank low frequencies. The EU is attempting to allocate spectrum for both frequency ranges but must harmonize differing uses of frequency across 27 member states and the UK. All of this means the next WRC is likely to be contentious, because of sensitivities around some of the low frequency bands in the US, for example, which are allocated for military use.

China's rising influence within the ITU and 3GPP on standards and spectrum allocation, and within UN organizations as a whole, has faced criticism, particularly from the US. Last year, of the 57 leadership positions of the 3GPP subgroups (chairman, deputy chairman), China held ten slots, up from eight in 2015. These posts are highly coveted and require election, and it is not surprising that Chinese companies and organizations with substantial experience on 5G issues have expanded their share of the key positions—specifically China Mobile, Huawei, ZTE, and the China Academy of Information and Communications Technology (CAICT). Four of the five Huawei representatives in the working group are not Chinese citizens but were hired by Huawei from leading telecommunications companies.

China's 5G strategy: Seeking first-mover advantage

No country has devoted more effort to preparing the ground for 5G than China. Beijing has made the development and deployment of 5G networks a national priority since the failure of Chinese standards-setting efforts around 3G and 4G. In 2013, the Ministry of Industry and Information Technology (MIIT), the National Development and Reform Commission (NDRC), and the Ministry of Science and Technology (MOST) established the IMT-2020 5G Promotion Group to push an all-government all-industry alliance on 5G. IMT-2020, a term coined by the ITU, refers to the International Mobile Telecommunication system (or 5G), with a target date of deployment in 2020. The Promotion Group effort includes collaborative work with the EU, Japan, the US, and South Korea.

All of the top players in the Chinese telecom ecosystem participate in the work of the Promotion Group: major research institutes under the MIIT such as the CAICT; Beijing University of Posts and Telecommunications; the Chinese operators, China Mobile, China Telcom, and China Unicom; infrastructure equipment makers Huawei and ZTE; and mobile device makers such as Oppo and Vivo. Broad participation provides a unified platform for Chinese contributions to the 3GPP process. More importantly, the Promotion Group is a venue for planning China's strategy for rapidly deploying standalone 5G networks at scale.

The country's 5G technical evaluation efforts are coordinated through one of the leading players in the Promotion Group, the China Evaluation Group (ChEG). ChEG is responsible for organizing and coordinating IMT-2020 technical evaluation tasks among Chinese participants. ChEG will play an increasingly important role as Chinese operators roll out trial networks and evaluate the performance of key portions of the network such as the radio network and core network.

ChEG in the structure of IMT-2020 (5G) Promotion Group

Source: Eurasia Group

In addition, all of China's major technology plans and strategies, including Made in China 2025, prioritize development of 5G technologies and related sectors such as IoT, big data, AI, semiconductors, and advanced manufacturing. Senior leaders such as Premier Li Keqiang frequently point to the importance of 5G for enabling China's economic growth, and key ministries such as the MIIT, the NDRC, and the MOST have issued documents and guidance on 5G development since the formation of IMT-2020. For China, it is all hands on deck.

Beijing's strategy is to enable operators, particularly leader China Mobile, to move quickly to standalone 5G, allowing China to gain valuable time in testing and validating the technology and business models for the advanced applications that SA 5G will enable.

As part of this effort, and in keeping with the state-managed model of "managed competition," it became apparent in mid-2018 that Beijing is considering merging the smaller mobile carriers China Unicom and China Telecom to reduce the substantial infrastructure costs associated with SA 5G deployment, leaving the field to two major players. In August, a variety of media sources indicated that senior officials were considering the merger. This was likely being discussed by the new Central Commission for Cybersecurity and Informatization, an inter-ministerial body that oversees the ICT sector in China, as well as the State-owned Assets Supervision and Administration Commission, which oversees state-owned enterprises.

While the discussion of a merger shows how focused Chinese authorities are on the 5G issue, conducting a merger of this magnitude, on the verge of the initial rollout of 5G capabilities, appears to be exceedingly complex and difficult, and it may be abandoned in favor of some type of infrastructure-sharing agreement.

China also appears to be attempting to alter the relationships between operators and application services to ensure that operators can consider early on how to ensure a return on investment for big outlays for new 5G equipment. In a sign of concern over the ability of smaller operators such as China Telecom and China Unicom to handle the investments that will be required for 5G, China's leading internet platform companies Baidu, Alibaba, Tencent, and JD.com, and ride hailing firm Didi Chuxing, agreed last year to take stakes in China Unicom that amount to nearly $12 billion. China Unicom indicated that some portion of the investments will be plowed into its 5G pilot rollouts across China.

The move also suggests that the country's over-the-top (OTT) players will work closely with operators to introduce 5G applications. Baidu, Alibaba, and Tencent all operate cloud services and are investing heavily in AI applications. All are likewise involved in consortia to develop autonomous vehicles, a sector that will require the full deployment of SA 5G and ultra-low-latency communications.

First-mover status brings political benefits

Decisions on 5G deployment in China will be driven as well by political considerations, as China attempts to seize the initiative in proving that 5G networks at low frequencies can be done successfully at scale and at a reasonable cost.

The advantages of first-mover status are twofold: First, success across large networks in China will demonstrate to carriers in other big markets that low frequencies can deliver on performance. This will give China a leg up in promoting its low-frequency approach in places such as the EU, the Middle East, Africa, Southeast Asia, and Latin America, where carriers are likely to be much slower to move to 5G.

Second, for China itself the upside of rapid deployment domestically of SA 5G is huge, since 5G will enable widespread use of IoT applications, smart cities, big data and AI, and upgrades to advanced manufacturing. If China successfully capitalizes on these technologies, its technology giants will also then have a leg up on exporting 5G systems along Belt and Road countries as part of the Digital Silk Road (please see Eurasia Group report: "China's Digital Silk Road to gain traction in 2018," 5 February 2018).

China's 5G timetable: Global alliances with carriers, equipment makers, and large-scale trial networks

The country's 5G strategy also includes pushing domestic 5G players to partner with component suppliers, equipment integrators, handset makers, and national carriers. As Chinese operators

roll out major trial networks, they are doing so in collaboration with a range of industry players across the 5G technology stack.

Government ministries are already conducting 5G trials to certify equipment compliance with performance and other technical standards, with the third phase completed in mid-2018. The MIIT is overseeing these—in particular, the CAICT, in its role as a key technical certifier in the IMT-2020 Promotion Group. In September 2017, the MIIT completed the radio portion of the trials and concluded that the participating carriers had met the ITU performance parameters for 5G in terms of peak data rates. The three leading carriers, along with ZTE, Huawei, Ericsson, and Nokia, all participated, highlighting the collaboration between competitors that has so far marked the development of 5G, but which will come under mounting geopolitical pressures.

Chinese operators each have plans to begin trial 5G networks in 2018, with commercial deployments scheduled for 2019. Each carrier is taking a slightly different approach to the trials, which will be focused on NSA 5G. China Mobile has the most ambitious plans, launching trial networks in five large cities: Wuhan, Hangzhou, Suzhou, Shanghai, and Guangzhou. Plans are already underway to install 500 5G base stations across these cities, and then expand to 12 other smaller municipal markets—but with high numbers of potential users—across the country later in 2018. These trials are designed to test specific uniquely 5G use cases, such as autonomous vehicles, augmented reality/virtual reality (AR/VR), and smart logistics. China Mobile is also taking the lead in developing AI algorithms to manage the 5G network. The China Mobile Research Institute's Center of AI and Intelligent Operation R&D is leading this effort.

China Unicom, meanwhile, plans to test 5G this year in 16 cities, including Beijing, Shenzhen, Tianjin, and Shanghai. Unicom has said it will install 300 5G base stations in Beijing alone in 2018, and it is testing the technology in additional second-tier cities such as Nanjing, Wuhan, Chengdu, Guiyang, Zhengzhou, Shenyang, and Fuzhou. The company has an R&D agreement with Huawei for testing network slicing, specifically for autonomous vehicles, advanced manufacturing, and gaming, using AR/VR applications. Logistics and drones are likely to be part of this effort as well. China Telecom, the smallest mobile player of the three, plans to conduct small-scale pilots in 12 cities, including Shanghai, Suzhou, Chengdu, Lanzhou, Shenzhen, and Xiong'an.

Yangtze River Delta Initiative highlights Beijing's focus on 5G deployment at scale

China's Yangtze River Delta Initiative (YRDI) is an effort to target 5G development within a critical economic region. China Mobile, China Unicom, and China Telecom, as well as infrastructure firm China Tower Corporation, plan to invest $30 billion over the next four years to launch a 5G application network across the region by 2021.

The Yangtze River Delta region includes key tech hub cities within the triangle-shaped region spanning Nanjing, Suzhou, and Hangzhou. It is home to large pools of high-skilled labor, high technology, and innovation, as well as the R&D centers of numerous international firms. The YRDI will also support the national ambitions of a fourth city, Shanghai, which is increasingly eager to become a technology player, with a growing focus and investment in AI, autonomous vehicles, and the IoT.

The Yangtze River Delta is central to President Xi Jinping's Belt and Road Initiative as well. Over the past ten years, the transportation network has expanded as rapidly as the high-speed trains it supports. Its railways, highways, and the Yangtze River waterway are considered essential to linking urban areas surrounding it with Shanghai at the nexus. By 2020, China aims to nearly double the region's contribution to national GDP from 12% to 21%.

However, the YRDI has not been left unscathed by the ongoing US-China trade war. The state-owned telecom companies spearheading the country's 5G efforts rely on critical components, such as semiconductors, from US exporters. The US's recent ban on ZTE nearly drove the firm to the brink of bankruptcy and hindered its ability to supply core technology underpinning information infrastructure. Moreover, a growing number of countries, including the US and Australia, have implemented bans on Huawei and ZTE equipment. This and concerns about the proposed merger of China Telecom and China Unicom have affected the share price and future fundraising ability of state-owned telecom infrastructure provider China Tower. Some of the nearly $7 billion raised during a summer IPO would likely cover part of the budget for the YRDI.

How fast China in general, and China Mobile in particular, will field a full standalone 5G network is not yet clear. China Mobile officials claimed at the World Mobile Congress in Barcelona in early 2018 that their trial rollouts would be geared toward a standalone network, and that they would be designed to test massive MIMO antennas and network slicing. With the standalone standards not yet finalized, China Mobile runs the risk of getting out too far in front, before interoperability issues for standalone are completed in 2020—though some of these can almost certainly be handled via software upgrades.

China Mobile claims it can deploy existing hardware and upgrade software to offer a "pre-commercial" customer experience in the second half of 2019. The carrier is the most financially sound of any global operator, so it may be in a position to seize the baton on standalone 5G. Nonetheless, it still faces a number of financial risks if it moves too rapidly. China Unicom and China Telecom, along with other early adopters such as SK Telecom and NTT DoCoMo, intend to follow the NSA network route initially, with integrated 4G/5G networks, given the high financial bar that will be required to get to full standalone—new base stations, small cells, antennas, and fiber backhaul all raise the cost of deploying SA 5G.

China does have another advantage—companies have already begun building out the fiber backhaul network that will be required for full standalone 5G. China Tower, which builds out mobile radio infrastructure, raised nearly $7 billion in an August IPO in Hong Kong, adding to government resources to facilitate the 5G infrastructure buildout.

The pushback begins: US and allies push country-of-origin limitations on 5G equipment

In late August, the Australian government formally issued a document that will restrict the use of Huawei and ZTE equipment for the country's 5G networks. This was the first official ban of this type and the first salvo in what will be an ongoing effort by the US and allies globally to essentially ban Chinese equipment from both the core and RAN segments of 5G. The Australian government press release issued in August does not mention Huawei explicitly, but the inference is clear. Industry insiders fully expected that Huawei would not be part of any core network component discussion of 5G for Australia, but it was far less clear that they would also be banned from the RAN. However, the official statement spells this out explicitly and is consistent with what equipment makers—and almost surely US government officials internally to allies—have been saying about 5G networks: The boundaries between core and radio network are so blurred in 5G that physical and logical separation is not possible or indeed meaningful.

There are signs of pushback elsewhere. The chief of the UK's signals intelligence service in mid-August warned that the deployment of new technologies creates risks for states in terms of "terrorists, hostile states, and serious criminals." Jeremy Fleming, director of the Government

Communications Headquarters (GCHQ), pointed specifically to the coming age of 5G connectivity as a concern. Fleming singled out China as a significant threat in this regard, advocating that security must be baked into new technologies, especially for protecting personal information.

Fleming is the latest senior European government official to call for a rethink of reliance on a small number of equipment providers—specifically, Chinese companies such as Huawei and ZTE—to build 5G networks that will support a range of critical infrastructure sectors when they begin to roll out next year. Officials across Europe are now calling for both stricter security requirements on companies that supply critical infrastructure operators and new measures to restrict investments from countries such as China in advanced technology sectors.

Chinese equipment suppliers' 5G market in the EU is beginning to look shaky. Though the UK has tested Huawei equipment and software for mobile networks in a joint testing center overseen by Fleming's GCHQ, his statement is another sign that the UK is having second thoughts about this approach and about the participation of Chinese firms in building next-generation networks. In March, the top UK cybersecurity agency said it would continue working with Huawei despite repeated allegations by US intelligence officials that the company's equipment poses risks to national security. Comments by an official from the UK National Cyber Security Centre, an arm of GCHQ, concerned the joint center set up in 2010 dedicated to uncovering bugs and security threats in the company's networking equipment and software. The Huawei Cyber Security Evaluation Centre (HCSEC) is staffed by Huawei-employed technicians with top-secret security clearances and overseen by a board consisting of senior UK government and telecommunications industry officials, including from GCHQ.

Prime Minister Theresa May is apparently wary of Huawei because of its opaque shareholder structure and its founder's military ties. With concerns about Huawei never fully resolved, keeping the HCSEC arrangement in place at least for now may reflect a desire to keep Huawei inside the tent, where security risks can be better monitored and controlled. But Fleming's statement suggests that the current arrangement may not work for 5G, and the UK will instead opt to limit or ban Chinese equipment suppliers from next-generation networks—a huge move given Huawei's inroads into the supply chains of UK operators. The decision almost certainly reflects new pressure from US officials, as the US shores up legislation and administrative action of its own geared toward excluding Chinese firms from the US 5G network.

In July, a Huawei 5G project in the Netherlands involving the port of Rotterdam came under fire from parliamentarians concerned about cybersecurity threats to critical infrastructure. One lawmaker has called for establishing standards to determine which companies would be eligible to supply equipment for critical infrastructure networks—he hopes that some EU countries would agree on this approach. If the UK takes more formal steps in the near term against Chinese companies operating in the country, as Australia has now done, this would send a major signal to the rest of Europe, and it could prompt other leading countries to follow suit.

The EU will almost certainly remain split among member states on the issue. In October, Huawei and German officials announced that a new joint lab would be opened in mid-November to facilitate source code reviews. The German Federal Office of Information Security will be involved along with other regulatory organizations. The 5G market in Germany will be one of the largest given the country's emphasis on advanced manufacturing, and this accounts for Huawei's willingness to establish the new facility.

German officials are being careful in characterizing the potential threat to national security—in October, the interior ministry told the Bundestag that there was no legal basis for excluding foreign telecom firms from the country's 5G networks, and that no efforts were being considered by the executive branch. Huawei is likewise actively courting local German governments,

particularly in key states such as North-Rhine Westphalia, and is already collaborating with Duisburg on a smart city project—Duisburg also happens to be a main European endpoint for China's Belt and Road Initiative.

US: Focus on blocking China while removing regulatory hurdles for private firms

Over the past two years, there has been significant discussion within the US intelligence and defense communities about how to ensure a secure US 5G network can be built without Chinese equipment. A leaked proposal in January, from a senior "National Security Council official" and outlined in documents obtained by Axios, was sufficiently advanced to reflect input from several Western technology companies and some US allies. The proposal called for the US to launch a crash program to build a next-generation 5G network within three years. US officials such as Federal Communications Commission (FCC) Chairman Ajit Pai ridiculed any suggestion that the government would own and operate 5G networks.

In the meantime, throughout 2018, the US has taken formal steps that bar Chinese firms from participating in US 5G networks. These include the FCC barring rural telecom carriers from using the Universal Service Fund to purchase equipment from companies of "national security concern" as well as the ZTE Amendment of the National Defense Authorization Act, which places limitations on government contractors in dealing with this type of company. None of the legal measures names Chinese firms explicitly, but the term "of national security concern" is a stand-in for Huawei and ZTE.

The final blow will be a legal instrument that amounts to a formal barring of Chinese firms from providing equipment to Tier 1 US carriers. A new executive order, long in the works, would give the Commerce Department powers under the International Economic Emergency Powers Act to develop a list of suppliers banned from participating in US 5G networks. The executive order will likely be issued before the end of 2018 or in early 2019.

One potential downside of the China-exclusion approach being pursued by the US and like-minded allies is that it is not yet clear whether a coalition of non-Chinese infrastructure vendors could be assembled to provide the full spectrum of 5G infrastructure equipment—base stations, smaller cells and other pieces of the radio access network, antennas, data centers, operations software including AI, fiber backhaul, and other equipment—in a cost-effective and timely manner.

Hints of where broader industry trends on 5G are headed began emerging in October with the announcement of two new alliances that are likely to be important to developing an alternative 5G ecosystem that limits Chinese company participation. Both alliances feature Japanese firms joining the fray. In mid-October, Samsung and Japan's NEC announced they would jointly develop 5G base stations. The two firms plan to split the development efforts, with Samsung focused on high-frequency bands and NEC on lower frequencies. In addition, Ericsson last month announced a tie-up with Fujitsu to deliver end-to-end solutions for 5G networks and related services.

A White House 5G summit held in late September reaffirmed that the US position would be to let companies and market demand drive the introduction of 5G networks in the US. The FCC issued an action plan focused on freeing up and auctioning high-, mid-, and low-band spectrum, infrastructure policy designed to reduce regulatory obstacles to deploying cellular infrastructure, and modernizing outdated regulations covering critical issues such as backhaul for 5G. Some of the speakers addressed the issue of banning vendors from participating in the context of the need to secure supply chains, and hinted that simply banning equipment was not necessarily the best approach. In October, Trump signed a presidential memorandum directing the Commerce Department to devise a national strategy governing spectrum to begin preparing for 5G deployment.

5G applications and use cases: US innovation vs Chinese knowhow

Beyond the political fight over the 5G network itself, the US and China are competing to develop innovative applications that will run on top of deployed 5G networks. Applications such as driverless cars, advanced factory automation, and smart cities will likely be the biggest source of long-term economic and political leverage from 5G. Here the US has an advantage in terms of innovation capacity and light regulatory touch, but China is likely to gain an edge in applications and use cases as first mover.

However, any initial advantage China may gain is likely to be offset by the considerable differences between the ways the two markets function. A US 5G sector driven by competition that drives investment will give rise to rapid innovation and experimentation. China's tech ecosystem has shown increased ability to innovate on mobile platforms, but the tendency for heavy regulatory measures and a more top-down approach is likely to slow the pace of innovation in 5G applications that require complex systems design. In major sectors enabled by 5G such as autonomous vehicles, the differing regulatory systems and driving environments will mean that no one company in either country is likely to gain a decisive competitive edge. There are likely to be many winners in 5G, and US firms will be among the leaders in both 5G technology deployment and 5G-enabled applications despite China's first-mover advantage in deploying standalone networks.

Media-generated raw comparisons of progress on 5G between China and the US will become more common in the coming months but are not always accurate. Whereas China may have a much higher density of mobile cellular sites, there are many other factors that are important in assessing 5G progress. In the US, long experience with shared cell sites means that multiple carriers can use a site and provide a range of services. In addition, investment in network buildout is driven by private sector companies in an efficient and rapid manner, particular as regulatory barriers are reduced, such as the FCC efforts to reduce roadblocks to local installation of smaller cells.

Conclusion: Third countries face difficult choices

De-globalization of global technology supply chains as a result of the US-China tech cold war could further slow the development of a China-free 5G alternative and related applications. As US trade pressure leads foreign companies to move supply chains out of China, it will raise the cost of both components and assembled products. The additional logistics and capital outlays required to create new supply chains will divert funds that would otherwise be available to new product development.

There could even be some limited interoperability uses—for example, around low- vs high-frequency bands if the US and China push ahead with separate spectrum strategies. Device makers are used to developing edge units that can handle multiple frequencies, but a split market of this magnitude would represent a substantial new challenge in determining how to address potentially differing security approaches and carrier requirements. Lower economies of scale and higher transaction costs with second-order effects for the cost of both user and infrastructure equipment will remain the most likely result of a split into China and non-China camps.

A bifurcated 5G ecosystem would force third countries—and developing markets in particular—to make some tough choices. Many countries more sensitive to cost will probably opt to go with Chinese equipment. While they are likely to come under pressure from the US and allies to avoid dependence on China for 5G over time, China's lower-cost and equal or

higher-performance offering is likely to maintain serious appeal, particularly if bundled with other enticements as part of the Belt and Road or similar infrastructure initiatives.

With the first true use cases set to begin testing next year, and China racing to begin the first commercial deployments of 5G networks in 2020, the geopolitics of next-generation networks will continue to pose challenges for industry participants, governments, and markets into 2019 and beyond.

The authors thank Eurasia Group Researcher Clarise Brown for her assistance in preparing this report.