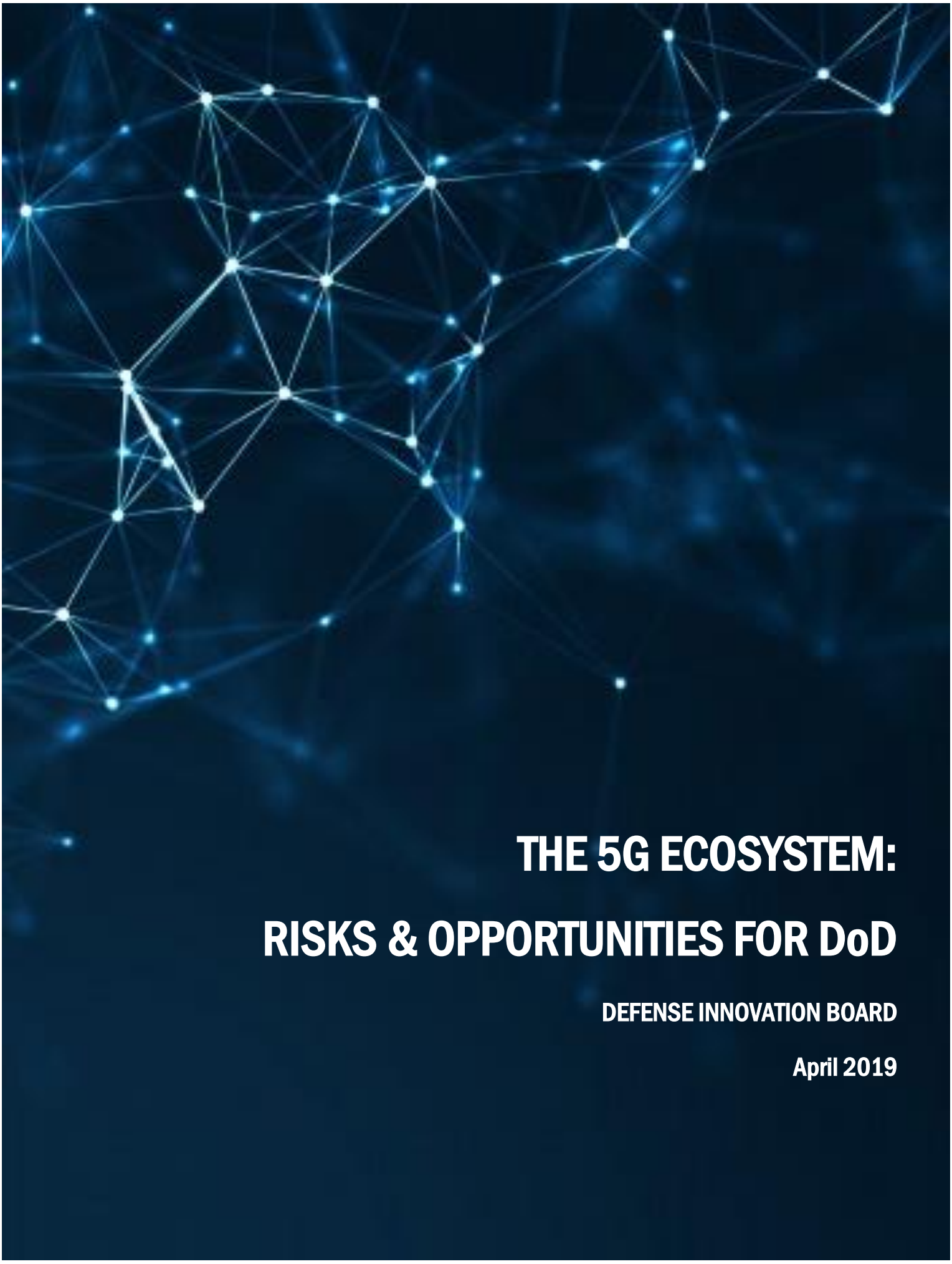


THE 5G ECOSYSTEM:

RISKS & OPPORTUNITIES FOR DoD

DEFENSE INNOVATION BOARD

April 2019

The 5G Ecosystem: Risks & Opportunities for DoD

Defense Innovation Board, 3 April 2019

Coauthors: Milo Medin and Gilman Louie

TABLE OF CONTENTS

Executive Summary

The term “5G” refers to the oncoming fifth generation of wireless networks and technology that will produce a step-change improvement in data speed, volume, and latency (delay in data transfer) over fourth generation (4G and 4G LTE) networks. 5G will enable a host of new technologies that will change the standard of public and private sector operations, from autonomous vehicles to smart cities, virtual reality, and battle networks. Historical shifts between wireless generations suggest that the first-mover country stands to gain billions in revenue accompanied by substantial job creation and leadership in technology innovation. First movers also set standards and practices that were then adopted by subsequent entrants. Conversely, countries that fell behind in previous wireless generation shifts were obligated to adopt the standards, technologies, and architectures of the leading country and missed out on a generation of wireless capabilities and market potential.

In the early 2010’s, AT&T and Verizon rapidly deployed LTE across the United States on the 700 Megahertz (MHz) spectrum they won at auction in 2008. Building on this deployment, the United States became the first country (after Finland) to see a comprehensive LTE network that delivered approximate 10x the consumer network performance of then-existing 3G networks. This step-change in performance drove rapid adoption of new handsets with new semiconductors that not only could move much more data, but were also computationally much faster. U.S. companies like Apple, Google, Facebook, Amazon, Netflix, and countless others built new applications and services that took advantage of that bandwidth. As LTE was deployed in other countries, those same handsets and applications spread across the world. This initiative helped drive global U.S. dominance in wireless and internet services, and created a U.S.-led wireless ecosystem on which the Department of Defense (DoD) and the rest of the world has operated for nearly a decade.

Since the rollout of LTE, these wireless competitive landscape has undergone many changes. Chinese telecommunications equipment giant Huawei grew global revenues from approximately $28B in 2009 to $107B in 2018, while other traditional market leaders like Ericsson and Nokia have declined in revenue over that same period. Chinese handset vendors like Huawei, ZTE, Xiaomi, Vivo, and Oppo have rapidly grown in global market share, and are still growing rapidly in adoption and influence despite minimal sales in the U.S. market. In 2009, all of the top 10 Internet companies by revenue were American. Today, four of the top 10 are Chinese. These trends are already in effect, and 5G has the potential to skew future networks even further in the direction of China if it continues to lead.

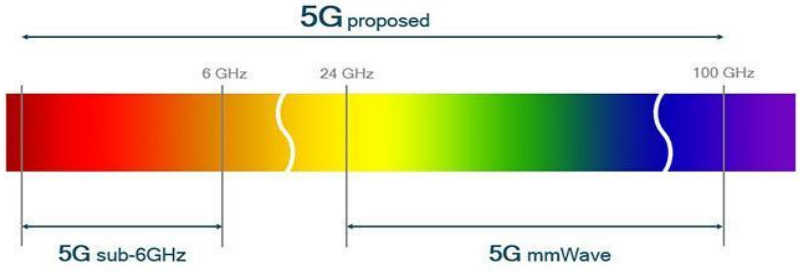
The shift from 4G to 5G will drastically impact the future of global communication networks and fundamentally change the environment in which DoD operates. While DoD will feel the impact of 5G, the rollout itself will be driven by the U.S. commercial sector. This study provides insight into the commercial landscape as well as the DoD landscape to give a comprehensive view of the stakeholders and future of 5G.

5G has the ability to enhance DoD decision-making and strategic capabilities from the enterprise network to the tactical edge of the battlefield. 5G will increase DoD’s ability to link

multiple systems into a broader network while sharing information in real time, improving communication across Services, geographies, and domains while developing a common picture of the battlefield to improve situational awareness. This improved connectivity may in turn enable a host of new technologies and missions, from hypersonics and hypersonic defense to resilient satellite constellations and mesh networks.

Spectrum will play a key role in the operation, development and roll-out of 5G. Peak data rates are driven by the amount of spectrum that is available to a wireless service. In 4G, up to five 20 MHz channels can be bonded together. But in 5G, up to five 100 MHz channels can be bonded together, enabling speeds approximately 20x faster than 4G and 4G LTE. While some 5G technology will be deployed in the currently-used cellular spectrum and achieve modest gains in performance (LTE is already fairly well optimized), full 5G development will require significantly more spectrum to provide another step-change improvement in performance for consumers, DoD or otherwise.

Countries are pursuing two separate approaches to deploy hundreds of MHz of new spectrum for 5G. The first focuses on the part of the electromagnetic (EM) spectrum below 6 GHz ("Low- to Mid-Band Spectrum," also referred to as "sub-6"), primarily in the 3 and 4 GHz bands. The second approach focuses on the part of the spectrum between ~24 and 300 GHz ("High-Band Spectrum," or "mmWave"), and is the approach taken by the United States, South Korea, and Japan (although all three countries are also exploring sub-6 to various degrees). U.S. carriers are primarily focused on mmWave deployment for 5G because most of the 3 and 4 GHz spectrum being used by the rest of the world for 5G are exclusive Federal bands in the United States, extensively used by DoD in particular.



The question of spectrum allocation is at the heart of the 5G competition, for the spectrum band of choice, whether sub-6 or mmWave, impacts nearly every other aspect of 5G development. Spectrum bands in the 3 and 4 Ghz range dominate global 5G activity because of improved propagation (range) over mmWave spectrum, resulting in far fewer base stations needed to be deployed to deliver the same coverage and performance. Because large swaths of the sub-6 bands in the United States are not available for civil/commercial use, U.S. carriers and the FCC (which controls civil spectrum in the US) are betting on mmWave spectrum as the core domestic 5G approach.

U.S. carriers may continue to pursue mmWave, but it is impossible to lead in the 5G field without followers. Leadership in wireless networks requires the global market to subscribe to

and build to the specifications of the leader's spectrum bands of choice, as these 5G subcomponents and products will ultimately drive interoperability across networks. The rest of the world does not face the same sub-6 spectrum limitations as U.S. carriers, and is subsequently pursuing 5G development in that range. As a result, the United States may find itself without a global supply base if it continues to pursue a spectrum range divergent from the rest of the world.

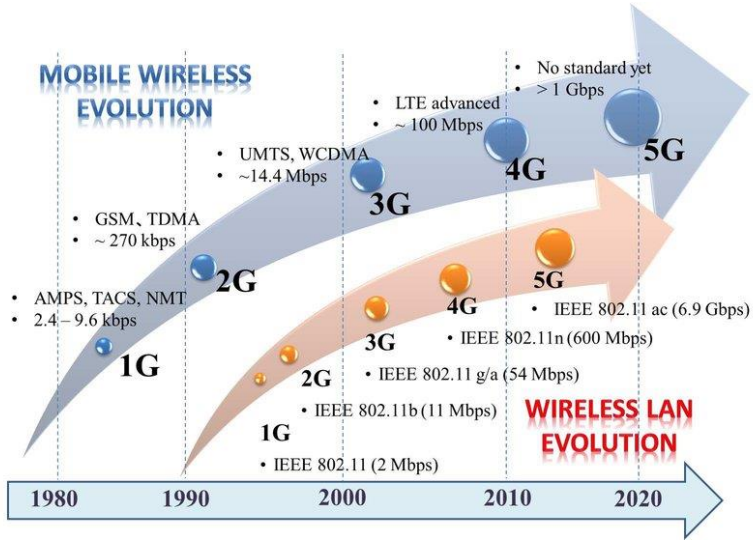
If the future 5G ecosystem adopted by most of the world is built on the sub-6 mid-band spectrum, the United States will also be faced with mmWave device interoperability challenges and sub-6 infrastructure security concerns. As sub-6 becomes the global standard, it is likely that China, the current leader in that space, will lead the charge. This would create security risks for DoD operations overseas that rely on networks with Chinese components in the supply chain. Even if the United States were to restrict use of Chinese equipment suppliers domestically, the United States is not a big enough market in wireless to prevent China's 5G suppliers from continuing to increase market share globally, resulting in significant pressure on a declining set of vendors that would serve the U.S. market. These vendors will in turn be unable to invest R&D towards future 5G offerings due to decreasing market share, limiting the number of competitive products and depriving DoD and U.S. industries of better and cheaper global supply chains.

China plans to deploy the first widespread 5G network, with its first set of sub-6 services becoming available in 2020. First-mover advantage will likely drive significant increases in their handset and telecom equipment vendors market along with their domestic semiconductor and system suppliers. As a result, Chinese internet companies will be well-positioned to develop services and applications for their home market that take advantage of 5G speed and low latency. As 5G is deployed across the globe in similar bands of spectrum, China's handset and internet applications and services are likely to become dominant, even if they are excluded from the US. China is on a track to repeat in 5G what happened with the United States in 4G.

CHAPTER 1: 5G HISTORY AND OVERVIEW

A History of Generation Technology

Mobile wireless technology has been in development for decades, with the first generation (1G) introduced in the late 1970s and fielded in the early 1980s. Since then, new generations of technology and wireless standards have been introduced every decade or so, culminating in our present state of transition between 4G and 5G capabilities. The value of each generation has increased exponentially, as each has enabled a host of other technology advancements across the commercial sector and military. All existing generations work within the low- to mid-band spectrum (less than 6GHz, or sub-6), but 5G has opened the door for millimeter wave (mmWave) spectrum use as well.



1G (Voice Calls): 1G mobile networks were fielded in the early 1980s with voice communications and limited emphasis on data transfer capability (early capability ~2.4 Kbps). 1G networks utilized analog signals to "hand off" cell users between a network of distributed base stations (hosted on cell towers) using standards like AMPS and TACS.

Source: https://www.researchgate.net/figure/Wireless-technology-evolution_fig1_322584266

2G (Messaging): In the 1990s, 2G mobile networks spawned the first digitally-encrypted telecommunications that improved voice quality, data security, and data capacity, while hosting limited data capability by way of circuit-switching using the GSM standard. In the late 1990s, 2.5G and 2.75G technology brought about improved data rates (upwards of 200 Kbps) using GPRS and EDGE standards, respectively. These later 2G iterations introduced data transmission via packet-switching, which served as a stepping-stone to 3G technology.

3G (Limited data: multimedia, text, internet): The late 1990s and early 2000s introduced 3G networks with faster data transfer speeds by fully transitioning to data packet-switching, with some voice circuit-switching that had been standard for 2G. This enabled data streaming, and in 2003 the first commercial 3G service was launched with mobile internet access, fixed wireless access, and video calls. 3G networks have now increased data speeds to 1Gbps when stationary and upwards of 350Kbps when mobile, using standards such as UMTS and WCDMA.

4G and LTE (True data: dynamic information access, variable devices): 4G network services were introduced in 2008 and featured data transfer at 10 times the speed of 3G by leveraging

all-IP networks and relying entirely on packet-switching. 4G networks enhanced the quality of video data due to larger bandwidths allowing for increased network speed. The introduction of the LTE network has since set the standard for high-speed wireless communications on mobile devices and data terminals. LTE is in constant evolution, and is currently on release number 12. "LTE advanced" can support ~300 Mbps.

5G: 5G's precise capabilities and extent of adoption are still to be determined. The speed, volume, and latency of data transfer will depend on the spectrum bands used, as well as the context of network usage (fixed or mobile). For example, a mmWave 5G network could enable incredibly fast speed for fixed local area networks under specific conditions that did not limit wave propagation, but would conversely struggle to maintain those speeds at extended range (on the "cell edge"). A sub-6 5G network might have lower maximum speed than mmWave, but could cover a much broader area without risk of interruption from a range of environmental factors. These conditions will ultimately determine the "standards" for 5G, and are currently in development globally.

History's Lessons: First-Mover Advantage in Generation Transitions

Transitions between wireless technology generations before 5G also had substantial commercial, competitive, and security implications for first-movers. Europe, led by Germany, gained first competitive advantage in 2G, and as a result companies like Nokia and Ericsson were able to roll out more advanced devices earlier and were already transitioning to 3G in the 2000s when the United States was still trying to implement 2G. The European wireless tech industry boomed during this period while U.S. companies struggled to keep pace. Europe lost this edge during the 3G transition, when they were hampered by regulations that required time-consuming auctions of 3G spectrum, rather than simply repurposing existing 2G spectrum bandwidth. Japan took the lead on 3G, and while the United States ultimately caught up to Japan, it took years to roll out 3G networks, which came at a huge cost to U.S. businesses as Japan sprinted forward with its 3G business model. The United States lost thousands of jobs and considerable revenue during this transition, during which multiple wireless technology companies failed or were absorbed into foreign companies.

The United States learned from its previous mistakes when it came to 4G and 4G LTE. Although it had been slow to implement 3G, there was a surge in 3G investment in the later years that ultimately gave the United States a head start when 4G arrived. Additionally, the FCC opened licenses for more bandwidth and set regulations to promote rapid expansion of the 4G network as it was being developed. Japan kept pace at first, but Japanese industry failed move quickly to develop the technology that would ultimately shape the 4G ecosystem. As a result, the United States took an early lead in the smart device market and ultimately displaced Japanese operating systems both in and out of Japan.

In the early 2010s, AT&T and Verizon rapidly deployed LTE across the United States in the 700 MHz spectrum they won at auction in 2008. The United States became the first country (after Finland) to see a comprehensive LTE network that delivered approximately 10x the consumer network performance of existing 3G networks. This step-change in performance drove rapid

adoption of new handsets with new semiconductors that not only could move much more data, but were computationally much faster as well. U.S. companies like Apple, Google, Facebook, Amazon, Netflix, and countless others built new applications and services that took advantage of that bandwidth and those new handset capabilities. As LTE was deployed in other countries, those same handsets and applications spread across the world, driving U.S. dominance in global wireless and internet services.

The United States has benefited significantly from this lead. Recon Analytics published a report in April 2018[1] estimating that the introduction of 4G contributed to 70% growth in the wireless industry between 2011 and 2014, bolstering GDP while increasing jobs in the wireless industry by over 80%. By leading the charge on 4G, the United States was able to build a global ecosystem of network providers, device manufacturers, and app developers that shaped the future of 4G and the experience of all other countries implementing it.

First-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products. For example, China is in the process of laying down fiber optic cables in its own territory and plans to do the same for the countries participating in its Belt and Road initiative, in addition to building 5G networks throughout Europe. This will allow China to selectively grant access to certain 5G companies and products to ride on that infrastructure.[2] China is using this opportunity to promote sub-6 spectrum usage, which will shape the entire 5G product market going forward. If companies want to sell their 5G products into China or into any network with Chinese sponsorship, they will have to build to Chinese preferred specifications and partner with Chinese companies. This increases the risk of product backdoors and vulnerabilities throughout the supply chain.

The shift to 5G will carry the same potential risks and rewards as previous generational transitions, but at an even larger scale. The leader of 5G stands to gain hundreds of billions of dollars in revenue over the next decade, with widespread job creation across the wireless technology sector. 5G has the potential to revolutionize other industries as well, as technologies like autonomous vehicles will gain huge benefits from the faster, larger data transfer. 5G will also enhance the Internet of Things (IoT) by increasing the amount and speed of data flowing between multiple devices, and may even replace the fiber-optic backbone relied upon by so many households. The country that owns 5G will own many of these innovations and set the standards for the rest of the world.

For the reasons that follow, that country is currently not likely to be the United States.

---

[1] "How America's Leading Position In 4G Propelled the Economy," Recon Analytics, 16 April 2018, https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.

[2] Susan Crawford, "China Will Likely Corner the 5G Market - And the US Has No Plan," *Wired*, 20 February 2019, https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/.

Spectrum Use and Options

Spectrum use and availability are the most important factors in fielding a viable 5G network, as they will determine the speed, volume, and latency of data transfer going forward. 4G data transfer capabilities cannot keep pace with current demand, and the 5G step-change would address the increasing rate of data consumption by fielding a functioning 5G network using mmWave bands, sub-6 bands, or both. The following sections describe the relative strengths and weaknesses of mmWave and sub-6 approaches, as well as their potential applications and roles in a future 5G ecosystem.

Millimeter Wave (mmWave)

MmWave spectrum operates in high frequencies found between 30 GHz and 300 GHz, and is attractive for a number of reasons. First, the shorter wavelengths of mmWave create narrower beams, which in turn provide better resolution and security for the data transmission and can carry large amounts of data at increased speeds with minimal latency. Second, there is more mmWave bandwidth available, which improves data transfer speed and avoids the congestion that exists in lower spectrum bands (prior to researching potential 5G uses of mmWave frequencies, the only major operators in that area of the spectrum were radar and satellite traffic). A 5G mmWave ecosystem would require a significant infrastructure build, but could reap the benefits of data transferred at up to 20x the speed of current 4G LTE networks. Finally, mmWave components are smaller than components for lower bands of the spectrum, allowing for more compact deployment on wireless devices. Outside of its physical properties, MmWave is also attractive to U.S. 5G developers because the U.S. government owns large swaths of the sub-6 spectrum, particularly in the 3 and 4 GHz range, making it difficult for carriers to purchase dedicated spectrum licenses at FCC auctions or even to share that part of the spectrum.

However, mmWave has its share of challenges. While its short wavelengths and narrowness of its beam allow for improved resolution and security of data transfer, these qualities can also restrict the distance at which mmWaves can propagate. This creates a high infrastructure cost, as a mmWave network would require densely populated base stations throughout a geographic area to ensure uninterrupted connectivity. This challenge is further aggravated by the fact that mmWaves can be easily blocked by obstacles like walls, foliage, and the human body itself. MmWave spectrum can achieve extended range in specific circumstances, such as in large buildings with flat reflective windows above the tree line, but few environments in the United States are conducive to this type of propagation.

Various studies have begun to test the efficacy of mmWave and sub-6 infrastructure builds in the United States. MoffettNathanson LLC recently conducted an analysis of Verizon's 5G mmWave efforts in Sacramento and discovered that after roughly six months in the market, Verizon's ~150 fixed wireless broadband (FWBB) base stations can only offer service to around 6% of residential addresses in the tested areas.[3] Verizon has been targeting particularly dense

[3] Craig Moffet, Ray McDonough and Jessica Moffet, "Fixed Wireless Broadband: A Peek Behind the Curtain of Verizon's 5G Rollout," p. 7, MoffetNathanson, March 20, 2019, https://www.moffettnathanson.com/?Section=Media%20/Telecom.

parts of Sacramento as optimal testing environments and is focused on developing a fixed network, which carries fewer challenges for mmWave deployment than a mobile network. However, even in these optimized circumstances it is clear that scaling this solution to provide more coverage would be a time- and cost-intensive endeavor requiring a massive infrastructure build-out.

Google also performed a preliminary study for the Defense Innovation Board to ascertain the approximate capital expenditure (capex) and base station counts needed for mmWave deployments, using 425 MHz of spectrum at 28 GHz (a mmWave configuration standard for current U.S. 5G trials), compared to 250 MHz of spectrum in the 3.4 GHz band (a sub-6 configuration, standard for Chinese 5G trials and deployment). This equipment was deployed on 72,735 existing macrocell towers and rooftops (the easiest choice for deployment) and was found to provide mmWave coverage to only 11.6% of the U.S. population at cell edge speeds of 100 Mbps, with 3.9% coverage at 1 gigabit. For sub-6, the same tower sites covered 57.4% of the population at 100 Mbps, and 21.2% of the population at 1 Gbps. The study used high-resolution geospatial data that included shadowing from foliage structures, but did not take into account shadowing from the human body or a vehicle, which realistically would exist in a deployed environment and even further disrupt connectivity for mmWave networks.

Most operators are looking at deploying mmWave 5G sites on utility poles, given the poles' ease of accessibility and abundance. Using a database of utility poles in the United States, the study indicated that it would require approximately 13 million pole-mounted 28-GHz base stations and $400B dollars in capex to deliver 100 Mbps edge rate at 28 GHz to 72% of the U.S. population, and up to 1 Gbps to approximately 55% of the U.S. population. Figures 1 and 2 below show the difference in "splat" (propagation) between 28 GHz (mmWave) and 3.4 Ghz (sub-6) deployments on the same pole height in a relatively flat part of Los Angeles (blue represents 100 Mbps speed, red represents 1 Gbps speed):

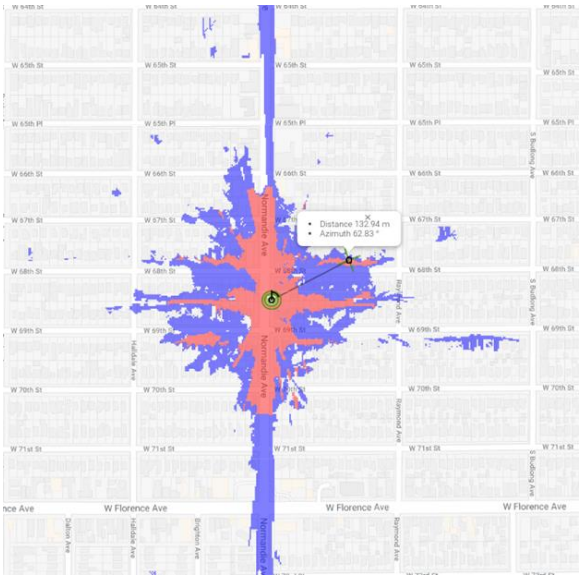


Figure 1: "Splat" chart with mmWave propagation

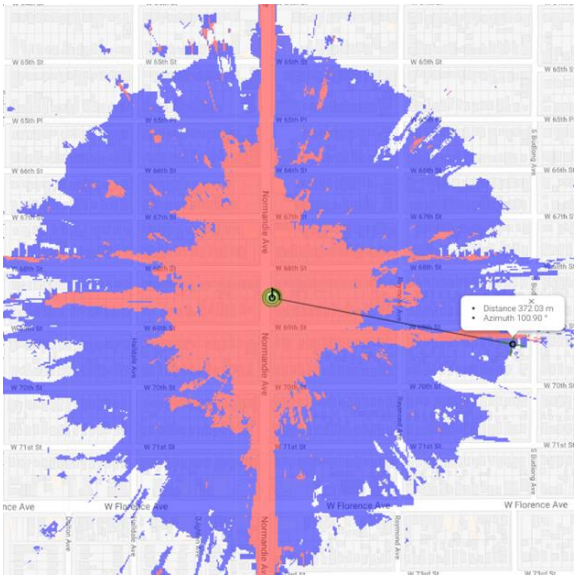


Figure 2: "Splat" chart with sub-6 propagation

There are ongoing efforts to mitigate these physics challenges, such as massive MIMO (multiple-input, multiple-output) and beamforming. Massive MIMO is an antenna array that will greatly expand the number of simultaneous connections and throughput, and will give base stations the ability to send and receive signals from many more users at once and increase the capacity of networks significantly, assuming multiple RF paths to users exist. Beamforming is a technique for identifying the most efficient data-delivery route to a particular user and reducing interference for nearby users in the process. These options can improve the propagation of mmWaves, but challenges remain with maintaining connectivity across a broader area using this part of the spectrum. Significant time and R&D will have to be devoted to solving the mmWave propagation problem before it can be deployed as a more universal wireless network solution.

Sub-6

Sub-6 includes the range of spectrum below 6 GHz. Sub-6 can provide broad area network coverage with lower risk of interruption than mmWave due to its longer wavelength and greater capacity to penetrate obstacles. It therefore requires less capex and fewer base stations, as compared to mmWave. This, together with the ability to leverage existing 4G infrastructure, makes sub-6 the lower hanging fruit for a potential 5G sub-6 ecosystem. Faster time-to-rollout is particularly important given the speed at which China is pushing forward. While mmWave may ultimately be deployed in specific environments where its propagation and cost challenges are not prohibitive, sub-6 will likely provide the broader solution for more wide area 5G coverage in the near term. This in turn will drive product design and manufacturing for the 5G supply chain, given the larger quantity of equipment that will feed that sub-6 network.

Maximizing the potential of 5G requires hundreds of consecutive MHz of bandwidth in order to optimize performance, and the sub-6 spectrum is already crowded with existing systems and uses. In the United States, sub-6 5G technologies will likely be deployed in existing macrocell networks and infrastructure through existing LTE spectrum. This would give modest improvements to RF system performance, but would not yield a 10x performance improvement over modern versions of LTE operating in the same spectrum. This failure to deliver the same disruptive speed improvements that LTE had over 3G would mute the impact of 5G deployment in the United States.

An additional challenge in the United States is that the government owns large portions of the sub-6 spectrum and limits commercial access to them. It is possible to relocate Federal users or share these bandwidths to allow commercial sector to develop 5G capabilities on them, but both of these processes are time-intensive. The average time it takes to “clear” spectrum (relocate existing users and systems to other parts of the spectrum) and then release it to the civil sector, either through auction, direct assignment, or other methods, is typically upwards of ~10 years. Sharing spectrum is a slightly faster process because it doesn’t require a complete upheaval of existing federal users, but even that has historically taken upwards of five years.

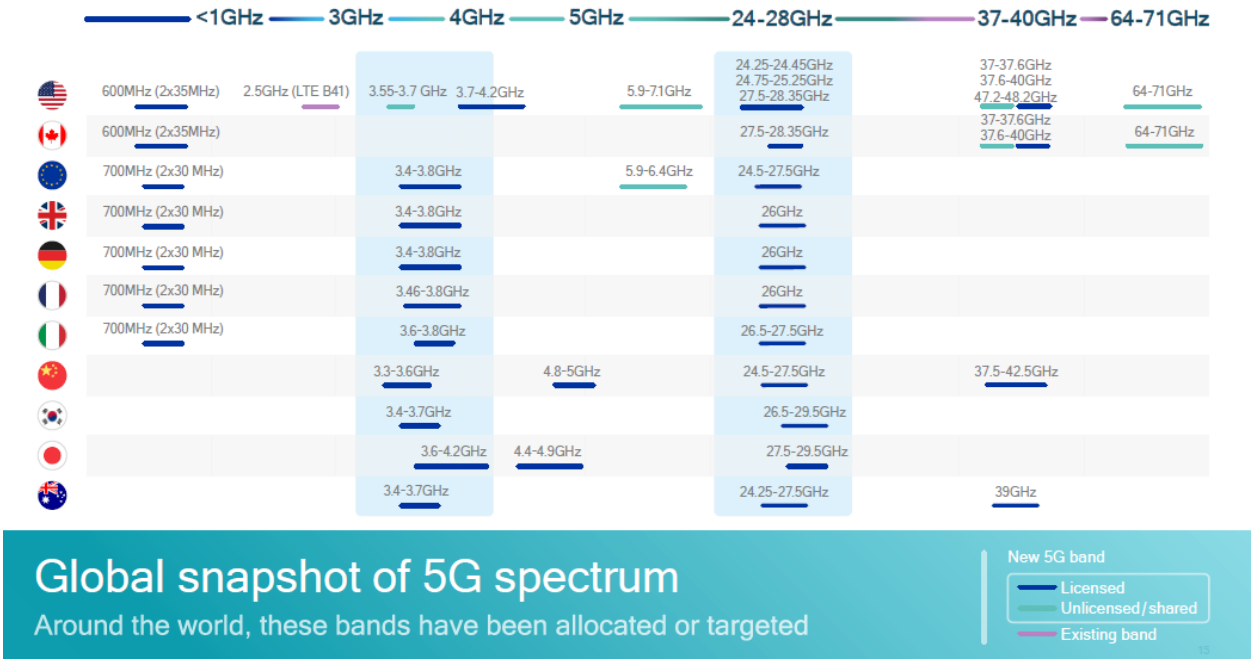
There are also legitimate concerns within DoD that sharing its bandwidths in the sub-6 spectrum will create a number of operational issues, from spectrum optimization to security vulnerabilities.

If DoD operators are forced to share their bands of the spectrum, there is concern that this may reduce the performance of systems. The addition of commercial users would also increase the overall congestion of the sub-6 spectrum, increasing the risk of connectivity interruptions for DoD operators. There is precedent for successful spectrum-sharing - in 2010, the FCC opened up the 3550-3700 MHz bandwidth (known as Citizens Broadband Radio Service, or CBRS) to the commercial sector. However, this process took more than five years, a timeframe that is untenable in the current competitive environment. This paper will explore the CBRS case study in more detail in Chapter 3.

Given these benefits and challenges associated with mmWave and sub-6, the future of 5G may involve some combination of both. Sub-6 is optimized for broad area coverage, which will make up a large part of the network, but mmWave may ultimately be able to provide more exquisite coverage in specific scenarios, and has some distinct military advantages in some topographies by virtue of being harder to intercept. This will require further research and testing in the mmWave spectrum targeting the current physics challenges around propagation, which may in turn lower the capex required for mmWave infrastructure deployment. In the near term, 3 and 4 GHz spectrum will likely serve as the dominant global bands that drive volume in infrastructure and device deployments. In the current state of 5G development and spectrum usage, it is unlikely that the United States will be able to leverage such technology, much less lead the rest of the world in that band of spectrum deployment as it did with 4G almost a decade ago.

CHAPTER 2: CURRENT STATE OF THE 5G COMPETITIVE FIELD

5G capability by country can be compared across five metrics: spectrum availability, widespread 5G trials, 5G roadmaps being established by the national regulator, government commitment (e.g., strategy documents and policies paving the way for 5G implementation), and industry commitment to early 5G launch.[4] Of these metrics, spectrum availability has the largest influence, as many of the other factors are dependent on that availability. For spectrum availability, there is ongoing debate on the merits of sub-6 versus mmWave and how to allocate spectrum in either of those categories, and in the United States there is a larger concern about allocating or sharing government-owned spectrum to the commercial sector. For infrastructure, carriers can take a "non-standalone" approach, which leverages existing 3G and 4G infrastructure as a stepping stone to get to full 5G capability, or a "standalone" approach, which requires a large up-front investment to build out new infrastructure for a 5G network.



Source: https://www.everythingrf.com/community/5g-frequency-bands

China

China has taken the lead in 5G development through a series of aggressive investment and spectrum-allocation initiatives. In addition to investing $180B in capital expenditure for 5G deployment over five years, China assigned 200 MHz of mid-band spectrum to its three state providers and is considering reallocating 500 MHz of C-band spectrum as well.[5] Domestically, China's 5G deployment is being implemented through its major telecommunications companies

[4] David Abecassis, Chris Nickerson and Janette Stewart, "Global Race to 5G - Spectrum and Infrastructure Plans and Priorities," Analysys Mason, April 2018, https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf.

[5] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jefferies, September 14, 2017, https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf.

(China Mobile, China Unicom, and China Telecom). All three are primarily focused on developing a standalone 5G network in China, with plans to deploy pre-commercial application in 2019 and formal commercial application in 2020. China now has ~350,000 5G-operable base stations deployed, which is nearly 10 times as many as are deployed in the United States. Globally, China's large manufacturers (Huawei and ZTE) are pushing 5G deployment through commercial sales of 5G-enabling equipment and devices primarily for non-standalone networks, and Huawei has already shipped upwards of 10,000 base stations overseas.[6]

Overseas, China has been developing partnerships with countries and foreign companies to expand its 5G influence. In Europe, Huawei and ZTE are offering their services to build individual countries' 5G networks, and have signed multiple 5G contracts despite pressure from U.S. officials demanding that allies block Chinese companies. Additionally, China has invested significant time and resources into its Belt and Road Initiative, including a push for Chinese-built network infrastructure to provide connectivity across the length of the route. This strategy has already had some success: in Q3 of 2018, Huawei held 28% share of the global telecommunications equipment market, up four percentage points from 2015.[7] Huawei is expected to continue growing that share as more 5G networks are rolled out relying on Chinese telecommunications equipment. These efforts will allow China to promote its preferred standards and specifications for 5G networks and will shape the global 5G product market going forward.

In aggregate, these approaches have given competitive advantage to China in 5G technology and capability. China's 5G strategy should be viewed in the context of the Chinese Communist Party's (CCP) grand strategy. Like artificial intelligence (AI), 5G development is a crucial component of Xi Jinping's "China Dream" vision and "Made in China 2025" roadmap. Social stability and economic growth are the CCP's top priorities because failures in those two areas are seen as direct existential threats to the regime, and 5G has the potential to transition China from a capital- and labor-intensive manufacturing economy to an innovation-led, consumption-driven economy with reduced dependence on foreign investment. In light of China's slowing growth and its ongoing trade war with the United States, the CCP likely feels pressured to pursue technological advancement initiatives like 5G more aggressively.

**For more detail on China's 5G strategy and capabilities, please see Classified Annex.*

South Korea

South Korea is closely following China in 5G maturity due to its early auction of spectrum and its general commitment to wireless technology. The South Korean government has built a clear roadmap including healthy investment to pursue 5G; in 2014, South Korea committed $1.5B to

[6] Isao Horikoshi and Takashi Kawakami, "Telecom's 5G revolution triggers shakeup in base station market," Nikkei Asian Review, December 25, 2018, https://asia.nikkei.com/Business/Technology/Telecom-s-5G-revolution-triggers-shakeup-in-base-station-market.
[7] Stéphane Téral, "Mobile Infrastructure Market Tracker - Regional," IHS Markit, December 3, 2018, https://technology.ihs.com/597909/mobile-infrastructure-market-tracker-regional-q3-2018.

promote 5G adoption and deployment by 2020, and in 2017, South Korea released its national broadband and spectrum plan ("K-ICT") to further promote 5G.[8] In line with the K-ICT plan, South Korea's Ministry of Science and ICT (MSIT) has since auctioned over 1,000 MHz of spectrum in the sub-6 and mmWave ranges to its three largest telecommunications providers (SK Telecom, KT Corp, and LG Uplus). South Korea has closely partnered with AT&T and Verizon to develop 5G mmWave networks, but has spread its risk in pursuing both sub-6 and mmWave by making its devices functional in both parts of the spectrum (as in the case of its Exynos 5100 5G modem).[9] AT&T is also working with Samsung to release a cell phone with mmWave and sub-6 capabilities at the end of 2019, but these dual-function devices may have less capability in the United States, given the restricted range of sub-6 spectrum available.

South Korea was able to leverage the 2018 Winter Olympics in Pyeongchang to showcase its 5G investment and conduct various network trials. South Korean industry already promotes high-intensity competition for 4G and LTE network technologies, which will fuel further rapid development of 5G. SK Telecom currently leads the field in investment and 5G trials, and was also able to acquire the largest amount of spectrum bandwidth in the 2018 MSIT auction, but all three telecoms providers plan to synchronize their launches of 5G cellular service in early 2019 for "Korea 5G Day." South Korea is well-positioned in the 5G field and will likely continue to be a leader going forward as its major telecoms providers take advantage of their newly-auctioned spectrum bandwidth.

Japan

Japan is following closely behind China, South Korea, and the United States in 5G capability. Japan has not yet auctioned off key parts of its spectrum bandwidth to commercial providers, but has plans to do so in 2019 and is currently developing both mmWave and sub-6 options (mmWave is being applied to limited, densely-populated geographic areas, while sub-6 is being used to cover the rest of the territory). Similar to South Korea, Japan hopes to use the 2020 Olympics in Tokyo to showcase and test 5G technologies and networks, and is driving most of its investment and activity around that 2020 timeline. In 2014, Japan stood up its 5G Mobile Forum (5GMF) to promote 5G research and development, coordinate 5G efforts across organizations, and promote general awareness of 5G.[10] In 2016, Japan's Ministry of Internal Affairs and Communication (MIC) released a strategy document ("Radio Policy to Realize 5G in 2020") that mapped out its commitment to and future deployment of 5G.[11]

---

[8] Lee Kangwook, "South Korean Government to Introduce K-ICT Spectrum Plan," December 23, 2016, http://www.ipnomics.net/?p=16629.
[9] Sean Kinney, "5G modem based on 3GPP Rel. 15, Samsung says," *RCRWireless News*, August 15, 2018, https://www.rcrwireless.com/20180815/5g/samsung-5g-modem-supports-sub-6-ghz-and-millimeter-wave-frequencies.
[10] Kohei Satoh, "Remarks by the 5GMF Secretary General," 5GMF, July 4, 2016, https://5gmf.jp/en/committee/20160704154530/.
[11] Kunko Ogawa, "Radio Policy to Realize 5G in 2020," Ministry of Internal Affairs and Communication (MIC), June 28, 2016, https://www.gsma.com/spectrum/wp-content/uploads/2016/08/MIC_Spectrum-for-5G-MIC-Kuniko-OGAWA.pdf.

Japan's three major telecoms providers (NTT DOCOMO, KDDI, and Softbank) are all in the process of testing 5G technologies with the intention of launching in 2020 before the Olympics. All three companies are conducting trials in the sub-6 and mmWave ranges, and MIC has conducted a "5G System Trial" in Tokyo and rural Japan.

Rest of World (Non-US)

While China, South Korea, the United States, and Japan lead the field, the rest of the world is playing catch-up on 5G deployment. The United Kingdom, Germany, and France can be considered "second tier" 5G developers, while Singapore, Russia, and Canada make up the "third tier," and the rest of the world comes after. These countries are beginning to auction off spectrum bandwidth with varying timelines and volume of spectrum made available, but many lack any formal policies or strategies to enable 5G implementation and most anticipate 5G launches outside of the 2020 timeframe.

Although Europe led the charge into 2G, it has since been hampered by regulations that have limited its ability to rapidly make spectrum bandwidth available, and has continued to lag behind in 3G, 4G, and now 5G. The rest of Asia has made some strides in 5G, but few countries have invested the same time and resources as China, Japan, and South Korea. Russia released its "Digital Economy of the Russian Federation" in 2017 that included a 5G roadmap, but has yet to develop any clear spectrum plan or devote significant resources to that roadmap.[12] Russia used the 2018 FIFA World Cup to launch some of its 5G efforts, but is still highly reliant on foreign 5G technologies and partnerships to move its 5G development forward.

Given the gap in 5G advancement between the first tier and everyone else, the rest of the world will likely be driven to implement the 5G network design and infrastructure of whichever country leads 5G. China is the current leader, and U.S. allies have taken different stances on how to respond to the Chinese drive to set 5G standards. Some are wary of Chinese influence because of security concerns and are actively working to push back on China's 5G roll-out. For example, in December the Czech Republic's cybersecurity agency (NUKIB) issued an official warning that Huawei and other Chinese companies posed a national security risk, citing existing Chinese statutes (*National Intelligence Law*, enacted June 27, 2017)[13] that require Chinese companies to actively cooperate with the intelligence community. This has driven a security review throughout Czech public and private sectors, effectively halting all sales of Huawei 5G goods into the country. Australia and Poland have also taken a hard line against China, and the United States has been heavily pressuring its other allies to follow suit.

---

[12] "The Digital Economy of the Russian Federation," accessed March 20, 2019, http://ac.gov.ru/en/projects/014097.html.

[13] Article 14: "State intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation"; Article 17: "As necessary for their work, the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings." China's *National Intelligence Law,* June 27, 2017.

However, other countries have been less enthusiastic about ousting China from their 5G markets, given the price and quality of China's offerings. Germany has refused to ban Huawei, despite U.S. threats to cut off intelligence-sharing, and the United Kingdom appears likely to take the same approach. Both Germany and the United Kingdom have pushed back on U.S. claims that Huawei and other Chinese telecommunications companies represent an unacceptable risk to national security, claiming that their security organizations could take measures to limit vulnerabilities in their networks. India and Italy have also expressed their hesitancy to exclude Huawei products from their 5G roll-outs, and in recent months New Zealand has eased its initial hard stance against China. In the coming months, Europe will continue to be a battleground for the future of 5G, as it represents one of Huawei's largest markets as well as a major source of U.S. allies. This fight also suggests a more concerning trajectory for the rest of the world's approach to 5G - in particular, developing countries that are more sensitive to cost will find the Chinese 5G price-point difficult to turn down, especially when the offer is sweetened with infrastructure and project-financing incentives like the Belt and Road Initiative.

United States

Private Sector

The telecommunications industry is organizing the effort to develop and deploy 5G in the United States, with increasing support from the U.S. government. Verizon, AT&T, Sprint, and T-Mobile are all developing their own 5G networks and 5G devices, each with their own strategy and method. Verizon and AT&T are focused on developing high-band mmWave networks and are in the process of deploying small cells in various test cities for mobile and fixed applications, Sprint is taking a joint approach of mmWave and mid-band spectrum to build out its network, and T-Mobile is focused on mmWave and low-band spectrum. While all carriers are looking into sub-6 spectrum options to some extent, they are inherently restricted by smaller amount of bandwidth available in sub-6 relative to the hundreds of GHz available in mmWave, and this constraint is exacerbated by the fact that the U.S. government owns large portions of the sub-6 spectrum. Carriers are piggy-backing off of existing 4G infrastructure, but those focused on mmWave will have to build out additional infrastructure to ensure uninterrupted connectivity through a dense network of base stations. There is debate over whether some of the networks deployed have qualified as true 5G, and there is intense competition between these providers to roll out 5G networks within the next few years. 5G development is being overseen by 3GPP (3rd Generation Partnership Project), the standards body that also oversaw the development of 3G UMTS (including HSPA) and 4G LTE standards.

Despite messaging from various marketing initiatives in the United States, very little U.S. territory has seen deployment of 5G infrastructure that can deliver 1 Gbps or even 100 Mbps service at the edges of coverage. Whereas LTE deployment resulted in 10x end user speed improvement across large parts of the United States, carriers to date have not demonstrated deployment capability that would deliver high speeds to large parts of the U.S. population.

As discussed in Chapter One, U.S. carriers have had some success in deploying limited mmWave for small geographic areas, but these have limitations for future scalability. Even in optimized circumstances, it is clear that scaling mmWave to provide more coverage would be a time- and cost-intensive endeavor requiring a massive infrastructure build-out.

There is the risk that these carriers will not even be able to commit the necessary capex to scale those mmWave networks, given the large number of base stations required. At the end of 2018, Verizon held ~$120B in debt with ~4% dividend yields, while AT&T held ~$175B in debt with over 6% dividend yields.[14] T-Mobile holds ~$25B in debt, and Sprint holds ~$40B in debt.[15] These companies are at the forefront of the U.S. effort to develop 5G, but their balance sheets suggest that they may struggle with the cost of a full mmWave network roll-out and the infrastructure it would require.

In the last decade, significant shifts have occurred in the wireless vendor community as well. Chinese telecom equipment giant Huawei grew global revenues from approximately $28B in 2009 to $107B in 2018. Ericsson's revenue during the same period fell from $27.9B to $23.9B,[16] while Nokia's revenue fell from $57.6B to $26.6B.[17] Chinese handset vendors like Huawei, ZTE, Xiaomi, Vivo, and Oppo have grown market share from less than approximately 6% in 2009 to over 30% share in 2018, and are still growing rapidly despite minimal sales in the U.S. market - for example, India represents a wireless market larger than that of the United States, and 59.7% of all handsets sold in India are Chinese.[18] Chinese internet application companies, led by Baidu, Alibaba, Tencent and new companies like TikTock are growing in influence and revenue. In 2009, all of the top 10 Internet companies by revenue were American. Today, four of the top 10 are Chinese.

These shifts have not just occurred because Chinese equipment is cheaper. In many cases, Chinese equipment is also superior to its Western rivals. Huawei and ZTE have been the leader in massive MIMO radio systems, with 64 transmit and receive elements. Many consider Huawei's P series and Mate Android phones the most advanced phones in the world, and these devices are powered by Huawei's own Hi-silicon division. Alibaba's cloud services are fourth in the world, behind Amazon, Microsoft, and Google, and growing quickly.

---

[14] "Schedule of Outstanding Debt," Verizon, accessed March 20, 2019, https://www.verizon.com/about/investors/schedule-outstanding-debt; "Debt Detail as of December 31, 2018," AT&T, accessed March 20, 2019, https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/debt/2018/4q18/Debt_List_4Q18.pdf.

[15] "T-Mobile Outstanding Senior Notes And Credit Facilities – Ratings And Maturity Dates (By Year)," T-Mobile, accessed March 20, 2019, https://investor.t-mobile.com/financial-performance/fixed-income/default.aspx; "Q3 News Release," Sprint, accessed March 20, 2019, https://s21.q4cdn.com/487940486/files/doc_financials/quarterly/2018/Q3/01_Fiscal-3Q18-Earnings-Release-FINAL.pdf.

[16] "Ericsson Revenue," Macrotrends, accessed May 31, 2019, https://www.macrotrends.net/stocks/charts/ERIC/ericsson/revenue.

[17] "Nokia Revenue," Macrotrends, accessed May 31, 2019, https://www.macrotrends.net/stocks/charts/NOK/nokia/revenue.

[18] "Just 2 Companies Control 50% of India's Smartphone Market," The Economic Times, February 15, 2019, https://economictimes.indiatimes.com/tech/hardware/just-2-companies-control-50-of-indias-smartphone-market/articleshow/68007602.cms?from=mdr.

Public Sector: White House

U.S. government interest in 5G has been ramping up over the last decade. In 2016, the White House launched a $400 million Advanced Wireless Research Initiative to promote wireless testing platforms, while the FCC passed its "Spectrum Frontiers" policy in which the United States committed to releasing large quantities of mmWave spectrum for both licensed and unlicensed use.[19] Interest in 5G has increased under the current administration, which has offered up a series of initiatives and directives emphasizing the importance of 5G and to develop a clear roadmap. The current administration supports a private sector-led 5G effort, rather than a government-led nationalized 5G plan.

In September 2018, the White House hosted a 5G Summit, during which industry and government leaders convened to discuss the future direction of 5G, promoting private-public sector collaboration while conceding that the United States had fallen behind in developing and fielding 5G. Shortly after, the White House released the "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," highlighting the need for the United States to lead 5G to promote national security and innovation across the public and private sectors.[20] The memo directed departments and agencies to submit a number of reports on current spectrum usage and future requirements, spectrum reallocation options, and the impact of future technologies on spectrum allocation, and also called for 5G legislative, regulatory, and policy recommendations. On the same day as the Presidential memo, the White House released an article titled "America Will Win the Global Race to 5G", looking at U.S. advantages gained from leading 4G (e.g., increased GDP and job opportunities) and comparing them to the potential benefits of leading 5G.[21]

Public Sector: FCC

The FCC plays a large role in the development and fielding of 5G with regard to spectrum allocation and policy for civil-use spectrum. In late 2018, the FCC held a vote to establish a framework for freeing up mmWave spectrum bandwidth to help expedite 5G development and deployment. The FCC controls U.S. spectrum auctions and held its first 5G spectrum auction in late 2018, which opened up the 28 GHz band. A second auction, held on March 14, 2019, made available the 24 GHz band.

[19] The White House, "Fact Sheet: Administration Announces an Advanced Wireless Research Initiative, Building on President's Legacy of Forward-Leaning Broadband Policy," 15 July 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/15/fact-sheet-administration-announces-advanced-wireless-research; Harper Neidig, "White House orders Commerce to develop 5G strategy," *The Hill,* 25 October 2018, https://thehill.com/policy/technology/413121-white-house-orders-commerce-to-develop-5g-strategy.

[20] "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," White House, October 25, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-developing-sustainable-spectrum-strategy-americas-future/.

[21] Michael Kratsios, "America Will Win the Global Race to 5G," White House Office of Science & Technology, October 25, 2018, https://www.whitehouse.gov/articles/america-will-win-global-race-5g/.

The FCC released its comprehensive 5G strategy, "Facilitate America's Superiority in 5G Technology (FAST) Plan," in September of 2018.[22] The plan focuses on three main goals: pushing more spectrum into the marketplace, updating infrastructure policy, and modernizing outdated regulations to facilitate 5G in the United States. With regard to the spectrum goal, the FCC plans to hold three more auctions in 2019 to sell bands of mmWave spectrum, and is conducting research to understand options for opening up low- and mid-band spectrum. With regard to the infrastructure goal, the FCC is working to increase the speed of review for small cells at the federal, state, and local levels to facilitate faster fielding of 5G. With regard to the modernization goal, the FCC is focused on adjusting existing regulations and making new ones to support 5G deployment, such as updating its rules on network equipment to allow for more rapid cell fielding and preventing the sale of network equipment from companies that pose a national security threat to U.S. networks.

The FCC has also started a proceeding to enable more flexible use of the 500 MHz of C-band downlink spectrum, which is positioned in the middle of the 3 and 4 GHz bands.[23] In 2015 at ITU's World Radio Conference, the Obama administration opposed the proposal to reclassify this band as an IMT-2000 allocation suitable for 5G use, which would have paved the way for global standardization of this spectrum for 5G mobility services. Even if the spectrum was reclassified as broadband, it would take some time before existing users could be completely removed from the C band. Sharing the band for 5G mobility use is difficult because mobile handsets emit radio energy in a broad pattern, and numbers of users operating near C band antenna could materially cause interference to satellite reception. However, fixed operations could share the spectrum through the use of highly directional antennas or beamforming systems, and this type of equipment would be ideal for providing fixed services to rural areas, as well as possible DoD uses for fixed network extensions.

If the United States were to aggressively pursue sharing and eventual reallocation of the C-band downlink spectrum, it could allow a second round of 5G spectrum expansion that could give the United States a boost in speed and coverage. However, the benefits of this spectrum reallocation would depend on global companies building their devices to operate within C-band, and the United States would need to push for acceptance of that part of the spectrum as a globally utilized band.

Public Sector: Department of Commerce

The Commerce Department's National Telecommunications and Information Administration (NTIA) manages federal-use spectrum allocation. The Department of Commerce is currently developing a "National Spectrum Strategy" to improve spectrum management, identify research and development priorities to create new technologies, and aggregate federal agencies' spectrum operational needs.[24] NTIA will work with members of a new Spectrum Strategy Task Force (established by the Presidential memo) in a multiyear effort to develop and implement this

[22] "The FCC's FAST Plan," FCC, accessed March 20, 2019, https://www.fcc.gov/5G.
[23] "FCC Expands Flexible Use of Mid-band Spectrum," FCC, July 13, 2018, https://www.fcc.gov/document/fcc-expands-flexible-use-mid-band-spectrum.
[24] Neidig, "White House orders Commerce to develop 5G strategy."

national strategy and align research, development, testing, and evaluation efforts.[25] If DoD were to share its spectrum, it would have to work closely with NTIA to manage that sharing process.

[25] McCabe, "White House directs task force to come up with 5G wireless strategy," *Axios*, October 25, 2018, https://www.axios.com/white-house-national-wireless-strategy-task-force-5g-5e884590-8a4b-4b12-9c16-a1b6401f84ad.html.

CHAPTER 3: DoD DEVELOPMENT AND ADOPTION OF 5G TECHNOLOGY

5G Impact on DoD

While much of the discussion around 5G revolves around the commercial sector as the driving force behind its rollout, 5G ecosystems of technology can equally revolutionize DoD operations, networks, and information processes. DoD must be able to communicate, engage, and operate faster to keep up with the changing environment. 5G will enable this new concept of operations, allowing larger volumes of data to be shared in close to real time across geographically dispersed systems. Currently, data sharing at that scale cannot be completed effectively with legacy communication networks. Existing networks will benefit by leveraging lower latency and higher capacity data transfer capability, but 5G's true potential will be in its impact on the battle network of the future. That network will increasingly include a large number of cheaper, more connected, and more resilient systems to function in a rapidly evolving battlefield.

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

However, 5G also presents a serious potential risk for DoD going forward. When operating overseas in the future, the vast majority of these networks and systems may depend on 5G infrastructure. If China leads the field in 5G infrastructure and systems, then the future 5G ecosystem will likely have Chinese components embedded throughout. This would pose a serious threat to the security of DoD operations and networks going forward. Additionally, the growth in the number of connected devices increases the potential "attack surface" for adversaries to target across DoD networks, which will require increased vigilance and security across systems. The larger volume of data being transferred will complicate this task, as it will make it more difficult to detect malicious traffic on a network.

Pivot to Sub-6 GHz

The United States may choose to continue down the path of mmWave, but the rest of the world is focused on building out sub-6 infrastructure, with China in the lead. As a government entity that operates overseas, DoD will ultimately have to learn to operate on that sub-6 infrastructure, regardless of how the United States chooses to implement 5G domestically. For this reason, the United States must invest in sub-6 capabilities and take steps to share its spectrum. However, there are legitimate concerns within DoD that opening up sub-6 spectrum will create a number of operational issues, from spectrum optimization to security vulnerabilities. If DoD operators are forced to share their bands of the spectrum, there are concerns that this may temporarily or permanently reduce the performance of systems. The addition of commercial users would also increase the overall congestion of the sub-6 spectrum, increasing the risk of connectivity interruptions for DoD operators.

However, if the United States and DoD do not pivot to sub-6, DoD will face further challenges with acquisition and practical deployment of 5G. Although mmWave components are typically more compact than sub-6 components, mmWave requires many more base stations positioned within close proximity of one another to maintain connection (and even then, there is still the risk that interference such as objects moving in front of the base station or weather will interrupt the connection). This quickly becomes logistically impractical if a person or platform has to carry multiple antennae, particularly at the fighting edge. Additionally, the DoD acquisition system is slow-moving and might take years to deploy the necessary systems for a mmWave network, at which point most of those systems might already be obsolete. Both DoD and the FCC are currently prioritizing mmWave over sub-6 mid-band spectrum with a particular focus on the 28 and 37 GHz bands, but this is a fundamentally flawed focus due to the impracticality of mmWave deployment. DoD must prepare to operate in a sub-6 5G ecosystem, which will require a shift in strategy and a consideration of where DoD is willing to share bandwidth in the sub-6 realm.

This shift may come with some inherent benefits. The anonymity that comes from utilizing the same infrastructure as any other company or country provides an industry-standard form of security all its own. Integration of government and civil use may provide a layer of security by allowing military traffic to "hide in plain sight" as traffic becomes more difficult to see and isolate. Similarly, adversaries might be deterred from jamming this spectrum because they might be operating on the same bands. Government will maintain primary spectrum access while also benefiting from technology advancements from the commercial sector that result from operations in the sub-6 range, which will help the government to close the gap between the commercial sector and current state of military communications. This also creates an opportunity for cyber and communications personnel to learn how to make spectrum more resilient by working regularly with shared spectrum and managing it both domestically and abroad.

A Path Forward for Sub-6 Spectrum Sharing

The idea of spectrum sharing is not new. In 2010, the FCC identified the spectrum band from 3550-3700 MHz, known as Citizens Broadband Radio Service (CBRS), as a potential spectrum-sharing opportunity. CBRS utilizes LTE networks to provide wireless voice, text, and data services, and this spectrum was freed as a result of the FCC's 2010 National Broadband Plan to provide more spectrum for new mobile users.[26] In 2015, the FCC formally authorized the 3.5 GHz band for shared wireless access in an area that was previously utilized by the U.S. Navy and DoD. CBRS will enhance the "last mile" of fiber access to deliver fixed wireless service and also offer point-to-multipoint capabilities. CBRS spectrum can be unlicensed by the user, or they may purchase temporary licenses for periods of use, and it allows services to be deployed in a more rapid and efficient manner. DoD remains the incumbent user of the band, so other users will be limited by the Spectrum Access System (SAS), which ensures that there is deconfliction

[26] "National Broadband Plan," FCC, March 17, 2010, https://www.fcc.gov/general/national-broadband-plan.

to remove interference with military use. SAS gives DoD priority in the band, but keeps the band open for commercial users when not occupied.

This precedent may serve as a guide for future spectrum sharing between DoD and the commercial sector. By offering up its own bandwidths to share, DoD can also encourage a system of "bi-directional" spectrum sharing in which civil and federal users could access one another's spectrum with varying prioritization. This would increase the amount of spectrum available to DoD on a secondary level, while maintaining priority access in its own bandwidths. Additionally, DoD stands to gain significant benefits from 5G development, for reasons listed at the beginning of this chapter. DoD may have some initial growing pains as it begins to share parts of the spectrum, but the net gain in capability from 5G will ultimately make up for that inconvenience. If DoD does not begin to share the sub-6 spectrum, it will increase the risk of dependence on a compromised supply chain as U.S. companies will be blocked from developing and competing their own sub-6 5G offerings, and foreign providers will increasingly embed their offerings in networks and systems globally.

Security Challenges in 5G

Supply Chain Risks

DoD is facing a future 5G environment where its supply chain will be increasingly vulnerable or compromised, from the subcomponent level to the integrated network level, as well as the services associated with each. In previous decades, DoD was able to operate on bespoke systems that fulfilled its unique requirements due to its position as a large user relative to the rest of the commercial world, but that privilege no longer exists. Commercial sector tech development and usage dwarfs that of DoD, and it is no longer practical for DoD to build and operate on siloed, bespoke systems and architecture. As a result, DoD is increasingly dependent on commercial off-the-shelf (COTS) equipment and commercial services, and the same will hold true for the future 5G ecosystem.

DoD can incorporate commercial inputs into its 5G infrastructure at four levels: the RF component, the integrated chipset, the device, and the service. RF components can include subcomponents ranging from semiconductors to switches and amplifiers. Integrated chipsets combine various subcomponents and other subsystems to interface with system components on a motherboard. Devices can range from mobile handsets to fixed computer systems, which include both the subcomponents and integrated chipsets listed above. Finally, each of these inputs comes with a set of service offerings to operate, manage and maintain them.

Commercial companies can supply any and all of the above inputs, but this comes with the risk of inadvertent or malicious security vulnerabilities that put DoD systems and networks at risk. The 5G ecosystem will especially run the risk of including security vulnerabilities if China becomes the global leader supplying 5G infrastructure from the subcomponent-level to the integrated system-level, for even if the United States limits sales of Chinese products into the United States, DoD will still have to operate on foreign networks overseas that will likely be built with a Chinese supply chain.

DoD has made the shift from bespoke to commercial-reliant computing systems over the past decade, but this change in approach carried less risk than is currently faced because the United States dominated the computing systems market and was able to "own" the supply chain and better secure it against vulnerabilities. As a result, DoD now incorporates varying degrees of COTS products into its computing systems while keeping vulnerability risk at an acceptable level. However, in the current 5G competition, neither DoD nor the United States writ large is in a position to dictate the content and integration of the 5G supply chain - our focus on building a mmWave 5G ecosystem leaves us out of the global supply chain for the sub-6 5G ecosystem. This mismatch will create serious security risks for DoD going forward if the rest of the world accepts Chinese products as the cheaper and superior option for 5G.

5G Infrastructure and Services

5G networks have a number of security risks to consider, regardless of what spectrum bands they operate in. While DoD security typically focuses on vendor-installed backdoors that could be used to remotely control a system or exfiltrate information, a wide variety of security issues could also be introduced through poor software development practices both during and after the rollout of 5G. Many of these risks were mentioned in a UK report on the joint effort with Huawei and the UK government to manage security issues with Huawei deployments in the UK.[27] Security issues from poor software development issues are a universal problem, and are not restricted to only Chinese vendors.

Even if the security of a particular release of software for a 5G base station may be secure and well-implemented, there is no guarantee that future releases will continue to be equally secure. Bugs will inevitably be found and require software patches, and these fixes may need to be fielded quickly without fully considering new security issues that might be introduced with the patch. It will become increasingly challenging to validate continued security with each iteration.

Even if base station code is secure and well-managed over time, the business model of the wireless infrastructure providers is such that personnel from the vendor are typically involved in the commissioning, operation, and maintenance of network infrastructure. This requires vendors to access core management systems that operate the network, and allows vendors to deploy software to equipment in the system. In many cases, network operators both in and out of the United States outsource entire operations of the network to the vendor of the equipment, increasing potential vulnerabilities via this third party activity.

Field maintenance is also typically contracted back to the vendor. Service staff visiting field sites are able to upload new software to the network and change network configurations. DoD has a long history of combating malware that has been transmitted into weapons systems through computers that were not patched, did not have multi-factor authentication, or were exposed to

[27] "Huawei Cyber Security Official Oversight Board Annual Report 2019," March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

security breaches through bad usage practices by personnel.[28] All of these issues and more apply to vendor maintenance computers. These support systems are rarely examined by security engineers, and yet they may be equipped with credentials that give them powerful abilities to insert vulnerabilities into the infrastructure.

Radio access network (RAN) vendors often dictate choices of core network infrastructure that manages traffic over backhaul links and across national fiber networks. They also provide core authentication services, the ability to perform legal intercepts, name server functionality and interconnection with the Internet. This control derives from vendor use of non-standard techniques to communicate and manage base stations and the overall radio network. As a result, an operator may have difficulty choosing non-Huawei core infrastructure for Huawei base stations. Multi-vendor networks are typically configured as islands of common vendor equipment, and if a vendor is found to have serious security issues, replacing that vendor in the infrastructure may require a near-complete rebuilding of the network.

5G core infrastructure has additional issues from functionalities like network "slicing" that exposes the network to non-operators. For example, if a virtual reality headset requires a managed slice of network infrastructure to communicate with a cloud-based gaming service, this increases the attack surface of the core network by enabling signaling and control to edge- and cloud-based compute entities.

5G Devices

In addition to 5G network infrastructure, DoD must also consider security risks associated with 5G devices. If the current trends of rising Chinese dominance in the wireless device market continues, Chinese vendors will continue to grow in market share and in sophistication, even if denied access to the U.S. market due to their device popularity with the rest of the world. To the extent U.S. forces deployed overseas use these devices, either for official business or for personal uses, DoD will have to address issues caused by their use.

Evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally. Many of these seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information about domestic users. In a recent case, Nokia android handsets were discovered to have a backdoor that sent a variety of data to a network server located in the network of China Telecom.[29] Nokia had deliberately built this code into devices sold into China, but had then accidentally installed it onto all its other devices. In 2018, software from XIONGMAI, a Chinese camera vendor that manufactures security cameras, was found to have to an undocumented backdoor user named "tluafed" ("default" in reverse) that could access millions of cameras. This is believed to be related to a hash

[28] "Weapon System Cybersecurity, GAO, October 2018, https://www.gao.gov/assets/700/694913.pdf.
[29] Jerry Hildenbrand, "How does a phone maker 'mistakenly' collect user data and ship it off to a server in China?" androidcentral, March 23, 2019, https://www.androidcentral.com/how-does-company-nokia-or-oneplus-mistakenly-collect-user-data-and-ship-it-server-china.

algorithm in the software development library provided by Huawei for its HiSilicon SOC, on which the camera is based.[30]

These and other incidents indicate that Chinese agencies may mandate backdoor access to devices shipped into China to aid their internal surveillance activities. Because of the nature of software development environments, it is difficult to maintain separate sets of code bases with some code options only compiled and installed on devices shipped to specific destinations. When those devices are shipped outside of China, those backdoors can still be used to exfiltrate information.

We can only speculate whether or not the spread of these security vulnerabilities is intentional or inadvertent. However, if Chinese policy does require backdoor access embedded in devices sold in China for internal security purposes, this compromised code applied to such a large market increases the risk that these vulnerabilities will spill over into the rest of the world. If China dominates the market for 5G devices, both as a manufacturer and as a large and attractive market of users, then this potential for vulnerabilities will only continue to spread and put the larger 5G ecosystem at risk.

[30] "Millions of XIONGMAI Video Surveillance Devices Can Be Hacked Via Cloud Feature," SEC Consult, accessed March 31, 2019, https://sec-consult.com/en/blog/2018/10/millions-of-xiongmai-video-surveillance-devices-can-be-hacked-via-cloud-feature-xmeye-p2p-cloud/.

CHAPTER 4: BOARD RECOMMENDATIONS FOR 5G

Board Recommendations

The Defense Innovation Board bases its recommendations on the assumption that mmWave fundamentally cannot be deployed on a large scale in the United States because of the propagation and cost limitations, and that sub-6 GHz mid-band spectrum (in the 3 and 4 GHz range) will become the global standard for broad area networks in coming years. This assumption is based on an assessment of the engineering requirements for mmWave and various studies projecting the required infrastructure and associated cost to support even a limited mmWave network. Additionally, the current financial state of U.S. providers may inhibit their ability to invest the required capex to support a mmWave network, limited or otherwise.

Recommendation #1

DoD needs to make a plan for sharing sub-6 GHz spectrum to shape the future 5G ecosystem, including an assessment of how much and which bandwidths need to be shared, within what timeframe, and how that sharing will impact DoD systems.

- **DoD and the FCC must flip their prioritization from mmWave to sub-6 GHz spectrum for 5G**. DoD and FCC have been prioritizing the 28 and 37 GHz bandwidths as options for 5G development, but this effort is misplaced. This study has covered the broad range of limitations associated with mmWave, and reasons why the rest of the world will adopt a sub-6 GHz 5G ecosystem. In light of this, DoD must prepare itself for that future operating environment by focusing on co-existing, if not explicitly sharing, with civil 5G operations in those bands of spectrum.

- **DoD should particularly focus on the bands of the sub-6 GHz spectrum that are already being used by China**. Chinese 5G systems and infrastructure operate in the 3.2-3.6 GHz range, as well as the 4.8-5.0 GHz range. As a result, the commercial world has developed semiconductors and handsets that are configured for that range, and DoD should angle for the most developed market to expedite 5G sub-6 GHz deployment in the United States. It takes approximately two years to add new frequency bands to complex multiband transceivers, and the United States would be able to avoid those two years of development by leveraging subcomponents and devices already on the market for more mature spectrum usage, such as existing Qualcomm products with functionality in the bands leveraged by China.

- As an additional consideration, **DoD currently occupies ~500 MHz of space in the 4 GHz spectrum.** DoD should take action to share parts of this space, given that it is a material amount of bandwidth that could make a serious impact on 5G development. 5G functions most optimally on large amounts of consecutive bandwidth, and this range could provide the real estate to drive 5G development forward.

  **For more detailed options around DoD spectrum sharing, see Classified Annex.*

- For additional spectrum availability, DoD should recommend that the NTIA, FCC and Department of State should **advocate the reallocation of the C-band satellite spectrum to IMT-2000 5G use** at the World Radio Conference later this year (WRC-19), and take measures to adopt sharing in all 500 MHz of the band in the United States on an accelerated basis for fixed operations. While this will have limited impact on the U.S. 5G mobile ecosystem, sharing in this band could provide broad coverage at 100 Mbps and above for **fixed broadband service** to a large section of the rural United States.

- **DoD should encourage other government agencies to incentivize industry to adopt a common 5G network for sub-6 deployment**. Incentives can include: accelerated depreciation, tax incentives, low interest loans and government purchase of equipment and services.

- **This recommendation does not call for the eviction of DoD systems operating in the sub-6 GHz spectrum, nor does it call for the sharing of ALL DoD spectrum.** DoD must conduct thoughtful but candid analyses of the cost and schedule associated with sharing different spectrum bands, and prioritize accordingly.

- However, DoD must bear in mind that **the status quo of spectrum allocation is unsustainable**. 5G capability requires larger bands of spectrum, and without that additional bandwidth, the United States will not gain true 5G capability beyond the limited range that mmWave can provide. **In the next year, DoD is in the position to enable or inhibit 5G adoption in the United States based on its use of sub-6 GHz spectrum.**

- DoD stands to significantly benefit if it shares some of its sub-6 GHz spectrum. As the commercial sector develops and deploys 5G technologies and networks, DoD will be able to **leverage commercial innovations** to build its own new and improved technologies and networks. At a strategic level, 5G can create a **step-change in situational awareness and decision-making** by integrating more systems into a network that shares more data faster and at lower latency.

- This effort will require **close coordination with NTIA** to clear and reassign spectrum. Timing is critical - it is not enough to simply share spectrum, it must be done quickly to keep the United States competitive with China, South Korea, and Japan.

- **Without aggressive action as outlined in this report, we believe there is a high likelihood that the United States will be unable to convince the rest of the world to adopt mmWave technologies as the standard 5G pathway.** This may bifurcate the global market and result in the majority of the world adopting 5G sub-6 technologies, which will be dominated by the Chinese equipment and handset manufacturers.

Recommendation #2

DoD must prepare to operate in a "post-Western" wireless ecosystem. This plan should include R&D investments towards system security and resiliency on an engineering and strategic level.

- Sharing parts of the sub-6 spectrum will certainly help the U.S. 5G effort, but gaining a competitive edge over China would require action at a rate and magnitude previously unseen within DoD. For this reason, it is probable that most of the world outside of the United States will adopt a sub-6 5G solution, forcing DoD to operate on a "post-Western" wireless ecosystem. In this event, **DoD should assume that all network infrastructure will ultimately become vulnerable to cyber-attack from both an encryption and resiliency standpoint.**

- **DoD must adopt a "zero-trust" network model.** Perimeter defense models have been proven to be ineffective, and 5G will only exacerbate this problem as more systems are linked into a common network. Information access should no longer be granted simply through attachment to a specific network, and instead should be granted through various security checks within the network. DoD should also plan to move to quantum-resistant key exchange mechanisms to deal with the eventual fall of public key exchange algorithms, particularly given China's investments in quantum computing.

- While "zero-trust" networks can protect context exchange through cryptography, these exchanges will still be subject to traffic analysis and detection of surges in network utilization. **DoD should work to keep large amounts of data flowing on a constant basis so that increases in operational tempo will not be noticed.**

- In addition to these security precautions, DoD must brace for cyber-attack and penetration by **improving resiliency and building in layers of redundancy throughout its networks** to ensure uninterrupted connectivity**.**

- DoD will need to consider options for defending against a compromised supply chain, where Chinese semiconductor components and chipsets are embedded across multiple systems. DoD should invest in R&D to study the impact of compartmentalizing systems to limit an attacker's ability to move laterally into other systems. This will come with performance costs, and **DoD must find the line where it can balance baseline capability with security.**

- **DoD should advocate for aggressive protection of U.S. technology intellectual property rights (IPR) in an effort to slow down China's telecommunications ecosystem expansion.** The United States should leverage export controls to slow the rate of market loss for Western vendors, even if it may increase the pace at which China becomes self-sufficient.

- **DoD will increasingly be driven to operate on shared commercial networks without their own bespoke infrastructure** (as in the case of nuclear C3). DoD must analyze the risks and benefits associated with that shift, and **adjust its concept of operations to account for it.**

  **For a more detailed assessment of 5G impact on nuclear C3, see Classified Annex.*

- DoD needs to consider the broader implications of a compromised supply chain, such as risk to personal devices and information that can be derived from activity on those

devices. If China is able to collect this data, **DoD should consider discrete directives to defend against these vulnerabilities that fall outside the traditional DoD systems and platforms**, such as training to limit inadvertent sharing of PII through personal device use.

- In addition to these efforts, **DoD should initiate testing and experimentation on its bases for future generations of wireless technology beyond 5G**. This testing and experimentation will occur over a longer timeframe to ensure that the United States is prepared to lead the next generational transition. These activities can include testing for sub-6 sharing, as well as future mmWave deployment and propagation improvement.

Recommendation #3

DoD should advocate for adjusted trade policies to discourage vulnerabilities in its supply chain on the grounds that they put national security assets and missions at risk.

- The **compromised supply chain issue** poses a serious threat to national security by introducing vulnerabilities into networks and systems, which can be leveraged by a hostile actor to disrupt DoD operations. The spread of these vulnerabilities creates an increasingly unstable environment by lowering barriers to offensive action while weakening defensive positions.

- The proliferation of security vulnerabilities creates incentives for all nations to take offensive action in a conflict, as the barrier to offense decreases while the difficulty of defense increases. This reality is reflected in the new U.S. Cyber doctrine of “forward defense”.

- To counter this threat, DoD should advocate that trade policy **reward good security/coding and penalize vulnerabilities through tariffs** (“monetization” of good development practices). For example, the United States could automatically impose a heavy tariff (say, 75%) on any goods **from any nation** found to have backdoors or serious security vulnerabilities. This would impose a market cost for insecurity, and would also create incentives for domestic companies to fund security researchers to find vulnerabilities in competitors’ products, thereby triggering the tariff. This would improve the overall security of DoD ecosystems without having to disclose vulnerabilities found by Title 50 entities.

- The United States should **encourage Five Eyes and NATO partners to adopt the same tariffs,** regardless of product country of origin. The United States stands to benefit the most in a trade conflict over security of devices.

- DoD should also encourage CFIUS to **block transactions of companies with a history of selling products with documented backdoors and security vulnerabilities.**

- Additionally, the United States should continue to **encourage partner nations to secure their own supply chains** and deny access to Chinese state-owned enterprises (SOEs) selling 5G wares.

  **For more information on Chinese 5G strategy and current state, see Classified Annex.*

Recommendation #4

See Classified Annex.