Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated March 14, 2023

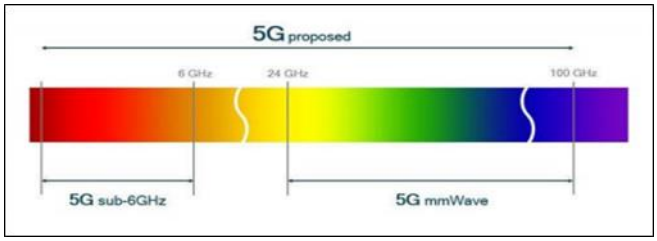
National Security Implications of Fifth Generation (5G) Mobile Technologies

The fifth generation (5G) of mobile technologies will increase the speed of data transfer and improve bandwidth over existing fourth generation (4G) technologies, in turn enabling new military and commercial applications. 5G technologies are expected to support interconnected or autonomous devices, such as smart homes, self-driving vehicles, precision agriculture systems, industrial machinery, and advanced robotics. 5G for the military could additionally improve intelligence, surveillance, and reconnaissance (ISR) systems and processing; enable new methods of command and control (C2); and streamline logistics systems for increased efficiency, among other uses. As 5G technologies are developed and deployed, Congress may consider policies for spectrum management and national security, as well as implications for U.S. military operations.

Spectrum Management

5G technologies plan to use three segments of the electromagnetic spectrum ("the spectrum"): high band (also called millimeter wave, or MMW), which operates between around 24 and 300 GHz; mid band, which operates between 1 GHz and 6 GHz; and low band, which operates below 1 GHz. Mid band and low band are often collectively referred to as sub-6 (see **Figure 1**).

Figure 1. 5G Proposed Spectrum



Source: https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

Millimeter waves allow faster data transfer rates, which some telecommunications companies argue is required for autonomous vehicles, virtual reality, and other data-intensive applications like smart cities; however, MMW travel comparatively short distances and can be absorbed by rain or disrupted by physical objects such as buildings and vehicles. As a result, 5G MMW technologies require installing a higher number of cell sites—at much higher cost and on a much slower deployment timeline than the sub-6 approach. 5G deployment thus relies on MMW for high-speed, high-bandwidth communications and on sub-6 waves for nationwide coverage.

Telecommunication companies around the world are deploying 5G in different ways. Chinese telecommunications companies are focusing on the less expensive sub-6 approach, while some U.S. telecommunication providers are focused on MMW deployments and others on sub-6.

The Department of Defense (DOD), however, holds large portions of the usable spectrum. Although DOD uses certain MMW frequencies for high-profile military applications such as Advanced Extremely High Frequency satellites that provide assured global communications for U.S. forces, it extensively uses sub-6 frequencies—leaving less sub-6 availability in the United States than in other countries. The Defense Innovation Board (DIB) advised DOD to consider sharing sub-6 spectrum to facilitate the build-out of 5G networks and the development of 5G technologies used in the sub-6 band. While DOD has been moving toward greater spectrum sharing, it has expressed concern that sharing presents operational, interference, and security issues for DOD users. As an alternative to spectrum sharing, some analysts have argued that portions of the sub-6 spectrum should be reserved for commercial use. This would require DOD to relocate certain applications to other parts of the spectrum. DOD has argued that moving out of the 3.1-3.45 GHz band alone could cost at least $120 billion and take decades.

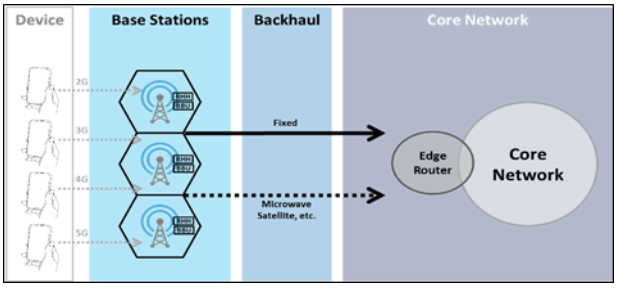
National Security Concerns

According to a DIB assessment, China is the current leader in sub-6 technologies and is likely to deploy the world's first 5G wide-area network. Chinese companies, which often receive government subsidies (e.g., subsidized land for facilities, R&D grants), are therefore well-positioned as global 5G suppliers. Huawei has signed contracts for the construction of 5G infrastructure in around 30 countries, including Iceland, Turkey, and Hungary.

Some experts are concerned that vulnerabilities in Chinese equipment could be used to conduct cyberattacks or military/industrial espionage. These experts claim vulnerabilities were introduced through the poor business practices of many Chinese companies. However, they note that vulnerabilities could also be intentionally introduced for malicious purposes. China's National Intelligence Law, enacted in June 2017, declares that "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of." Some analysts interpret this law as requiring Chinese companies to cooperate with intelligence services, including compelling installation of backdoors to provide private data to the government.

Other analysts argue that the risks posed by Chinese telecommunications equipment vary depending on the equipment's location within the cellular network architecture. Most cellular networks are broken into two groups: the core network, which provides the gateway to the internet and ensures devices meet the provider's standards, and the radio access network, composed of the cellular towers that broadcast and receive radio signals (see **Figure 2**). These analysts state that, while the risks posed by Chinese core networks are significant, the risks posed by Chinese radio access networks could be managed. Other analysts have argued that having any Chinese equipment in the network could pose potential security concerns. Such concerns have prompted some analysts to argue that the United States should limit intelligence sharing with any country operating Chinese-supplied 5G equipment.

Figure 2. Cellular Network Architecture



Source: https://medium.com/@miccowang/5g-c-ran-and-the-required-technology-breakthrough-a1b2babf774.

In response to these security concerns, Congress passed the Secure 5G and Beyond Act (P.L. 116-129), requiring the President to develop a 5G protection strategy. Similarly, Section 254 of the FY2020 National Defense Authorization Act (NDAA) (P.L. 116-92) required the Secretary of Defense to develop a DOD 5G strategy. These strategies were released in March 2020 and May 2020, respectively. DOD released an associated 5G implementation plan in December 2020. In addition, Section 224 of the FY2021 NDAA (P.L. 116-283) directed DOD to create a 5G governance structure, while Section 225 directed DOD to demonstrate the maturity of 5G component technologies. Finally, Section 233 of the FY2022 NDAA (P.L. 117-81) directed the service secretaries to develop a plan for 5G pilot programs on military installations; Section 221 of the FY2023 NDAA (P.L. 117-263) directed the Secretary of Defense to identify a target date for 5G deployment at all installations. Section 234 of the FY2023 NDAA additionally tasked specified Assistant Secretaries with developing three-year transition plans for 5G.

Implications for Military Operations

5G technologies could have a number of potential military applications, particularly for autonomous vehicles, C2, logistics, maintenance, augmented and virtual reality, and ISR systems—all of which would benefit from improved data rates and lower latency (time delay).

Autonomous military vehicles, like their commercial counterparts, could potentially circumvent on-board data processing limitations by storing large databases (e.g., maps) in the cloud. Safe vehicle operations would require 5G's high data rates and low latency to download off-board information and synthesize it with on-board sensor data. Likewise, 5G could be used to transfer sensor data between operators and uninhabited vehicles and to network vehicles, potentially enabling new military concepts of operations, such as swarming (i.e., cooperative behavior in which vehicles autonomously coordinate to achieve a task).

5G technologies could also be incorporated into ISR systems, which increasingly demand high-bandwidths to process, exploit, and disseminate information from a growing number of battlespace sensors. This could provide commanders with timely access to actionable intelligence data, in turn improving operational decisionmaking. Similarly, 5G could reduce latency in other data-intensive activities, such as logistics and maintenance, and could additionally enable augmented or virtual reality environments that could enhance training.

Finally, command and control systems could benefit from the high speed, low latency capability of 5G. For example, the U.S. military currently uses satellite communications for most of its long-distance communications. However, satellites on orbit can significantly increase latency due to the amount of distance a signal needs to travel, causing delays in the execution of military operations.

DOD has selected 12 military installations as test beds for 5G applications: Marine Corps Logistics Base Albany, GA, and Naval Base San Diego, CA ("smart warehouses"); Hill Air Force Base, UT ("spectrum sharing between 5G and airborne radar"); Joint Base Lewis-McChord, WA ("augmented and virtual reality"); Nellis Air Force Base, NV ("survivable command and control and network enhancement"); Naval Base Norfolk, VA ("ship-wide and pier connectivity"); Joint Base Pearl Harbor-Hickam, HI ("enhancing aircraft mission readiness"); Joint Base San Antonio, TX ("augmented reality support of maintenance and training" and "evaluating DOD's 5G core security experimentation network"); Tinker Air Force Base, OK ("spectrum sharing between military communications and 5G"); and Camp Pendleton, CA; Ft. Hood, TX; and Ft. Irwin National Training Center, CA ("connectivity for forward operating bases and tactical operations centers").

Potential Questions for Congress

- What approach to spectrum management (e.g., spectrum sharing, spectrum reallocation) will best protect DOD missions while meeting growing commercial demands?
- What are the risks to U.S. national security posed by Chinese 5G infrastructure in allied and partner nations? Can that risk be managed and, if so, how?
- Should the United States limit intelligence sharing with countries operating Chinese-supplied 5G equipment?
- Are any changes to operational concepts, force structure, doctrine, or posture required as a result of developments in or applications of military 5G?
  To what extent would commercial 5G technologies be vulnerable to adversary jamming attacks?

This report was originally co-authored by John Hoehn.

Kelley M. Sayler, Analyst in Advanced Technology and Global Security

Disclaimer