Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

June 12, 2019

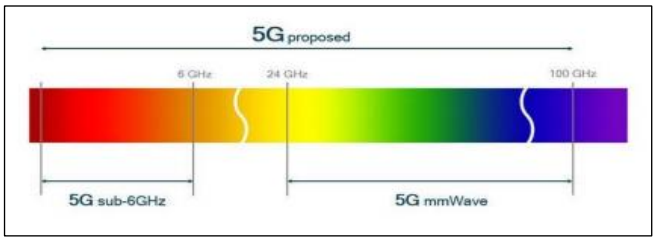
National Security Implications of Fifth Generation (5G) Mobile Technologies

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. According to a Defense Innovation Board (DIB) report, in the military realm, 5G will additionally improve intelligence, surveillance, and reconnaissance systems and processing; enable new methods of command and control; and streamline logistics systems for increased efficiency. 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 requires deployment of technologies that work in various segments of the electromagnetic spectrum ("the spectrum"): sub-6, which operates below 6 GHz, and millimeter wave (MMW), which operates between around 24 and 300 GHz (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 for greater bandwidth and faster transfer rates, which some telecommunications companies have argued is required for autonomous vehicles and other data-intensive applications; however, MMW travel comparatively short distances and can be absorbed by rain or disrupted by physical objects such as buildings, vehicles, and people. As a result, the use of MMW requires the installation of 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 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 likely require DOD to relocate certain applications to other parts of the spectrum. The DIB estimates that this approach would take around 10 years to complete, as opposed to 5 years for spectrum sharing.

National Security Concerns

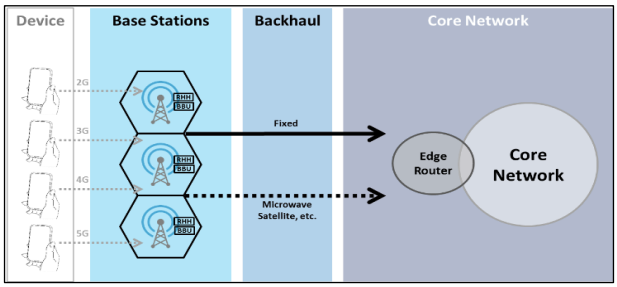
According to a DIB assessment, China is the current leader in sub-6 technologies and is likely to deploy the world's first 5G wide-area network. Chinese companies, which often receive government subsidies (e.g., subsidized land for facilities, R&D grants), are therefore well-positioned as global 5G suppliers.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

Some experts have expressed concern that vulnerabilities in Chinese equipment could be used to conduct cyberattacks or military or industrial espionage. These experts claim that such vulnerabilities have been 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 telecommunications companies to cooperate with intelligence services to include being compelled to install backdoors or provide private data to the government.

Other analysts have argued 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. Still 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

Implications for Military Operations

5G technologies could have a number of potential military applications, particularly for autonomous vehicles, command and control (C2), and intelligence, surveillance, and reconnaissance (ISR) systems—which would each benefit from improved data rates and lower latency (time delay).

Autonomous vehicles are currently in development across the military services. These 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, in turn, require 5G's high data rates and low latency to quickly download off-board information and synthesize it with on-board sensor data. Similarly, 5G applications could be used to transfer sensor data between operators and uninhabited vehicles. 5G could also be used 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).

In addition, 5G technologies could 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.

Finally, command and control applications could benefit from the high speed, low latency capability of 5G. For example, the U.S. military currently uses satellite communications for the preponderance 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. Having terrestrial communications like 5G could potentially reduce latency in video- and teleconferencing, thereby improving communications and situational awareness among deployed forces.

While each of these applications could increase military effectiveness, DOD may refrain from using them due to concerns over data security, particularly passing sensitive information like intelligence or operational requirements over commercial systems. These risks could potentially be mitigated using end-point encryption, where devices would encrypt data before transmitting it over the network, to prevent adversaries from gaining access to information.

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?
- What impact would the use of Chinese 5G infrastructure by allied and partner nations have on military effectiveness and interoperability? 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?
- How might encryption techniques and technologies allow the United States to utilize commercial networks to communicate?

CRS Products

CRS Report R45485, *Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress*, by Jill C. Gallagher and Michael E. DeVine

CRS In Focus IF11105, *Defense Primer: Emerging Technologies*, by Kelley M. Sayler

CRS In Focus IF11155, *Defense Primer: Military Use of the Electromagnetic Spectrum*, by John R. Hoehn

CRS Report R45392, *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*, coordinated by Andrew Feickert

Other Resources

Defense Innovation Board, *The 5G Ecosystem: Risks and Opportunities for DOD*, April 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

John R. Hoehn, Analyst in Military Capabilities and Programs
Kelley M. Sayler, Analyst in Advanced Technology and Global Security

Disclaimer