CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Spectrum Policy and AI Leadership as U.S. Military Advantage

NOVEMBER 2026

AUTHORS
Clete Johnson
C. Sean Spivey
Matt Pearl

In an ongoing paper series, the CSIS Strategic Technologies Program has explored the national security implications of spectrum allocation. The series has argued that it is a national security imperative for the United States to make additional spectrum available for commercial licensed, full-power 5G and future-generation terrestrial wireless technologies to secure its position as the leader in trusted networks. A comprehensive, long-term spectrum allocation policy will allow the United States and allied partners to thwart efforts by autocratic governments, particularly China, to dictate the development and deployment of spectrum-based emerging technologies.

An earlier paper in this series explored the nexus between spectrum allocation for commercial licensed use and the development of trusted technology. Harmonizing such spectrum allocations creates economies of scale upon which trusted technologies can be developed and deployed, thereby transforming smaller, discrete markets into global markets for new and innovative technologies. Companies need sufficient spectrum resources to innovate and manufacture advanced wireless technologies and components for commercial (as well as governmental) use. China recognizes this nexus and is acting accordingly. While the United States is not emulating Chinese spectrum policy (and should not attempt to do so), it must present a compelling alternative for other countries to pursue alongside the United States. Scale promotes commercial strength and technological innovation, both essential elements of U.S. national security.

This paper explores a related issue: the importance of commercial spectrum allocation to future U.S. and allied military operations and capabilities. Even with an approximately $1.5 trillion budget request for fiscal year 2027, the Pentagon, along with other U.S. executive departments and agencies, can

All views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).
© 2026 by the Center for Strategic and International Studies. All rights reserved.

benefit from leveraging the capabilities of commercial firms that are researching and developing emerging spectrum-based technologies—particularly dual-use technologies and applications. As the U.S. government acknowledged recently in its **National Security Science & Technology Strategy**, "The Federal Government must partner effectively with the private sector, recognizing that the private sector contributes critical capabilities that the government does not possess." A robust commercial wireless ecosystem drives a flywheel of innovation, producing trusted technology that can later be adopted by military forces and other governmental users. Commercial wireless networks enable the use of new artificial intelligence (AI) technologies in the physical world. Devices such as sensors and robots used by the military can benefit from commercial wireless networks to share data and computing resources. This relationship affects the range of AI technologies available to the military. At the same time, achieving these benefits requires ensuring that essential military operations are protected during and after spectrum transitions.

As this paper series has argued, spectrum policy is not and must not be a fight between commercial interests and national security. To the contrary, both commercial dynamism and military systems are indispensable elements of U.S. national security. Many of the same security concerns shape commercial networks and military operations on future battlefields, and trusted networks supporting advanced commercial activity today can provide critical infrastructure for sensitive military operations tomorrow. Maintaining a battlefield advantage requires U.S. and allied leadership in developing the technologies and standards underpinning AI, cyber operations, and battlefield communications.

U.S. Military Use of Commercial Spectrum at Home and Abroad

The U.S. military relies on electromagnetic spectrum for a broad array of operations and missions worldwide. Domestically, these uses include

- homeland defense, which involves the protection of U.S. sovereignty, territory, populace, and critical infrastructure against external threats and aggression;
- **Defense Support for Civil Authorities**, or support provided by the military in response to a request from civil authorities for domestic emergencies, cyber incidents, law enforcement support, or other special events;
- mobilizing military units for overseas deployment by moving personnel and equipment on the ground from home stations to aerial or seaports of embarkation; and

- equipping and training of the military forces—or in military-speak, "train as you fight"—through research, development, and testing of systems used for sensing, communications, and other operations.

These domestic needs for spectrum use are similar to U.S. military operational needs overseas. No matter the theater, the electromagnetic spectrum now plays a central role in essentially every aspect of the battlefield, both physical and cyber.

Specifically, there are three types of core functional operations that military units undertake using electromagnetic spectrum: (1) unit communications; (2) sensing and situational awareness; and (3) electronic warfare (EW) such as jamming, spoofing, and other manipulation of spectrum.

These functions are directly relevant to almost any conceivable warfighting scenario for the United States and allied militaries, such as defending Israel, South Korea, Taiwan, or Ukraine—particularly given newer developments in remote warfare, namely management of drones for offensive and defensive purposes. The same is true for possible direct combat, at home or abroad, with one or more of the United States' four primary adversaries: China, Russia, Iran, and North Korea.

As discussed further below, EW capabilities allow military forces to control spectrum and to attack or defend against enemies by disrupting, degrading, and denying an opponent's ability to use spectrum signals, and these tactics are becoming ever more central to warfare.

Whether at home or abroad, spectrum monitoring and management capabilities that derive from—or even operate on—commercial spectrum infrastructure will enable U.S. military units to perform these functions efficiently and decisively in combat. Federal government **policy** already requires that all functions normally associated with providing telecommunications services for the government's own use must be performed by the private sector except in limited circumstances, namely, only where a commercial service is not available to the federal user during the time needed, is not adequate from a technical or operational standpoint, or would be significantly more costly. Leveraging commercial 5G networks for advanced warfighting capabilities is consistent with this general policy.

Commercial Supply Chain and U.S. Military Operations

Part I of this series, released in 2024, focused on trusted supply development, as the United States was falling behind in spectrum leadership. Circumstances have changed significantly since then, with Congress **enacting** the Working Families Tax Cuts Act in July 2025. The law includes a provision **requiring** a

pipeline of 800 megahertz (MHz) of new spectrum for commercial wireless use, with the U.S. government directed to identify 500 megahertz of mid-band spectrum frequencies for reallocation to non-federal use, shared federal and non-federal use, or a combination thereof, for full-power commercial licensed use cases. Subsequently, President Trump **issued** a Presidential Memorandum in December 2025, "Winning the 6G Race," in which he established "the policy of the United States to lead the world in 6G development," including by "identifying a significant volume of radiofrequency spectrum that can be harmonized for 6G networks internationally." The National Telecommunications and Information Administration is studying four key spectrum bands to satisfy this statutory directive, including the 1675–1695 MHz, 2690–2900 MHz, 4400–4940 MHz, and 7125–7400 MHz bands.

Finding solutions for commercial access to mid-band spectrum is crucial for military operations. For supply chain security reasons discussed in the **earlier paper**, fighting in the "friendly virtual terrain" of trusted networks is a vital operational advantage in modern warfare. This is the case for all military missions and operational capabilities pertaining to spectrum, including EW. As noted in the **National Security Science & Technology Strategy**, "The United States must guard against foreign adversary exploitation of critical technology systems and supply chains," including communications and network systems.

Greater access to internationally harmonized commercial spectrum, particularly bands harmonized among the United States and its allies, strengthens the market for trusted equipment and components, expanding the size of the supply base available to the U.S. and allied militaries—thereby enabling them to compete with the PRC's scale.

China's Digital Silk Road strategy for technology infrastructure has become a major component of China's Belt and Road Initiative, which focuses on global transportation and logistics infrastructure built by China-based companies. Digital Silk Road support helps further advance (or entrench) China-based "national champion" technology companies in other countries' communications and technology infrastructure. These investments **ostensibly** serve the purposes of improving recipients' telecommunications networks, but they also provide advanced surveillance technology and AI capabilities for China wherever an untrusted vendor builds and operates a network. China-based equipment and services in commercial networks that may be pertinent to warfighting would provide the People's Liberation Army multiple layers of operational advantage in a conflict.

Consider the acute example of a potential U.S. and allied defense of South Korea in the case of a North Korean and/or Chinese attack. Any U.S. servicemember in the Indo-Pacific knows that among the most urgent U.S.

missions in such a scenario is the logistical surge (e.g., ships, aircraft, trains, and other transport capabilities) that will quickly bring tens of thousands of U.S. and allied troops and millions of tons of military equipment, weapons, and ammunition to the Korean peninsula.

Much of this logistics operation would involve seaports such as those at Pohang, Inchon, and Busan. The United States focuses intently on all aspects of the security of its seaports and would never want untrusted vendors to provide connectivity infrastructure at U.S. ports. Likewise, security is presumably one reason South Korea decided to bypass **Huawei's smart port offering**, instead turning to Samsung to help **construct** Busan New Port, which uses **automated** guided vehicles in its terminal. Such ports illustrate how connectivity, automation, and AI converge: a commercial ecosystem that supports intelligent cargo handling and vehicle coordination can also provide the key building blocks of military mobilization and logistics.

The U.S. military would begin with a severe operational disadvantage in any warfighting mission where it needed to navigate logistics in a port in which an untrusted vendor has wired connected. Likewise, for purposes of unit communications, sensing and situational awareness, and minimizing EW threats, the more global market share that untrusted equipment and services gain in global networks—at seaports and otherwise—the worse the operating environment for U.S. and allied forces in wartime. The inverse is true for networks developed, equipped, and serviced by U.S. companies and those based in trusted allies.

Put simply, supply chain security is military operational security. As discussed in the **earlier paper**, the nexus between licensed spectrum availability and deployed equipment means that "networks and applications will be designed either to advance the principles that support the United States and its market-democratic allies or to serve . . . the deepening autocratic alliance of China, Russia, Iran, and North Korea." This is true both in peacetime and in war. These principles are foundational to the **agreement** among the United States and 24 other allied nations enshrined in the Call to Action for 6G Leadership and Security, which senior Trump Administration officials **refer** to as the "imperative" of developing "allied scale."

Maintaining Spectrum Management Leadership to Maintain Battlefield Advantage

Even with a secure supply chain, the importance of spectrum monitoring and management capabilities will continue to increase in future operational warfighting scenarios. It is essential for the U.S. military and allied forces to be able to interoperate in available spectrum bands; harmonizing U.S. spectrum allocations

with allies' allocations helps ensure that U.S. military systems can operate with wireless equipment in other countries where U.S. forces may be needed.

Technologies that rely on spectrum are, of course, essential tools for modern warfare. Using devices connected to 5G networks, modern forces can deploy sensors across battlefields and in and around other areas of conflict, communicating with up to one million **devices** per square kilometer. Automation and AI systems can use these sensors for efficient mobilizations and to develop efficient supply chains in the event of large-scale armed conflict with peer or near-peer adversaries. The usefulness of AI applications relies both on the accuracy of the underlying models and on the availability of timely data to appropriate end users. Capabilities of commercial wireless networks can help facilitate information sharing for AI applications. On-device and edge computing can help reduce reliance on data centers. These sensors also support troop safety by enhancing the deployment of unmanned aircraft systems or detecting small enemy drones.

The benefits of commercial 5G spectrum access in warfighting or other defense scenarios are not theoretical—they have been demonstrated in **live network environments**. Last year, Telia, Nokia, and the Finnish Defence Forces **successfully tested** a continuous and secure data connection over a dedicated slice of Telia's commercial 5G network across the borders of three separate NATO countries. This type of cross-border connectivity over reserved 5G network capacity is only possible, however, if interoperable and standardized spectrum is available in multiple countries, and if original equipment manufacturers are willing (and able) to provide network technology at sufficient scale in these markets. Telia has since demonstrated additional defense applications using 5G, such as connectivity for hydrogen-powered airships that operate in low altitudes and can serve as an alternative to satellite- or drone-based operations.

5G networks can also support the resiliency of Position, Navigation, and Timing (PNT) technologies used by military forces. At the Pentagon, PNT technology has long been "embedded in and essential to the effective employment of virtually all [defense] systems," including navigation for planes, ships, and munitions as well as for communications networks. GPS is the military's **primary** PNT technology for its operations. However, GPS signals are vulnerable to jamming and other disruptions. Russia, in particular, is capable of disrupting GPS signals, as seen in its effective use of **jamming technologies** in Ukraine. 5G-based PNT capabilities may serve as a domestic supplement to GPS in GPS-denied areas as part of a "system-of-systems" approach to PNT resiliency, particularly in urban environments where GPS efficacy is particularly challenging. The global wireless communications standards development body known as the **3rd Generation Partnership Project** has already completed significant standards work for 5G-based positioning services, which could be provided over existing wireless networks and infrastructure.

Additionally, the Russian military's **resistance** to allocating the 3.3–3.8 gigahertz (GHz) band for civilian applications may provide an opportunity for U.S. and allied companies. Because the 3.3–3.8 GHz band serves as the backbone for many other nations' 5G deployments, Russia has effectively handicapped 5G deployment within its own border. The United States and its allies should seek opportunities to provide equipment for commercial 5G uses that are interoperable with U.S. and allied military equipment, particularly in allied or partner countries close to Russia.

All of these considerations become increasingly important as spectrum-dependent capabilities in remote warfighting—including EW capabilities—improve and advance. Beyond operational flexibility, recent advances in EW have made spectrum-wide management instrumental to the future of warfare. The more spectrum that is available for commercial use in the United States, the more U.S. engineers will innovate in spectrum management, precision, interference management, and overall control superiority.

For example, the Defense Advanced Research Projects Agency (DARPA) launched the COmpact Front-end Filters at the ElEment-level (**COFFEE**) program in 2022. COFFEE first developed filter technology in the 2–18 GHz frequency ranges to protect wideband radar, communications, and EW systems from jamming and interference. Last year, the program transitioned to demonstrations at the system level, enabling integration into hardware and thereby validating performance in operational settings. **According to** DARPA, "[a] key goal is to highlight COFFEE's dual-use impact: enabling more resilient defense systems while also supporting commercial platforms, such as 6G and satellite communications."

To address such technological advancements, Russia has sought to ensure that it has more (and better performing) jamming **equipment** than Ukraine. A spectrum management **arms race** is underway in a cat-and-mouse game of rapidly improving technology and operational capabilities.

Electronic warfare on Ukraine's frontline has **focused** on the ability to use and defend from reconnaissance and strike drones as well as long-range missiles. Both Ukraine and Russia have invested substantial resources into developing autonomous and remote-controlled systems and **measures** to combat those systems. For example, Russian **jamming** has **successfully** used truck-mounted systems to block Ukraine's communications with drones and also U.S. and allied-made GPS-guided artillery shells, High Mobility Artillery Rocket Systems, and bombs guided by Joint Direct Attack Munition. Ukraine has **adapted** to Russia's jamming by relying on systems that do not depend on GPS, using other guidance mechanics, and changing the frequencies over which their drones operate.

Ukraine's **approach** to military use of drones and EW has leveraged experts and innovations outside the military, including from its private sector IT

experts. To promote rapid innovation, the Ukrainian military has **pivoted** from largely government-directed to private sector–led research and development. Ukraine's government is helping to **develop** its domestic tech sector through legal and regulatory changes and by building relationships and collaborations with international investors. Foreign companies also operate and test innovative technologies in Ukraine. For example, Latvian company Atlas Aerospace **designed** a smart frequency-hopping system to evade Russian jamming technologies.

The Ukrainian government is **funding startups** working on drones for military uses. **Brave1** is a funding and support platform for Ukraine's defense tech, and the **Ukrainian Startup Fund** finances early-stage projects, helps startups raise funds, and helps manage regulatory approval processes, including speeding up approval of unmanned vehicles. Ukraine's military has also partnered with companies providing relatively inexpensive anti-jamming solutions, such as using consumer phones to **identify** the existence of jamming equipment.

Conclusion

The technological battlefields of future wars must be optimized for U.S. and allied operations rather than those of adversaries, and U.S. and allied engineers and spectrum managers must be provided with the tools they need to succeed. A sufficient allocation of commercial, licensed, full-power spectrum will create commercial innovation at scale and promote critical AI deployment: spectrum policy builds the trusted wireless ecosystem through which AI-enabled military capabilities can be developed, tested, and deployed. In sum, stronger 5G (and next generation) wireless networks make a stronger warfighter, and it is to the United States' military advantage to facilitate robust commercial mobile wireless network connectivity at scale.

Clete Johnson *is a senior fellow (non-resident) and* ***C. Sean Spivey*** *is a senior associate (non-resident) with the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.* ***Matt Pearl*** *is director of the Strategic Technologies Program at CSIS.*

This project is made possible by support from CTIA and its members.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

© 2026 by the Center for Strategic and International Studies. All rights reserved.