Testimony of Clete D. Johnson

Senior Fellow,
Center for Strategic and International Studies

Partner,
Wilkinson Barker Knauer, LLP

U.S. Senate Committee on Commerce, Science, and Transportation

Hearing on

Spectrum and National Security

March 21, 2024

Spectrum and National Security

Chairwoman Cantwell, Senator Cruz, Members of the Committee, thank you for allowing me to share my perspective on spectrum and national security.

It is a special honor to be here today, as this Committee – and this very room, the birthplace of the NIST Cybersecurity Framework – have played such an important role in developing U.S. cybersecurity and network security policy. The bipartisan consensus that has shaped this policy over the past two decades, advancing the principles of technology innovation and dynamism and government-industry collaboration, in many ways began here.

With your leadership, we now have the opportunity to apply these principles to U.S. spectrum policy. This is absolutely crucial to the security of the United States and our allies, because spectrum policy is key to the future of the networks and applications on which our societies operate. Those networks and applications will be developed either by us, with the free market principles this Committee has long espoused, or by the deepening autocratic alliance of China, Russia, Iran, and North Korea.

It is that simple. The security of the United States as a free market democracy hangs in the balance. Fortunately, successive Administrations and Congresses have taken meaningful actions to address this threat, and now we have the opportunity to leverage spectrum policy in favor of our principles – dynamism, innovation, and freedom rather than surveillance, control, and oppression. This will require maximizing all critical uses of spectrum, from weapons and defense systems to commercial 5G and next generation wireless networks, including both local wireless connectivity and wide area coverage.

To secure our core national interests, we have to lead the world in all of these areas, and we can. However, right now we are in danger of falling far behind China in mid-band licensed spectrum that can support wide area coverage, which is critical to bringing mobile services and technologies to every part of the country. This is a grave threat to the security of our network infrastructure.

Addressing this severe licensed spectrum shortage while also maintaining our present world-leading position in defense systems and local wireless connectivity will be difficult. But as this Committee well knows, the United States is quite capable of accomplishing difficult technical achievements, particularly at the intersection of military capabilities and commercial strength. One example in the spectrum arena that I saw first-hand as an Army logistics officer in the late 1990s: The Department of Defense partnered with large industry players to develop and scale the RFID tag system for real-time global tracking of supply shipments, thereby revolutionizing supply chains and inventory management. This example is one of many reasons the United States leads the world in both military force projection capabilities and commercial dynamism.

We need to apply that type of solutions-oriented action to spectrum policy as well. As one astute colleague put it, spectrum availability is "an optimization challenge, not a scarcity problem." The invisible radio waves that make up the radiofrequency spectrum are a critical natural resource, and we can either argue over their scarcity or work together to optimize their use. Our economic and national security depends on making the right choice.

Why Does Spectrum Matter for Network Security?

There is a direct relationship between the availability of spectrum and the ability of manufacturers and innovators to enhance and expand the state of wireless technologies. Spectrum is the lifeblood of the wireless ecosystem, serving as a core component of the technology landscape and the mutually interrelated technology development processes. This relationship is not perfectly linear or sequential, but to be clear, our security interests depend directly on spectrum availability.

Wireless research and development, technology design, standards and intellectual property, and thus hardware, software, and the applications they enable – that is, the wireless network supply chain and capabilities – are specific to particular spectrum bands. If we view Huawei, ZTE, TikTok, and other China-based "national champions" as a threat, then we must view commercial 5G spectrum availability in the United States as an antidote to that threat.

In the future, we may achieve the technological ability to obviate the connection between particular spectrum bands and technology design and development, but that is not the present reality. That is one reason why we have had to expend billions of dollars (and still counting!) to "rip and replace" Huawei and ZTE gear, as those China-backed companies were the only suppliers that built radios for the spectrum bands on which many of our small carriers operated. We should never let that happen again.

It is a national security imperative to make commercial spectrum available for 5G and future-generation wireless technologies to secure the U.S. position as the leader in trusted network technologies as autocrats seek to take the lead. China's aggressive strategy to dominate technology in general, and 5G and future-generation networks and applications in particular, underscores the significant impacts that spectrum access and technology processes have on the security of the wireless supply chain and the applications the network enables.

There are two elements of this spectrum environment that are becoming security setbacks for the United States: (1) global harmonization and scale, and (2) U.S. capacity.

First, global harmonization and scale. The specific spectral frequencies available to commercial operators are indispensable to the ability of a trusted and commercially viable equipment market to develop in a harmonized environment. Wireless antennas, radios, and other network components are typically designed to operate under a band-specific framework. While future technology developments in chipsets, software, and artificial intelligence may enable wireless radios and equipment to operate without regard to spectrum-specific design, the ability of network equipment to speak different frequency "languages" is not likely to be achieved in the immediate near term. This further underlines the need for trusted and harmonized frequency availability, and for leadership by the United States and our allies.

Global harmonization of spectrum bands creates global scale for technology development, and developers that are designing for a large global market have significant tangible and intangible advantages over those that are designing for a smaller market bespoke user or use. The more that U.S. spectrum uses are harmonized with our allies and global markets, the more scale trusted suppliers have for secure technology development. In short, we need the world's technology discourse to take place in the spectrum bands in which we operate – the frequency "languages" that we speak – but we are in danger of giving away that position to China and its untrusted suppliers.

China knows that this starts with leading in the availability of licensed mid-band spectrum for wide-area coverage; today, it leads the U.S. by 2.5 times in access to these frequencies. For scale and market positioning purposes, China wants its developers to design equipment that speaks the frequency language most broadly spoken in the mid-band environment, putting it on a trajectory toward adopting or even leading globally harmonized spectrum. Meanwhile, the United States is becoming a mid-band spectrum island that operates largely outside of core globally harmonized spectrum bands; if this trajectory continues, the U.S. technology ecosystem will operate within a U.S.-only spectrum "dialect" that lacks influence and global scale.

The result of this dichotomy is that China-based national champions like Huawei and ZTE would gain enormous advantages across a variety of critical use cases and architectures. Connected vehicles are a prime example. The Department of Commerce's Bureau of Industry and Security (BIS) is currently examining the state of this marketplace to determine the threat landscape for foreign adversary influence over integral communications technologies and services associated with such vehicles. BIS is proposing a rule to govern transactions that might otherwise enable untrusted China-based suppliers to become embedded in this technology. Targeted restrictions can indeed be valuable, but as we have seen in the "rip-and-replace" setting, they are both costly and insufficient. It is necessary that U.S. and allied technology developers can compete with China-based developers at the same capacity and harmonized scale in the first place. The availability of harmonized spectrum is indispensable to that imperative.

Critically, the risks of autocratic leadership in essential wireless supply chain elements extends to federal and military uses of commercial systems as well. As Deputy National Security Advisor Anne Neuberger has highlighted, the security considerations that exist in a purely commercial setting are also central to the future battlefield. The technology ecosystem in which our warfighters will wage the battles of the future will be shaped by commercial spectrum availability for current and future generations of wireless. For operational warfighting reasons, it is crucial that future technology, standards, hardware, software, and applications – including AI, cyber operations, and battlefield communications – are developed by U.S. and allied companies with sufficient spectrum harmonization and scale to lead the world.

Second, U.S. capacity. As NTIA recently highlighted in its National Spectrum Strategy Implementation Plan, "U.S. leadership in next-generation technologies and services requires greater spectrum access for both the private and public sectors in the near- and medium-term." Indeed, it is essential that U.S. wireless companies have the spectrum resources they need to work alongside like-minded nations to innovate and manufacture advanced wireless technologies and their components – including chipsets, software, radios, and more – for use in both the commercial and federal sectors. Today, however, the United States is anemic regarding this critical network input for licensed wide area coverage, which will run out of capacity in the coming years unless we act with urgency to address the shortage.

Consider local wireless connectivity (for instance, WiFi in a building or home or office campus) as the "capillaries" of the wireless ecosystem, drawing on broadband service to nourish local applications and network functions. Our wireless capillaries are robust and healthy; the United States has far more unlicensed spectrum allocated than China or any other country, which is one of many reasons that WiFi is a resounding American success story. But the "arteries" of our wireless ecosystem – the licensed wide area coverage that provides mobile connectivity broadly across our vast continent – are already near capacity, with no further expansions presently in the spectrum pipeline. We have gone from leading the world on this metric to drastically trailing China and a dozen peer countries, and that deficit is expected to grow substantially in the next decade.

The existing disparity between U.S. licensed mid-band spectrum allocations as compared to the rest of the world is a major national security challenge, as it has created a platform for China to shape the near-term and future technology environment in its own strategic interest. China is ensuring that its mid-band arteries have plenty of capacity, while our 5G and next-generation mid-band wireless ecosystem is limited today and soon to reach its limits, putting a corollary structural bound on the ability of the U.S. to lead in these technology developments. This problem broadens the threat landscape throughout the global network technology supply chain, further highlighting the imperative of ensuring there are sufficient licensed spectrum allocations available to support U.S. innovations in wireless.

Addressing the Risks of the U.S. Spectrum Shortage

We must act urgently to optimize spectrum use so that the United States can lead in all key areas of the wireless environment. This optimization process should be organized to benefit all parties, so everyone comes to the table transparently and with an eye to mutual benefit and advancing the interests of the United States, rather than a zero-sum game with distinct losers and winners. The real loser in this zero-sum approach is U.S. national security.

This obviously must begin with restoring the FCC's statutory authority to auction spectrum. The ongoing lapse in this authority severely damages U.S. leadership, and thus U.S. security, every additional day it lasts. We need urgent action to restore auction authority in such a way that the studies of the bands identified in NTIA's Implementation Plan are not just academic, but instead lead to concrete advances in spectrum capacity and auctions for necessary licensed mid-band spectrum.

With this authority in place, stakeholders should work together collaboratively and with urgency to make spectrum optimization a reality, particularly in the bands identified for study in NTIA's Implementation Plan. Again, this process is not a zero-sum game; it should and will create mutual benefits. Federal agencies, including the Department of Defense, can maintain and in many cases upgrade or otherwise advance their vital operations, while commercial providers can build out innovative 5G networks nationwide to drive U.S. technological leadership worldwide.

Government and industry should collaborate on initiatives to maximize spectrum use in any given band. Most immediately, we must advance presently viable spectrum sharing regimes; when fully clearing a spectrum band for new uses is not practical, coordinated sharing through proven methods can be a solution. Government and industry should collaborate to advance "static" sharing, in which parties benefit from predictable spectrum access by coordinating their use over geography, time, or frequency. These sharing methods provide coordinated access and certainty, and technological developments are increasing the precision of these sharing methods. We should focus immediately on these proven models of sharing to advance our national interest in maintaining 5G leadership globally.

In parallel over the long term, we should also seek breakthroughs in "dynamic" spectrum sharing – in which each party's use of frequencies changes dynamically according to real-time needs – to overcome existing practical impediments to real-world implementation. Such breakthroughs will likely take years to become practically and economically viable at scale, and U.S. global leadership and collaboration with allies will be required to address the need for global harmonization and scale sufficient to support diverse and competitive trusted suppliers in such a sharing environment. Absent strategic leadership, bespoke U.S.-only sharing frameworks could mean we deploy more slowly than other countries that simply

implement globally harmonized, standardized frameworks, and the custom sharing solutions would be so circumstance-specific that they would have no global market.

In conclusion, U.S. spectrum leadership is directly pertinent to a secure supply chain and application ecosystem, and thus to our core national security interests. We must not walk away from globally harmonized bands and cede the supply chain to China. Rather, we must undertake immediate steps to maintain U.S. leadership in spectrum policy to secure the technology future.

This will require recognizing that spectrum policy is not a fight between commercial interests and national security. That binary frame is a false and dangerous dichotomy in the twenty-first century, when U.S. national security derives from economic strength and technological innovation as much as traditional sources of power.

I look forward to your questions.