



The Promise and Peril of 5G

May 21, 2019 **Richard M. Harrison** *The National Interest*

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; International Economics and Trade; Science and Technology; China

With increasing frequency, we are hearing about a revolution that is taking place in technological connectivity—one being spearheaded by the development of 5G (fifth generation) networks. But what can 5G do, really? Faster movie downloads and near instantaneous access to information on phones and computers is just the tip of the iceberg. Buoyed by greater bandwidth, faster speeds, and lower latency (the ability to transmit more data, faster, and with a quicker response time), 5G has far-reaching commercial and military applications. But 5G also presents serious national-security concerns that U.S. policymakers need to better understand and address.

The potential commercial implications of 5G are sweeping. They include revolutionized medicine through augmented and virtual reality, networked sensors in constant communication (paving the way for smart cities and smart roads for driverless vehicles), and a universal connection to the Internet of Things. The impact is expected to be nothing short of seismic; according to one market study, by the year 2035 5G-supported technology may generate as much as \$12.3 trillion in economic value and help to create 22 million new jobs.

For the U.S. military, meanwhile, such improved connectivity will translate into enhanced situational awareness, artificial intelligence that will help fly swarms of drones, and near real-time information sharing that will enable faster decision-making. However, 5G is also a shaping up to be a clear challenge to American primacy.

While America led the world in the creation of 4G networks, China is surging forward today in the development of its successor. Beijing has implemented a five-year plan that invests \$400 billion in 5G technology and has already built ten times more 5G domestic infrastructure than the United States.

America is likewise lagging in the race to roll out 5G globally. While U.S. telecommunication companies are still saddled with debt from the 4G rollout, China heavily subsidizes its “national champions,” Huawei and ZTE, by allocating a high percentage of domestic market share and providing financial incentives.

Beijing's grand plans include the “Made in China 2025” initiative, which prioritizes advancements in China's high-tech sector, and the vaunted Belt and Road Initiative (BRI), which leverages Chinese financing, manpower and technical knowledge to develop massive infrastructure projects throughout over sixty countries in Europe, Asia and Africa. Together, these efforts have enabled Chinese telecoms to begin to erect a “digital silk road” of 5G infrastructure around the world.

But the proliferation of this Chinese technology carries significant risks. As Bloomberg reported last year, China has already demonstrated an extensive ability to infiltrate major U.S. companies and the U.S. military through compromised computer hardware. It stands to reason that Beijing is doing the same in other countries as well. If foreign nations rely on firms like Huawei to install 5G equipment—firms that can be compelled under Chinese law to engage in espionage for Beijing—then there is the potential for Chinese tech to become a Trojan Horse.

It's no surprise, therefore, that Australia, Japan, New Zealand, and America, have opted not to include Huawei technology in their respective domestic 5G networks. FBI Director Chris Wray warned Congress last year of the risks “of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks.” Such penetration, Wray explained, “provides the capacity to maliciously modify or steal information, and...to conduct undetected espionage.” In turn, these concerns are codified in the Trump administration's recent Executive Order on the protection of telecom infrastructure and the supply chain from foreign espionage.

China's advances in 5G also carry negative implications for the U.S. military. A recent joint statement by several senior American military leaders noted that Chinese-led 5G infrastructure provides Beijing opportunities for forced data collection and could potentially compromise the integrity of future U.S. military operations. Moreover, they warned that this would give China's authoritarian government the ability to clandestinely collect private information from billions of people and use that data for coercion.

These worries are well-founded. China has already spent close to \$80 billion distributing technology that can be used to surveil or repress the populations in over fifty nations. If China provides 5G infrastructure to these countries, the U.S. military may be forced to maneuver around a “digital iron curtain” in future conflicts.

But slowing China's progress as a world leader in 5G is complicated. Due to government subsidies, China's telecoms are better positioned to offer 5G infrastructure to foreign customers, and to do so at much cheaper rates, than their U.S. competitors. Beijing also had the foresight to make inroads with the International Telecommunications Union (ITU), the international body that sets standards for global telecom, in order to influence the worldwide specifications for 5G in a way that has benefited Chinese companies.

Technical differences are also a problem. 5G can operate on various radio frequency bands in the electromagnetic spectrum, including low-bands (below 1 gigahertz [GHz]), mid-bands (1-6 GHz), and high-band (above 6 GHz). Higher frequencies translate to faster speeds, but a diminished ability for data to travel across long distances. Therefore, most countries are focusing on developing the mid-band spectrum for 5G coverage because it offers both good speed and broad area coverage. But U.S. carriers are today mostly focused on developing high-band spectrum to provide ultrafast coverage (particularly in urban areas) because the U.S. government and military owns and operates on most of the mid-band spectrum, preventing them from using it. As a result, it's difficult for U.S. telecoms to build out infrastructure in the area of the spectrum that will most likely be adopted globally.

Furthermore, China doesn't suffer from the same problem. As a recent Defense Innovation Board study noted, "as 5G is deployed across the globe... China's handset and internet applications and services are likely to become dominant, even if they are excluded from the U.S." In other words, the way American telecoms are developing 5G infrastructure isn't competitive globally. Because American firms can't compete as well, America is progressively ceding the emerging global marketplace for fifth-generation connectivity to China.

Potential Chinese 5G dominance represents a dangerous state of affairs. Unless the United States and its allies put forth a credible alternative plan for the development of global 5G infrastructure, America could soon find itself operating in a digital environment that is almost entirely dominated by Beijing.

Richard M. Harrison is vice president of operations and director of defense technology programs at the American Foreign Policy Council in Washington, DC.