

**TO:** National Security Community of the United States, its Allies, and Partners  
**FROM:** General James L. Jones, U.S. Marine Corps (Ret.)  
**DATE:** February 11, 2019  
**SUBJECT:** Recommendations on 5G and National Security

---

China's aggressive attempt to subsidize the development of global 5G networks as a tool of Beijing's geopolitical and economic power requires an urgent and robust, public- and private-sector response from the United States government, its allies, and partners to bring secure 5G technology to our allies. Allies and partners who choose Chinese technology over a secure 5G backed by the US will allow Beijing a backdoor into the defining technology architecture of the future and will undermine their future security relationship with the United States.

### **What is 5G?**

5G is fifth-generation wireless technology. It is a "disruptive" technology which, when used in its secure mode, will transform our societies in ways that we are only starting to understand. It is up to 100 times faster than current 4G networks, operates wirelessly, and over time could eliminate the need for fiber-optic cable in cities. 5G has low latency, meaning that networked devices can communicate with one another nearly instantaneously. 5G will allow the connection of billions of machines to enable the internet of things (IOT) and "smart cities" of the future. Simply put, 5G technology will revolutionize how we work, live, move, communicate, and make decisions. It will, for example, help driverless cars relay information to each other in real-time, warn manufacturers when machinery needs to be repaired, and help swarms of military drones communicate and identify targets. As society becomes more reliant on these networks, it is critical that we have "secure 5G" that is robust to cyber intrusions and attacks.

### **The 5G Technology Race**

The nation that leads in developing and widely deploying 5G technology will have an important first-mover advantage, with both economic and national security implications. Chinese national champion Huawei is the current global leader in 5G, and China's ZTE is also a major player in the industry. Huawei is aggressively pursuing export of its 5G systems to install digital infrastructure around the globe. Huawei is an attractive option to many nations because it is cheaper than its competitors. The products of firms competing with Chinese companies will be more expensive because of unfair subsidies from the Chinese Communist Party, which artificially reduce prices. Huawei is a tool of state power and a critical asset in China's global economic and geopolitical competitions and ambitions.

Huawei faces competition from Samsung USA and others as an end-to-end producer, and still other companies produce 5G components (such as antennae, chips, and base station architecture) including Ericsson, Nokia, and Qualcomm. These firms are more expensive because they are not the beneficiaries of unfair state subsidies. However, they offer other advantages, including enhanced security, more rigorous training of personnel, protection of intellectual property, and privacy. From a national security perspective, this race is not about US commercial market share, but rather mitigating China's ability to influence US allies and security partners.

### **Why is 5G Important for National Security?**

If China controls the digital infrastructure of the 21<sup>st</sup> century, it will exploit this position for its national security purposes and be capable of coercive leverage over the United States and allies. These networks will process all manner of data, and China certainly will use the network to conduct espionage on the

United States and allies for national security and industrial purposes. It will allow for the emplacement of “backdoors” in networks that could be activated to conduct catastrophic cyberattacks on US and allied “smart cities” in the event of conflict. Put another way, Huawei’s 5G technology is the 21<sup>st</sup>-century version of the mythological Trojan Horse. The spread of Chinese 5G networks will threaten NATO and allied interoperability, as the United States will become unable and unwilling to integrate its secure 5G network with any aspect of Chinese systems.

Finally, this race, and its outcome, rises to the level of importance of such projects as the Manhattan Project and the ‘man on the moon’ efforts of the 20<sup>th</sup> century. 21<sup>st</sup>-century security, both public and private, will be profoundly affected by the decisions taken in the next few months. For countries who select the Chinese alternative and the consequences attendant to such a decision, the costs of reversal will increase exponentially as they proceed.

For these reasons, the United States and several close allies (the United Kingdom, Australia, New Zealand, Japan, Canada, Poland, France, and others) have either banned or are considering bans on Huawei 5G systems. However, many other states, including US allies, have installed or are considering installing Huawei’s networks.

This is an urgent problem that will shape economies and societies for future generations. The infrastructure investment decisions that will determine the future 5G architecture will be made in the coming weeks and months, not years.

#### **Recommendations: What Should We Do Now?**

- The USG should launch a national campaign to inform the public about 5G and its critical importance to the economy and national security.
- The USG should conduct a robust diplomatic campaign to explain to US allies and security partners the serious risks associated with deploying Huawei, ZTE, and other Chinese telecommunications equipment.
- US allies and any nation concerned about the possibility of malign Chinese influence should halt work with Huawei and switch to alternate companies for the development of their 5G infrastructure.
- The USG should require that 5G technical standards be designed to withstand cyberattacks and work with Congress and industry to incentivize 5G cybersecurity. Building cybersecurity on the front end is cheaper than trying to add it at the back end.
- The administration needs to accelerate plans for a whole-of-government process to develop a long-term national spectrum strategy and the creation of an ongoing inter-spectrum (mid-band) for 5G that allows the US to synchronize federal, state, and local policies and procedures to facilitate the rapid and cost-efficient deployment of 5G network equipment.
- The USG should seek to streamline regulations and procurement practices and reduce impediments for 5G and IoT. This will reduce China’s autocratic advantages derived from its state-led capitalist approach.
- The USG should strictly enforce new Committee on Foreign Investment in the United States (CFIUS) and related legislation to carefully screen adversarial acquisition of emerging technologies and applications from US start-ups and smaller businesses.

---

**General James L. Jones is Executive Chairman Emeritus of the Atlantic Council, former Commandant of the U.S. Marine Corps, former Supreme Allied Commander, Europe, and former National Security Advisor to President Obama.**