STATEMENT BY FORMER U.S. MILITARY LEADERS - April 3, 2019

As military leaders who have commanded U.S. and allied troops around the world, we have grave concerns about a future where a Chinese-developed 5G network is widely adopted among our allies and partners. Our concerns fall into three main categories:

1. Espionage: Chinese-designed 5G networks will provide near-persistent data transfer back to China that the Chinese government could capture at will. This is not our opinion or even that of our intelligence community, but the directive of China's 2017 Intelligence Law, which legally requires that "any organization or citizen shall support, assist, and cooperate with" the security services of China's One-Party State.

2. Future military operations: The Department of Defense is still considering how it could use future 5G networks to share intelligence or conduct military operations. The immense bandwidth and access potential inherent in commercial 5G systems means effective military operations in the future could benefit from military data being pushed over these networks. There is reason for concern that in the future the U.S. will not be able to use networks that rely on Chinese technology for military operations in the territories of traditional U.S. allies or emerging partners in Europe, Asia, and beyond. While our concern is for future operations, the time for action is now. Physical infrastructure like ports can easily change ownership, but digital infrastructure is more pernicious because, once constructed, there are limited options to reverse course. This is even more true for Chinese telecommunications firms whose systems are not interoperable with other companies' equipment, cultivating a persistent reliance on the Chinese firm.

3. Democracy and human rights: The export of China's 5G technologies and suite of related digital products to other countries will advance a pernicious high-tech authoritarianism. If China is invited by foreign governments to build these networks, Beijing could soon have access to the most private data of billions of people, including social media, medical services, gaming, location services, payment and banking information, and more. This information will give China's repressive government unprecedented powers of foreign influence to favor authoritarian allies, coerce neighboring countries seeking to preserve their sovereignty, and punish human-rights activists the world over. This will make authoritarian governments more powerful while making liberal states more vulnerable.

We believe calls for the intelligence community to produce a "smoking gun" to illustrate Beijing's pernicious behavior misunderstand the challenge at hand. The Chinese Cyber Security Law and other national strategies like "Military-Civil Fusion" mean that nothing Chinese firms do can be independent of the state. Firms must support the law enforcement, intelligence, and national security interests of the Chinese Communist Party—a system fundamentally antithetical to the privacy and security of Chinese citizens and all those using Chinese networks overseas. The onus should instead be on Beijing to explain why it is prudent for countries to rely on Chinese telecommunications technology when Beijing's current practices threaten the integrity of personal data, government secrets, military operations, and liberal governance.

Admiral James Stavridis
USN (Ret.) Commander, U.S. European Command; U.S. Southern Command

General Philip Breedlove
USAF (Ret.) Commander, U.S. European Command

Admiral Samuel Locklear III
USN (Ret.) Commander, U.S. Pacific Command

Admiral Timothy J. Keating
USN (Ret.) Commander, U.S. Pacific Command

Lieutenant General James R. Clapper Jr.
USAF (Ret.) Director of National Intelligence

General Keith B. Alexander
USA (Ret.) Commander, U.S. Cyber Command & Director, National Security Agency