The Huawei Case Signals the New US–China Cold War Over Tech

ZACHARY KARABELL

03.11.2019 08:00 AM

The Huawei Case Signals the New US–China Cold War Over Tech

US allegations against China's Huawei are less about keeping Huawei out of American networks and more about the rest of the world.

WANG ZHAO/GETTY IMAGES

The deepening saga of the US government's campaign against Chinese tech company Huawei intensified this week, with Huawei filing a lawsuit in Texas alleging that the government's ban of Huawei equipment is "illegal" and based on propaganda, not facts. The case may not have much of a chance legally, but it underscores how this contest has become a microcosm of the larger competition between the US and China over who will define—and control—the technology of the 21st century.

Zachary Karabell is a WIRED contributor and president of River Twice Research.

The main thrust of the US push versus Huawei is that the company is inextricably bound with the ruling Chinese Communist Party and that its equipment, especially its superb 5G telecom equipment, will either be embedded with backdoors that will allow the Chinese government to spy or that it will have no choice but to permit Chinese government access to the traffic that flows through its equipment.

The clash is reminiscent of the Cold War, when the US and the Soviet Union vied to outfit other nations with planes and tanks. Now, the US and China clash over the technological infrastructure in Europe, Asia, Latin America, and Africa. Looked at through that lens, is Huawei's relationship to the Chinese government fundamentally different than the ties between the Pentagon and contractors such as Lockheed, Boeing, and General Dynamics? Is this just us versus them, dressed up as a defense of freedom and security, much as the Cold War was often about commanding the allegiance of most of the world and not about capitalism versus communism? It's a hard and uncomfortable set of questions, which we absolutely need to ask.

One brief against Huawei is that the company would be bound by the Chinese National Intelligence Law compelling it to give the government access to networks, an argument that the company vehemently rejects. At the Mobile World Congress in Barcelona last month, US government officials aggressively pressed Europeans to reject Huawei as a supplier of 5G equipment largely on those lines. Some countries such as Poland were receptive, but major Western European nations such as Great Britain, Spain, and Germany were unconvinced that Huawei represented a security risk fundamentally different than other suppliers.

In fact, while there is almost universal concern about the potential dangers of Huawei's ties to the Chinese government, sotto voce many countries and executives see the US asserting a double-standard and attempting to freeze out a rival for trillions of dollars of business around next-generation telecom networks.

That's because there are a limited number of global providers of equipment, and each can be seen as compromised. If you are, say, the government of India and you want to spur investment in 5G and upgraded telecom, you can buy from Huawei or Cisco or Ericsson or Nokia. As an Indian security official, you're faced with a series of problematic choices. You know, for instance, that the US National Security Agency has attempted to and has indeed (as Edward Snowden's leaked documents showed) embedded backdoors in US equipment or induced the cooperation of US tech companies to provide information and intelligence on foreign targets.

Other countries look at the United States and see what can charitably be described as a fuzzy relationship between government and suppliers of sensitive equipment. Think of the cozy revolving door between the Defense Department and senior ranks of major contractors such as Boeing, Lockheed, Raytheon, and General Dynamics. Acting secretary of defense Patrick Shanahan comes from a 30-year career at Boeing; hundreds of former Defense Department officials have in turn been hired by those companies. While there are laws constraining lobbying by former administration officials, those haven't usually prevented the easy back-and-forth flow of personnel, contracts, and ideas between the Defense Department and its suppliers.

There's less clarity about the interaction between tech companies and US law-enforcement and intelligence agencies. There have been a few high-profile instances where companies pushed back on requests, most notably Apple's refusal to help the FBI crack the cellphone of a shooter in the San Bernardino attack in 2016. But it is equally true that all of the big tech companies have sold equipment and data that aids intelligence agencies, whether it is granular Google Earth imagery used by the NSA, Amazon developing facial recognition technology for US Immigration and Customs Enforcement, or Palantir serving as an outsourced data scientist for the government.

Whatever your stance on these intersections, if you are not American or Chinese, it can be difficult to discern how arrangements between the US government and American technology companies differ fundamentally from relationships between the Communist Party and Chinese technology companies. In a world where the two increasingly dominant technology superpowers, China and the US, are jockeying for position globally, other countries and foreign companies see all choices as potentially compromising their own domestic security. Or to put it differently: Who do you want spying on you, the Americans or the Chinese? If it's going to be both, how do you best protect yourself?

In that light, Washington's fight against Huawei looks less like a clear case of defending against Chinese government espionage and cyber threats. It looks more like a cyber version of a new Cold War, where the United States and China are both attempting to line up proxies and divide the world into technology spheres of influence. It comes down to whose side you're on, and not whether Huawei's equipment makes a user more vulnerable, especially if all equipment makes users vulnerable.

For now, much of the world seems to be choosing to mix and match equipment from multiple companies and countries, presumably to make it harder for any one to exploit backdoors and protocols. They are all starting with the maxim that they have no privacy and are working to make the best of that. But we're in the early stages of this contest, which transcends Huawei and will soon encompass ever more players in a morphing three-dimensional chess game.