CHINA US Focus

Blacklisting Huawei Could Cost Trillions, So Let's Look Before We Leap

Daniel Ikenson

July 5, 2019

Last weekend in Osaka, the U.S. and Chinese presidents agreed to resume bilateral talks to resolve the yearlong trade war. That decision was conditioned upon Xi Jinping's agreeing to increase purchases of U.S. agricultural products and Donald Trump's agreeing to defer any new tariffs on Chinese products. It also required Trump to relax the restrictions his administration imposed in May on U.S. companies transacting with Huawei Technologies.

The Huawei concession isn't sitting well with the likes of Senators Marco Rubio (R-FL) and Chuck Schumer (D-NY). They and other China hawks in Congress believe Huawei presents an intolerable risk to national security and are vowing to find a legislative solution that takes decisions about the Chinese technology giant's fate out of Trump's hands.

They may be right. Huawei may present an intolerable national security risk. After all, it is the most successful and recognizable firm in an industry that has benefited from years of Chinese indigenous innovation policies and subsidies. It produces gear that facilitates crucial communications, but also nefarious activities, such as eavesdropping, surveillance, and other forms of espionage. The company seems to enjoy a privileged relationship with the Chinese government and the Chinese Communist Party. There are a good number of examples and a lot of seemingly credible evidence that the company has violated U.S. export control laws, stolen U.S. intellectual property, and produces components that have been found to contain backdoors and other vulnerabilities to cyber malfeasance.

But there are also some big problems with the case against Huawei. Foremost is that the allegedly damning evidence remains classified. And some of those who have presumably seen or been briefed about that classified information—people like President Trump, British Prime Minister Theresa May, and German Chancellor Angela Merkel—are apparently unconvinced that the threat cannot be mitigated through measures less extreme than a total ban on Huawei gear. For example, rather than ripping out all Huawei components from its network, British Telecom is taking a more surgical approach, after concluding that the threat is not as pervasive as U.S. officials portray it to be.

The contention that Huawei represents a national security threat because it could channel intelligence or trade secrets or other proprietary information to the Chinese government, or that

is could enable state-directed cyber-attacks on critical U.S. infrastructure is certainly plausible. But it's also plausible that Huawei is in the crosshairs of U.S. policymakers because it threatens U.S. technological preeminence. Earlier this year Trump tweeted that he wanted the United States to "win through competition, not by blocking out currently more advanced technologies" when it comes to 5G.

These differing threat level determinations are important and should give us pause before we commit to a course of action that will be astronomically expensive and difficult to reverse. Cyberespionage, cybertheft, and other forms of cyber malfeasance present genuine threats that governments have a legitimate interest and obligation to protect. But cybersecurity measures cannot be considered in a vacuum, as if there were no costs to weigh against the expected benefits.

The U.S. Congressional Research Service estimates that by 2035, global revenues generated from developing 5G infrastructure and producing 5G enabled devices—products like smart appliances, wearable heart monitors, and autonomous vehicles—will amount to $12.3 trillion. A U.S. ban on Huawei components and U.S. efforts to dissuade other governments from using Huawei gear will delay development and the roll-out of 5G networks around the world, which will limit the expansion of "internet of things" industries, depriving people of life-enhancing technologies and the global economy of sources of economic growth.

As the low-cost provider of high-quality network gear, Huawei has made deep inroads into the telecommunications networks of countries around the world, including in rural America. Whereas Huawei gear accounts for a mere one percent of the overall U.S. telecommunications equipment market, it is much more prominent in rural areas. The specter of local carriers having to devote the preponderance of their resources to replacing Huawei components with more expensive equipment from Lucent Technologies or Ericsson, means that expanding high-speed internet services in rural parts of the country will be delayed for years to come.

Meanwhile, those costs likely will be too much to bear for developing countries in Africa and elsewhere, where Huawei components are ubiquitous in communications networks. Forcing governments to choose between Huawei and western alternatives likely will perpetuate a race between Washington and Beijing to carve up the world into spheres of influence based on competing 5G standards. Dividing the world into these competing spheres likely will deprive the technology ecosystem of global economies of scale and open the door to bloc-based tariffs and other forms of protectionism, making the world a poorer place.

It is reasonable to conclude that Huawei presents some degree of threat to U.S. national security, but one that likely can be mitigated through measures less comprehensive than banning all forms of commerce. But if U.S. policymakers are going to insist on the more extreme measure, they should be compelled to share the conclusive evidence first.

Dan Ikenson is director of Cato's Herbert A. Stiefel Center for Trade Policy Studies, where he coordinates and conducts research on all manner of international trade and investment policy.