Is safety the real reason to ban Huawei

Those who remember Sputnik – and lived through the space race between the U.S. and the Soviet Union – may recognize a similar thread of techno-nationalism in today's efforts to develop and introduce 5G mobile technology. Everyone wants to be first. They want "their side" to win. But is that the best way to build the strongest and most secure networks for people around the world?

5G is not just a faster Internet connection for your smartphone. It is the foundation of tomorrow's digital economy, powering everything from banks to hospitals to civil aviation and the management of cities. Unlike previous innovations in network technology, 5G has become colored by politics and now Huawei – the world's largest telecommunications equipment provider and second-largest smartphone maker – faces unprecedented scrutiny, and even legal challenges under the guise of network security.

Right now, Huawei is roughly a year ahead of its competitors in terms of 5G capabilities. We are the only company that can provide end-to-end 5G systems – from smartphone chips to wireless base station antenna to network routers and switches. Huawei has invested heavily in 5G research over the past decade, and since 5G standards were finalized in mid-2018 we have signed more than 30 contracts and agreements with more than 50 customers, and shipped more than 30,000 5G base stations to Europe, Asia, and the Middle East. This year, we will launch smartphones powered by 5G chips. These customers would not buy 5G equipment from Huawei if they did not trust us.

Our success has alarmed our critics. Huawei's detractors say we cannot be trusted because we are Chinese, and pressure from the U.S. has led some countries to consider the security implications of having Huawei equipment in their networks.

Despite what has been suggested in the media, there has never been a major cyber security incident involving Huawei, nor has anyone ever produced evidence of any security problems with our equipment. Huawei is the most audited and inspected company in the tech industry. For example, we have set up testing facilities where customers and independent third-party experts can examine our products. We offer

these experts access to our source code and hardware schematics. No other vendor of telecoms equipment provides such a high level of transparency.

Last November, Huawei opened a testing facility in Bonn and we will open another in Brussels early this year. In the UK, government representatives for the past eight years independently managed a Huawei testing center. We have offered to build a cyber security center in Poland and hope to do so soon. As part of our continued commitment to security, we will invest more than US$2 billion over the next five years to further upgrade our software engineering processes with the aim of making our network equipment more secure.

Given all of our security measures and the fact that there has been no evidence of any major issue in the past 30 years, why is the U.S. up in arms? It is difficult to believe that a handful of U.S. politicians know more about how to secure telecommunications networks than the companies that actually build and run those networks. Moreover, keeping out individual companies does not improve security. Blocking Huawei may help politicians score points on social media, but it does nothing to secure telecommunications networks.

Equipment bans create an illusory sense that the problem of security has been dealt with. But strip out every bit of Huawei gear from your network and a hack bot still won’t care about the nationality of the equipment. Vulnerabilities in the global supply chain mean that any technology can be compromised, virtually and remotely, from any location in the world. Sometimes derided as “cyber security by logo,” blocking individual companies is an approach advocated by politicians and others who appeal to emotion. Real security experts advocate a rigorous program of testing for all vendors, regardless of where their headquarters may be located.

If Washington is truly concerned that Beijing could force Chinese companies to spy for them, they should look beyond targeting individual companies. Huawei has succeeded because customers and consumers like our products – and trust them. If evidence against Huawei exists, the U.S. should present it. If 5G is going to support tomorrow’s complex digital systems, those systems must be made secure. That can be done only through collaboration among governments, regulators, and technology companies around the world. Let’s leave politics to the politicians and focus on the development of safe and well-protected next-generation networks.