Huawei, my way or the highway: Which way should the EU turn?

by Ian Bond

18 June 2019

On May 15th, US President Donald Trump declared "a national emergency with respect to the threats against information and communications technology and services in the United States". His action seemed designed to shut China, and specifically the telecommunications giant Huawei, out of the US market for 5G technology. On May 23rd, however, Trump appeared to suggest that he might be willing to ignore security concerns about Huawei as part of a trade deal with China.

Trump's first statement signalled an escalation of the conflict between the US government and Huawei. The US alleges that Huawei has links to Chinese intelligence and has violated US sanctions by supplying products incorporating US technology to banned destinations, including Iran. His second muddied the waters, suggesting that US security concerns would vanish if China offered the right trade deal. In a similar move last year, China's other major telecommunications equipment provider, ZTE, was accused of breaching US sanctions on Iran and North Korea, but was spared punishment by Trump after China's President Xi Jinping persuaded the North Korean leader, Kim Jong-un, to agree to a summit with the US.

The Huawei dispute exemplifies a wider problem for the EU: as the US increasingly treats China as a "foreign adversary", it also puts other countries under more pressure to take sides. If the US prohibits the inclusion of essential US technology in Huawei's hardware, it will effectively force European countries to opt for other suppliers. But Europeans fear that if they exclude Huawei from their 5G networks, only for Trump to reverse course, they risk Chinese retaliation and commercial disadvantage.

Despite its 'special relationship' with the US, the UK faces this dilemma too. The UK is reportedly planning to allow Huawei to supply certain kinds of 5G equipment regarded as less of a threat to Britain's network. After a public warning by US Secretary of State Mike Pompeo against allowing "open doors for Beijing's spymasters", officials were braced for Trump to threaten to reduce US intelligence co-operation with the UK; but in his press conference with Prime Minister Theresa May on June 4th he said "We have an incredible intelligence relationship and we will be able to work out any differences".

European countries are in a quandary. The decision to ban or not to ban Huawei on national security grounds is one for individual member-states – they cannot leave it to the European Commission to make

the choice and take the blame (even if some would prefer to). Most think that the risks are over-blown and would rather not put their security ties with the US or their hopes of future Chinese investment at risk. Though Huawei is ostensibly a private company, the Chinese government has threatened dire consequences for those who follow the US example. The Chinese ambassador in London, Liu Xiaoming, warned that it would send "a very bad and negative signal" to potential Chinese investors.

European companies are also in a tricky position. For instance, only days after announcing the launch of 5G in the UK in July, with Huawei handsets and domestic routers as options for consumers, Vodafone changed its 5G plans after US technology giant Google announced that it would not supply its Android operating system for new Huawei devices or upgrade it on existing ones. Vodafone's rival EE took similar action, but will still have Huawei equipment in parts of its core network until 2022. If the US carries out its threat not to allow telecommunications firms using Huawei equipment to connect to US networks, a company like the German T-mobile, with networks in Europe and the US, will find it difficult to operate.

After earlier optimism about the economic boost Chinese investment would bring, in recent years European countries and companies have joined the US in becoming more worried about China. Concerns include its theft of intellectual property, its use of state subsidies to enable Chinese firms (including Huawei) to undercut their foreign rivals and potentially drive them out of business, and its willingness to exploit economic ties to generate political leverage. At the same time, the EU feels that in the absence of hard evidence that Huawei is helping the Chinese government to penetrate European telecommunications networks, it cannot simply ban the company as the US has.

The EU has slowly been taking steps, however, to ensure that Chinese activity in Europe is subject to more scrutiny. The investment screening regulation entered into force in April 2019 and will be fully operational in October 2020; it will allow the Commission and member-states to raise concerns about foreign investment in sensitive sectors (though it leaves the final decision to the member-state in which the proposed investment would take place). In March, the EU issued recommendations on cybersecurity for 5G, declaring "Any vulnerability in 5G networks or a cyber-attack targeting the future networks in one Member State would affect the Union as a whole", and noting that member-states can refuse to allow foreign companies into their 5G networks if they pose a threat to national security.

These steps were clearly (though not explicitly) aimed at China. In case the message was not clear enough, the Joint Communication on China, also issued in March 2019, contains a lengthy section on the steps needed to mitigate possible security risks to critical infrastructure.

In some respects, the Huawei issue shows the EU behaving like the US and the US behaving like the EU: the Union normally champions the precautionary principle, banning (for instance) the import from the US of hormone-treated beef without having proof that it causes harm to human health. The US usually complains about the EU's application of the precautionary principle and argues in favour of risk management. On Huawei, however, the EU is arguing for risk management, while the US is pressuring EU countries to ban Chinese firms from the market entirely, without providing evidence that their involvement in 5G would be harmful. Ironically, among the companies that will benefit if the EU follows the US lead are two of Huawei's European competitors, Sweden's Ericsson and Finland's Nokia. Ericsson earns more in the US, where it faces no competition from either Huawei or a US alternative, than in Europe (where Huawei is still very successful).

The EU cannot stop Trump mixing trade and national security. But it can and should discuss with the US the range of risks associated with procuring equipment from Huawei, and then consider whether they can be eliminated or effectively managed.

First, there is the risk of espionage. The EU and US both want to make it harder for China to conduct espionage against Western governments, or steal technology from Western firms. But China has conducted highly successful espionage operations without Huawei equipment: between 2012 and 2015 hackers believed to be associated with the Chinese intelligence services managed to extract sensitive data (including finger prints and security questionnaires) relating to 22 million current and former US public employees from the computers of the US government's Office of Personnel Management. And Beijing has compelled Western investors in China to transfer technology to their Chinese partners as the price of doing business – though at the EU-China summit in April 2019 the two parties agreed in their joint statement that "there should not be forced transfer of technology".

It is hard to tell whether Huawei's involvement in 5G would make things much worse. The US seems to be concerned that even if Huawei's products were flawless at first, the Chinese government could oblige the company to use updates to create openings. Huawei has suggested 'no spying' agreements with its Western partners, but it is unclear how these could be policed, or why the Chinese government would respect them. There may be ways to mitigate the risks, however, for example by keeping Huawei equipment out of government communications networks and other sensitive facilities, or (as the UK apparently intends) limiting the types of equipment it supplies.

Second, there is the risk of hacking and cyber-attacks, including on critical infrastructure, from whatever source. Huawei's approach to cybersecurity seems to be haphazard. The British government obliged Huawei in 2010 to fund a facility in the UK, the Huawei Cyber Security Evaluation Centre (HCSEC), "to mitigate any perceived risks arising from the involvement of Huawei in parts of the United Kingdom's (UK) critical national infrastructure". The latest report from its Oversight Board records serious security concerns arising from poor cybersecurity practices within Huawei; it does not say whether it regards any of these practices as deliberate. The board concludes that it cannot guarantee that "all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term".

Eventually, 5G will be an integral part of the infrastructure for driverless cars, industrial processes, telemedicine (including remote surgery using robots controlled by doctors far from their patients) and much more. One fear is that in a time of crisis, the Chinese government could force Huawei to turn off such systems or allow China to interfere with them to cause disruption. But without the highest level of cybersecurity, 5G will also be vulnerable to criminals seeking to steal personal data, commit fraud or blackmail users reliant on the technology – a problem explored by Camino Mortera-Martinez in a CER policy brief, 'Game over? Europe's cyber problem', in 2018. Not only do most EU member-states not have an equivalent of the HCSEC, but the EU-wide cybersecurity certification framework (which applies to all suppliers, not just Huawei) is only voluntary. Given the extent of data flows between them, the EU and US should work to develop common cybersecurity standards, and the EU should move to a compulsory certification system.

Third, there are industrial policy concerns. The EU does not want Huawei to use easy access to low-cost finance and other Chinese government subsidies to drive European firms out of business and monopolise 5G provision. According to a recent report by the Henry Jackson Society, thanks to such

support Huawei has been able to undercut European competitors by 18-30 per cent. The European Commission wants a high quality 5G network based on healthy competition between suppliers, not a Chinese monopoly. On the other hand, banning Huawei entirely would delay the roll-out of 5G in the EU, postponing the productivity benefits it is supposed to bring. Paradoxically, through its European subsidiaries, Huawei takes part in some EU-funded research projects designed to give the EU a head-start in 5G technology – including as a research partner of its main competitors. Existing WTO rules on state aid are inadequate to deal with the Chinese system, but reforming them will take many years. At a minimum, as long as Huawei benefits from unfair Chinese government support, the EU should not allow it to take part in EU-funded research projects (still less to control any intellectual property produced by them).

In the end, the US can make it hard for Huawei to operate outside China. The firm relies on chips from US manufacturer Qualcomm, the supply of which the new US rules would prevent. Without Google's Android operating system and other applications for Huawei handsets, they will lose market share outside China (Huawei does not use Google products in China). But heavy-handed US sanctions will stoke resentment among European consumers and damage Huawei commercially, without eliminating the threats that Washington (and Brussels) worry about. It would be much better to try to find a co-operative approach that raises all-round standards of cybersecurity and promotes fair competition between any 5G providers that meet the higher standards. And if the EU can keep trade policy and national security issues on separate tracks, so much the better.

Full disclosure: Vodafone, BT (the owner of EE) and Qualcomm are corporate members of the CER. The views expressed here, however, are solely the author's, and should not be taken to represent the views of those companies.

Ian Bond is director of foreign policy at the Centre for European Reform.