National security and cybersecurity risks stemming from Huawei

30/05/2019

TMT analysis: Emily Taylor, CEO at Oxford Information Labs, associate fellow with the International Security Department at Chatham House and editor of the Journal of Cyber Policy, explains some of the concerns surrounding Huawei and the broader political and security issues.

What are the concerns about Huawei?

Huawei is one of China's first global technology firms, growing from humble origins with startup capital of US$5,000 in 1987 to a US$100bn turnover in 2018. Unlike other Chinese tech giants, which blossomed in domestic markets while shielded from international competition, Huawei had to make its fortune overseas.

It is claimed that 80,000 Huawei staff are engaged in research and development, and in 2018, it overtook Apple as the world's second-most popular mobile handset provider. But its core business is telecommunications infrastructure—a lucrative market with few competitors.

There are two principal concerns raised about Huawei:

- national security
- cybersecurity risks

National security risks

What exactly is the nature of Huawei's relationship with the Chinese state? As a young man, the company's founder Ren Zhengfei served in the People's Liberation Army. The company's ownership structure and funding sources are opaque. Those familiar with the business environment in China point out that it is difficult for a company to thrive without links to the regime. The Chinese state has been accused of mounting hostile cyber operations, and the US in 2015 indicted members of the People's Liberation Army for alleged theft of western intellectual property.

National laws in China require providers of critical communications infrastructure to share data and cooperate with the state, and any operator sitting at a low level in a network will have ample opportunity to intercept, distort or exfiltrate data, should it choose to abuse its position.

The US knows from experience just what can be achieved when a state can access data from its home-grown tech giants. National security concerns about Huawei are plausible and are shared across the political divide in the US. Depending on your viewpoint, it's natural, or convenient, that if evidence exists, it will be classified.

Huawei denies being owned or controlled by the Chinese state.

Cyber security risks

The next generation of mobile broadband, 5G, will be an enabler of the internet of things, machine to machine communication, smart cities, driverless cars, wearables, and much more. The volume of digital chatter, already mind-boggling, is expected to balloon exponentially, and the threat landscape will increase accordingly.

In late March 2019, the UK's National Cyber Security Centre (NCSC), the civilian branch of the UK's signals intelligence agency, the UK Government Communications Headquarters (GCHQ), published its annual Huawei oversight report. The report makes for grim reading, pointing up serious defects in Huawei's processes and software. Huawei has pledged a multi-billion-dollar, multi-year refactoring exercise, but it made similar promises last year and the NCSC report notes that little progress has been made, beyond aspirational statements by Huawei that it will improve.

Any network that enables remote access (eg, for network administration) also has the potential to be compromised by an adversary. The 5G network will be different in nature to its predecessors, being fundamentally a software-driven,

cloud-enabled network. On any rational analysis, having a company with buggy software at the core of such a network poses a major cybersecurity risk.

Why are these concerns being voiced now?

The US and China are engaged in high-stakes trade negotiations. At the same time, many states are awarding contracts to build out the fifth generation of super-fast mobile broadband, 5G, which are significant, long-term investment decisions. Huawei has found itself at the centre of a geopolitical perfect storm.

Since December 2018, these tensions have escalated into action. Huawei's Chief Financial Officer (CFO) was arrested in Vancouver, Canadian nationals have been detained in China, tariffs have been imposed, and in May 2019, the US President issued an Executive Order citing a 'national emergency', and placed Huawei on a list of entities with whom US companies are prohibited from trading without a licence.

The ban had an immediate, dramatic impact on global markets. Google announced that its Android platform will no longer be available in Huawei handsets. UK chip designer ARM will cease supply of technology that underpins most smartphones on the planet. These responses exposed the global interconnectedness of tech supply chains. The impact on US business, including many SMEs who supply Huawei, may have influenced the US decision to impose a 90-day temporary general licence, neutralising the ban just days after it came into force.

Is this about more than cybersecurity?

On 28 May 2019, Huawei announced its intent to apply for summary judgment in its constitutional challenge to the US National Defence Authorisation Act. Currently, it is difficult to see how the cycle of escalation, measure and countermeasure can be broken.

While there are plausible security concerns—both national and cyber—relating to Huawei, there is more at play here. Trade negotiations between the US and China are stalling, with potential damage to the global economy. Each chess move in this story—from the arrest of Meng Wangzhou, Huawei's CFO, to the publication of indictments against her—have coincided with key stages in the US and China trade talks.

The US Executive Order was brought in on the basis of a cybersecurity emergency, then delayed. If there is a national emergency, how can a delay be justified? On 23 May 2019, President Trump conceded that while Huawei is 'very dangerous', it might be included in the trade deal, feeding speculation that US national security concerns are a pretext for aggressive economic nationalism.

To some extent, the US and China are running with earlier versions of each other's playbooks, with the US pursuing protectionist policies previously followed by China, while Xi Jinping's 'Made in China 2025' strategy seeks to re-position China as a technical innovator—a position that the US has held unchallenged for decades.

Is the UK's approach to use of Huawei technology different from the international approach?

Huawei has been providing telecommunications equipment in the UK since 2005. The company is now deeply embedded in the UK's 4G infrastructure, which will be used in the successor 5G networks. So, even if the UK decided tomorrow that Huawei poses a national security risk, it is unlikely that 4G networks would be ripped up and replaced.

Instead, the UK has adopted a risk management approach, establishing the Huawei Cyber Security Evaluation Centre in Oxfordshire, under the oversight of the NCSC. Huawei employees work alongside members of the UK intelligence community to build confidence in the products, and the annual report provides a measure of accountability. It's not a perfect solution—a staff of 35, however talented, will not be able to get across every line of code, or spot every vulnerability, but it is a rational, evidence-based approach.

The other key element of UK policy is competition. The 5G trials that have taken place in the UK adopt a multi-company strategy. When Vodafone launches its 5G offering in July 2019, Huawei will be one of the providers it relies on. So, other suppliers are involved in infrastructure provision, and no single entity has sole control of the network.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.