Written evidence submitted by Prof. Christopher Balding, Associate Professor, Fulbright University and an Associate Fellow at the Henry Jackson Society

The Security of 5G

Christopher Balding is an Associate Professor at the Fulbright University Vietnam as well as an Associate Fellow at the Henry Jackson Society and an expert on the Chinese economy, financial markets, and companies. He specialises in data and corporate irregularities within China. His work on Huawei and data discrepancies on growth and bank accounting have helped frame what we know about the Chinese economy.

Submission Summary:

- The current debate over whether high-risk vendors should provide network technologies focuses on narrow technical issues revolving around forecasts of how new network technologies will develop. Unhelpfully, this often boils down to a discussion over 'core versus edge'.
- Lacking in this debate is empirical or observed evidence of high-risk vendors' behaviour. This may include, but is not limited to, monitoring or surveillance of foreign individuals or firms, the way high-risk vendors may work with the state or state-linked entities to leverage their position as network provider, and integrated data collection capabilities for state ends.
- High-risk vendors are often multilayered businesses. Many do not provide simply one product or service, but multiple channels that raise their overall risk profile. In the case of Huawei, they provide not only network gear, but also handsets and cloud services. This allows them broader and deeper penetration into information gathering efforts.
- High-risk vendors are important within Civilian Military Fusion of adversarial states. Such vendors work closely with authoritarian states to promote their specific vision of governance, surveillance, and cooperate with other state linked firms.
- In this submission of evidence, I submit cogent evidence that adversarial states are engaging in broad data collection and monitoring of Chinese and foreign individuals and firms aided by high-risk vendors like Huawei Technologies. This includes, but is not limited to, monitoring of foreign individuals and firms and near real time population counting camera with facial and gender recognition.
- The evidence presented here demonstrates that high-risk vendors within Civil Military Fusion authoritarian states engage in surveillance and monitoring activity of domestic and international individuals and institutions. This should raise significant concerns for open liberal democracies considering allowing high risk vendors to participate in their telecommunication network.

Introduction

The United Kingdom is studying the risks of allowing a high-risk security vendor, which is effectively owned by a political public organisation of an adversarial state, to provide critical national infrastructure. The current debate has focused primarily on the ability to mitigate the risk that the Chinese government or Chinese Communist Party, directly or indirectly, poses through high-risk vendors and their potential ability to access information or data.

The debate must account for the broader questions of how to place network gear within the broader context of their corporate and link to statist policies.

I will not focus on issues under technical dispute concerning 'core and edge' equipment, but rather provide evidence about Huawei and Chinese data collection and monitoring activities focusing on their work gathering information on Chinese and foreign individuals and firms.

1 Background Evidence:

Before focusing on the new evidence, it is important to take certain facts as given so that the new evidence can be understood within a common framework.

1.1 Ownership

Huawei is not a private enterprise but is, effectively, a state-owned company. In China, a state-owned enterprise is a specific corporate registration classification. Huawei is not registered as a state-owned enterprise according to official records and therefore is not a state-owned enterprise. Huawei Board of Directors Chief Secretary Jiang Xisheng in a conference call with global media in April 2019 acknowledged Huawei is not legally a private enterprise stating, "Huawei has chosen to use the Union as the registered shareholder of Huawei."[1] The Huawei Investment Holding Trade Union is the owner, not the employees.

The trade union committee, as is clearly specified under Chinese law, is what is known as "public" or "mass" organisation. Under Chinese law a trade union committee is recognised as a legal person, and thus the trade union committee has no shareholders. All trade unions in China are under the umbrella organisation of the All China Federation of Trade Unions (ACFTU).[2]

The ACFTU is a highly-political and state-managed institution that carries out a broad range of CCP and state-linked activities. Importantly, the Huawei trade union legal registration designation is the same corporate legal classification as other Party organisations such as the Communist Youth League. It is fundamentally false and misleading to claim that Huawei is a private enterprise.

In a conference call in 2019 with journalists, Huawei Board of Directors Chief Secretary Jiang Xisheng actually acknowledged employees do not actually own shares in the company stating, "shareholding employees are not registered as shareholders. They don't directly hold the shares of the company. That's

[1] "Transcript of Huawei Board of Directors Chief Secretary Jiang Xisheng's Interview with International Media" from April 25, 2019

[2] For a fuller exposition on the legal status of Huawei's ownership structure please see "Who Own's Huawei?" by Christopher Balding and Donald Clarke at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669

why we call the shares virtual shares."[3] It is at best misleading, if not outright deception, for Huawei to claim it is a private enterprise based upon their own admission and legal registration status.

1.2 Links to Intelligence Agencies

Based upon a database of employee resumes, it has been demonstrated that Huawei is actively engaged in a variety of intelligence, security, and intellectual property activities.[4] For instance, employees state that they act on behalf of the Ministry of State Security within Huawei. Other employees worked simultaneously for research units of the People's Liberation Army likely in units managing cyber warfare.[5]

This clearly implicates Huawei and their personnel in a range of behaviours that are publicly denied by the company but which are pertinent to the debate on high-risk vendors. From descriptions of information interception, technical activities and expertise that focus on offensive penetration, and intellectual property theft, Huawei and its personnel engage in a variety of worrisome behaviours. In one case, an individual was linked by time, activity, and geographic location to a known public case of unauthorised network access by Huawei.

2. The Broader Framework for Telecommunications in China:

Though the United Kingdom debate is taking place focused on 5G network gear, Huawei provides a broad range of goods and services within the telecommunication space. It would be a mistake to analyse potential risks of a high-risk vendor divorced from its other activities or role as a favoured firm of an adversarial state.

In its handset business, Huawei provides pre-loaded software from itself and third party service providers. However, this opens up United Kingdom consumers to additional threats. The End User License Agreement (EULA) between Huawei and United Kingdom handset consumer specifically lists the governing jurisdiction is the People's Republic of China with carve outs for any additional protection as provided consumers as afforded by local laws. The EULA specifically notes that:

> *Data collected from your device during use may be processed or transferred to Huawei and its affiliates/licensors in countries outside of the country you reside. This means the data may be transferred to or accessed from other jurisdictions which are outside of the country where you use Huawei's products or services. These jurisdictions may have different data protection laws or such laws may not even exist.*[6]

Due to the fact that Chinese national security law explicitly gives the state access to all data with firms required to assist, Huawei has explicitly told UK consumers it will make their data available to China.

Though Huawei has publicly said that they will not share consumer or client information with the Chinese state, their legal documentation says otherwise. It is worth noting that UK data privacy laws does not explicitly prohibit use of data in this manner as the consumer has a relationship with the handset provider.

---

[3] "Transcript of Huawei Board of Directors Chief Secretary Jiang Xisheng's Interview with International Media" from April 25, 2019

[4] Accessed at https://www.telegraph.co.uk/news/2019/07/05/huawei-staff-cvs-reveal-alleged-links-chinese-intelligence-agencies/ on April 2, 2020

[5] For a fuller exposition on Huawei links to Chinese security services please see "Huawei Technologies' Links to Chinese State Security Services" at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726

[6] Accessed at https://consumer.huawei.com/en/legal/eula/ on April 7, 2020

Finally, the Chinese government treats domestic companies as vectors of state control and the security apparatus. China has named this link between the state and non-state Military Civil Fusion. Chinese telecommunication and technology firms throughout the Chinese corporate world are deeply embedded within the Chinese state carrying out and actively assisting in security policies. Potential high-risk vendors other business activities as well as the national legal, regulatory, and policy environment cannot be divorced from our analysis of the risks they present within one specific domain.

3. Evidence of Chinese and High-Risk Vendor Activity:

After my work on Huawei resumes, I was provided data on Chinese surveillance and monitoring activity by other individuals. I worked to confirm, authenticate, and analyze the data provided to me. Since authenticating the data, I have provided the data to others for authentication and analysis. What I am presenting here is a portion of what we have analyzed and authenticated to date.

Based upon our analysis of the data we collected, five themes that stand out as pertinent to the debate around high-risk vendors and Chinese Military Civil Fusion.

- First, China uses domestic technology firms as a channel to build surveillance, monitoring, and security gathering capabilities. Data collected through electronic channels from handset to IP camera streams are stored in cloud storage repositories, many of which are managed by Huawei, and can be made available to Chinese public officials upon request.

- Second, China is building out surveillance and data gathering capabilities on foreign nationals and firms mirroring its domestic security capabilities. China technology firms are building databases monitoring foreign individuals and firms, including military and political personnel at all levels, as well as influential persons and institutions such as think tanks. According to our data, China keeps data on approximately 1% of the population in many countries such as the United Kingdom. The Chinese surveillance state is not limited to domestic individuals and firms but encompasses foreign actors.

- Third, China is using firms such as Huawei, which provide hardware and software to foreign individuals and firms, as an entry point to gain access to monitoring and surveillance data. We have found repeated instances of Chinese firms storing foreign customer data in China. Though Chinese firms like Huawei note in their EULA that the data contains no personally identifiable data, given the ability of technical personnel to match device identifiers to individuals it is entirely possible to personally identify someone from stored data if desired.

- Fourth, Huawei providing network, handset, wearables, and cloud services among others coupled with their documented links to the Chinese state security and intelligence institutions make them a central risk to any country concerned about data gathering by the Chinese state. Foreign ata device records from Chinese and foreign individuals and firms are stored in China. This data would allow any trained technician wide ability to track, surveil, monitor, and intercept information from foreign individuals and institutions.

- Fifth, the Chinese internet, servers, and devices are not secure typically lacking basic encryption. This matters because high risk vendors with poor security practices from their home market resell the same or similar products relying on poor security. The Huawei Cyber Security Evaluation Centre Oversight Board has long noted the low security standards of Huawei gear which Huawei promised to address but failed to correct. The low security standards of Chinese internet across all

facets, make it likely these practices will simply be transferred to the United Kingdom raising risks for consumers and business.

I will detail some of the specific data provided to me.

3.1 Dataset #1:

A Chinese dataset we are analysing provided directly by a person linked to the Chinese technology firm who compiles it, appears intended for information and influence monitoring of foreign individuals, firms, and institutions. This is a large dataset used by various agencies within the Chinese government, which we believe to include the Ministry of Foreign Affairs as well as security agencies, used to track and monitor foreign individuals and institutions. The dataset appears designed to monitor and track influential individuals around the world across nearly every profession from their social media footprint to work history and familial relationships.

The analysis appears to show that multiple branches of the Chinese government use the database. We cannot say exactly how much of the database they use or where the information is deployed for analysis, but we can say it appears to be used by multiple Chinese government agencies.

What is notable about the data is not its depth of information, but the easily accessible breadth of information about foreign individuals and institutions. Of the general population of most every country reviewed; this Chinese database maintains records of between 0.5-1.25% of the population of every country reviewed. In the United Kingdom alone, this database covers more than 1% of the population. Additionally, there is data on think tanks, political aides, family members of major politicians complete with links to and summary of work history, written works, social media profiles and history, and other key information.

We find it notable that other than think tanks that have produced a written work about China as all their work is catalogued, individuals and institutions that deal heavily with China in their work are largely absent from this database. In other words, the database does not appear to focus or target specific individuals, institutions, or information we suspect Beijing would prioritise. While these are generally influential people and institutions, most have little if anything to do with China. We have evidence that higher sensitivity data on targeted individuals and institutions is kept in a separate location.

Fourth, China is building an in-depth catalogue of social media activity. What is notable, however, is the depth of their activity in tying the picture together. The data shows millions of Tweets, but then catalogues trends in likes including people who liked, for instance, a politicians Tweet. This activity extends well beyond standard influencers, but covers a wide variety of individuals and institutions, including deployed military personnel around the world at all levels and individuals at all levels of society.

This data confirms some of the concerns about the presence of high-risk vendors from adversarial states building monitoring and surveillance capabilities on foreign individuals and firms. China is not limiting surveillance and monitoring capacity to Chinese citizens and firms, but is extending it to foreign individuals, family members, and institutions.

3.2 Database #2:

Here I present data provided to me of cameras distributed throughout China. These specific cameras are distributed throughout numerous provinces of China and regularly gather specific data. While China is the

most surveilled country in the world, of which we have additional data not presented here, this data was interesting for several reasons.

First, the cameras collect population data broken down by gender, age groups, and totals recorded on the last day of the month. It is not clear whether the data recorded is a snapshot or some type of average or sum of population or flows through the area within the past month. Given the data breakdown, it appears the camera is loaded with facial recognition capability that allows it to sort individuals into specific categories.

Second, these cameras appear to act almost as a real time population monitoring net with millions of cameras covering wide swathes not just of populated areas, but remote areas with no population. Geolocation and population totals indicate a majority of these cameras lie in rural and forested areas measuring population. Though we only have data for a handful of Chinese provinces, we have reason to believe this system extends to a significantly larger number, if not all provinces.

Third, given the existence of other camera systems we know exist that would allow the government to track an individual throughout a building or part of town, this camera system appears to focus on a specific task with greater allocation to less populated areas. One puzzle is why this camera system is gathering population data in less populated areas? Using geolocation data to find cameras on Google Earths places the majority of these cameras in unpopulated areas of China.

The Chinese government is building out its surveillance capability domestically. The threat of high-risk vendors via Huawei and camera firms used heavily in the United Kingdom like HIKVision, the possibility of surveillance is significant. We have additional evidence of Chinese domestic and foreign surveillance and data collection capabilities.

Conclusion:

The evidence of high-risk vendor involvement in state mandated activities including security, monitoring, and intelligence on domestic and foreign individuals and institutions is clear.

I have presented evidence of wide scale data collection facilitated by Huawei and linked high risk technology firms from China engaged in data collection in the United Kingdom and China. High risk Chinese vendors, including but not limited to Huawei, are involved in many layers of the Chinese security state and the implications this may have for the United Kingdom. Huawei network gear and the recognised security weaknesses are only a portion of their risk profile, but also data collected from UK consumers through handsets stored in China on cloud services.

Due to space, source, method, and privacy constraints, I have only presented a small fraction of the data given to me on Chinese activities. The data covers a variety of other functional and topical areas that may be of interest to the United Kingdom defence and security services for what they reveal about Chinese activities in monitoring their own citizens and firms, as well as foreign individuals and firms.

Most importantly, I have provided evidence of monitoring and surveillance activity that raises concerns about allowing high risk vendors into critical telecommunications infrastructure. This monitoring and information gathering takes place using high risk vendor hardware and services as well as those of other state linked technology firms.

17 April 2020