Huawei Technologies' Links to Chinese State Security Services

By: Christopher Balding

Associate Professor

Fulbright University Vietnam

Abstract

Using a unique dataset of CVs, this paper analyzes the relationship between key Huawei personnel and the Chinese state security services. Based upon an analysis of this dataset, I find there is strong evidence that Huawei personnel act at the direction of Chinese state intelligence, and that there exists a deep and lasting relationship between Huawei, its employees, and the Chinese state. This should raise questions within Western governments worried about Chinese access to domestic information.

Acknowledgements

The author would like to thank Samuel Armstrong, Dr John Hemmings, and Dr Andrew Foxall at the Henry Jackson Society, for their support of this research from fact checking, digging deeper, verifying translations, asking tough questions, and helping to publicize the research among other things. Additionally, there are many people that have played a crucial role in bringing this research to publication stage. Given the nature of the research, they will be thanked anonymously, but whether large or small, I want to publicly thank them for their help. Their help and support in a variety of ways was truly invaluable.

Disclaimer

This research and all errors are the sole and absolute responsibility of the author. The conclusions and opinions are the authors alone and do not necessarily represent Fulbright University Vietnam, the Henry Jackson Society, or any others. Nor should anything contained in this report be considered to represent the opinion or beliefs of any affiliated or mentioned person or organization. All errors or omissions are the sole responsibility of the author.

Introduction

There are long standing questions about the links between Huawei Technologies Co., Ltd. (hereafter referred to simply as "Huawei") and the Chinese state. One specific question centers on the relationship between Huawei and the Chinese state security services. A major reason for this is that Huawei's co-founder Ren Zhengfei held a senior position within the People's Liberation Army (PLA) before starting the company.

This specific question has taken on added importance as Huawei has become more important to telecommunications networks globally, with concern in the West that Chinese state security services may potentially be able to access everything from personally embarrassing information (which could be used as *kompromat*) to national security secrets. Such is the gravity of the latter concern that the Trump administration has threatened to end intelligence cooperation with the United Kingdom if London allows Huawei into its 5G network.[1] This places a heightened level of importance on understanding what is the relationship between Huawei and the Chinese state military, intelligence, and security establishment.

Using a unique dataset of CVs that leaked from unsecure Chinese recruitment databases and websites and emerged online in 2018, I analyze the relationship between Huawei and the Chinese state security services. In the first of what will be a series of papers, I find that key mid-level technical personnel employed by Huawei have strong backgrounds in work closely associated with intelligence gathering and military activities. Nor is the relationship purely titular. Huawei personnel outline and discuss technical work, such as information interception, on their CVs. In some cases, Huawei personnel can be linked at a metadata level to specific instances of hacking or industrial espionage conducted against Western firms.

As it proceeds, this paper is divided into four sections. The next section provides a series of notes about the data used in the paper. The following section describes data collection and methodological approach. The third section presents three CVs. The final section outlines conclusions. Taken together, this paper is based on a unique dataset that provides the most

[1] Please see https://www.reuters.com/article/us-britain-huawei-ncsc/uk-cyber-boss-downplays-threat-of-five-eyes-security-rift-over-huawei-idUSKCN1S00SB

convincing, publicly-available evidence on Huawei's relationship to the Chinese state security services.

Data and Methods Note

The research presented in this paper is highly sensitive. As such, a number of points need to be made in advance about the data the paper uses, the methods the paper employs, and the conclusions the paper draws.

1. The research presented below takes the form of three profiles based on three "CVs" taken from a database of CVs that leaked online in 2018 from unsecure Chinese recruitment databases and websites. While these three "CVs" are portrayed faithfully in the profiles below, they are presented in such a way as to prevent anyone from replicating the research I have undertaken. I have done this to protect people and firms that may have intentionally or unintentionally assisted in the research for this paper at various stages.
2. Multiple people have independently reviewed the three profiles presented in this paper. In doing so, I provided them with the raw information contained within the database of CVs and asked them to compare this to the three profiles I created. In each case, these reviews led me to edit the profiles in order to further obscure the three individuals' identities; nevertheless, in doing so I was able to remain faithful to the information stated on their CVs. I do not reveal in this paper what edits I made, but I should be willing to do so with trusted parties.

To protect the safety of persons or organizations involved or targeted, intentionally or unintentionally, in the production of this research I have taken steps to prevent the replication of this research. This includes, but is not limited to, using fictitious names or omitting key information. This is a commonly accepted technique in research where uniquely identifiable information may put individuals or organizations at risk. Where I have changed descriptions of individuals' experiences, I have done so as little as possible while still being able to hide identities.

Data Collection Background and Methods

In 2018, information began to emerge that large numbers of Chinese *curriculum vitae* (CVs) were leaking from unsecured databases or websites run by recruitment platforms. According to one recent news article, researchers identified nearly 600 million CV's in various data leaks.[2] Based upon unpublished information, it is quite possible that this number is even higher. Given the data and information challenges present in China, this data source had the potential to provide significant and detailed granularity about a variety of questions, not only those about Huawei. This paper provides an initial review of whether and to what degree Huawei is connected to Chinese military and security institutions or personnel, and whether there is evidence of behavior by Huawei that would fall outside the realm of traditional telecommunications networking manufacturer.

Data from CV leaks was obtained, secured, and distributed in multiple on- and off-line environments to guarantee future accessibility. It is important to note that while this is likely illegal in China given the broadness and malleability of Chinese national security law that requires companies and individuals to cooperate with intelligence officials when requested and can make all information national security data a state secret retroactively.[3]. CV databases were not password protected and required only minimally more technical competence than entering a website address into standard internet browser. This is noted to emphasize that while there may be understandable questions about how the data was procured, it involved no activity that might be considered as 'hacking', such as network penetration, phishing, or stealing passwords. The data was entirely and fully available to the public and was not password protected.

After securing the data, I requested technical assistance to "clean" the data to prepare it for more standard formatting and improved searching capability. It is important to note what is meant by "cleaning" the data. CV datasets came from two primary sources. First, data that is captured when a job seeker uploads their CV to a website or enters data manually. Second, when a crawler finds a CV on a job site and automatically sends back data to a database. In the database, due to a variety of issues, it is not uncommon to have data out of place for a job seeker. To take a simple example, the database field or variable name for the job seeker's "city" might be blank but the

[2] Please see "Chinese companies have leaked over 590 million resumes via open databases" at https://www.zdnet.com/article/chinese-companies-have-leaked-over-590-million-resumes-via-open-databases/ as a good recent summary of the issue

[3] Please see https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

field or variable name for the "province" will contain the city name. There are many different error possibilities given that so much of the data is compiled automatically, the data frequently needs additional work to make it readily usable. Given the size and variation of the data, standard commands were used to clean up the data. In a small number of cases, where large amounts of an entire record is contained in one field, additional cleaning (undertaken manually) was required. This "cleaning" did not involve editing, deleting, or adding to the data in any way. Cleaning the data only involves making it more standard and readable.

At this stage of the research, I conducted narrow targeted searches rather than explore the full range of records available. To that end, I extracted records that contained variations of the word "Huawei". For instance, searches for the shortened simplified Chinese characters "华为" and the roman lettering "Huawei" provided a subsample of CVs that were tied, at least superficially, to Huawei. After extracting these records from the complete dataset, additional searches were then conducted using specific search terms containing both institutional terms, such as the "People's Liberation Army", and variants, such as "PLA". The subsequent research focused on a subset of CVs that were connected to Huawei and contained key search terms or other institutional links of interest.

There are four final points about the data and sampling. First, at this stage it is difficult to know how representative a sample the CV data are relative to Huawei. Consequently, while it is possible to make claims about specific activities or links that involve Huawei, I am reluctant to go beyond what can be demonstrated with the data in hand and how that might apply to other parts of the company or their activities, without clear evidence. Second, the CVs are a valid source of information about Huawei and its activities, but they also contain clear limitations. As in any country, they typically only contain general descriptions of work, skills, projects, and or clients. Third, the research presented here provides detailed analysis of three CVs but does not provide broad descriptive statistics or other analytics. Given the data, at this stage I felt it more important to do a 'deep dive' into a small number of subjects rather than provide broad descriptive statistics which may not provide as much information. Fourth, the three cases I present are only a small sample of what has been found. There are significant numbers of additional job candidates I am holding back even within the limited search parameters identified.

Profiles

CV #1-Working for the PLA Strategic Support Force and Huawei

Yang Guozhi works for Huawei Technologies Co., Ltd. (hereafter “Huawei”) in Shenzhen as a software engineer in the Quality Management Testing department. His work for Huawei primarily focuses on software testing of mobile base stations across legacy and emergent standards from LTE to 5G. This includes manual and automatic as well as local and remote testing of base station operations. The controller platform for base station allows control over a variety of aspects including software upgrades, the device, logs, alarm, and frequency within the platform developed by Huawei. This work includes remote testing and control of the test process comparing it to platform test results available to the user.

While the work for Huawei in Shenzhen appears to give Guozhi and Huawei enormous control over access to user and provider data, something which is implied but not stated explicitly in the CV is the simultaneous position Guozhi holds. According to the CV, Guozhi also holds a teaching and research position at the National University of Defense and Technology (NUDT) in Changsha through which he is officially employed by the People’s Liberation Army (PLA). Guozhi’s research work for the NUDT focuses on signals, remote management, and scripting, and which matches relatively closely his work for Huawei.

There are a few specific points about the positions as a Huawei software engineer and a teacher at a key PLA university that need emphasizing. First, the CV data list the start date at Huawei in 2011 and the NUDT as 2012 with Guozhi still present and active and present in both positions. There is no reason to discard this seeming overlap. This is not a situation that we have encountered in other CVs, meaning that if it were a data error from the crawling script we would have expected to see it more often. Furthermore, for key people in China, holding multiple positions is not an uncommon arrangement. We believe the data to be accurate but cannot rule out there is a mistake in the data we have.

Second, the specific position functionality within PLA research and their unit places them within a branch under something currently called the Strategic Support Force (SSF) which was merged from previous organizations. Their CV does not specifically say they work under the SSF, however, given the functional work and the related PLA unit listed on their CV, I believe their work is clearly under the SSF umbrella. A Rand report notes “the SSF is charged with overseeing Chinese military space, cyber, and electronic warfare capabilities, and its development will have important implications for China's emerging aerospace expeditionary and power projection capabilities."[4] Underneath the umbrella is a division focused on "cyber warfare, electronic warfare, psychological warfare, and technical reconnaissance."[5] The SSF electronic warfare division and its predecessors have been linked to various incidents, such as the notorious 61398 unit based in Shanghai which has been charged in multiple hacking cases against American companies.[6] It raises extremely troubling questions about why a Huawei software engineer managing base station control, holds a dual position in the PLA in a division focused on cyber warfare.

We cannot say categorically what Yang Guozhi has done, for example whether he has injected code that would allow the PLA SSF or related entities to monitor data traffic of individual users or all base stations. The CV does not say that. We can say, however, that based upon information contained in the CV that Guozhi worked on this hardware, conducting software and code creation, testing, developing functionalities that would allow those actions, while holding a joint position within a branch of the PLA known to conduct those types of operations. The circumstantial evidence appears quite strong to support valid concerns about the relationship between Huawei, the PLA, and concerns about intelligence gathering.

CV #2-Helping the Ministry of State Security Capture Network Flows of Information

Li Jingguo studied computer science and engineering at Xi'an Jiaotong University before moving to Shenzhen and working for a small subsidiary of a state-owned enterprise (SoE). During his three years at the enterprise, he worked on neighborhood development connectivity network projects around numerous cities in China. Involved in many aspects of small-scale network roll out and planning, he was able to leverage this into a role at Huawei Technologies Co., Ltd. (hereafter "Huawei") as an R&D (Research and Development) Engineer in the software development and systems integration unit.

[4] Please see *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations* at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2058/RAND_RR2058.pdf
[5] Please see *China's Strategic Support Force: A Force for a New Era* at https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf
[6] Please see https://www.reuters.com/article/us-cybercrime-usa-china-idUSKCN0J42M520141120

Moving to Huawei gave Jingguo access to larger projects and more responsibility. During the next few years he worked on larger network role out, covering countries throughout south east Asia, and was central to the development of Huawei's market expansion plans in the United Kingdom. His increased responsibility and project size gave him experience in a wide range of work, from software development and integration with hardware to network planning and internet protocols across emerging Asia and a key European market as well as Chinese network build out. He was involved in most aspects of large-scale internet network roll outs.

There a number of specific experiences cited by Jingguo that raise concern about his activities. First, he served as a Ministry of State Security (MSS) representative working for Huawei. It appears from a close reading of his CV that he served as an MSS representative on a specific project or product development. It does not appear that he was an actual MSS employee but rather served as the MSS representative within a specific business unit likely guaranteeing project specifications. Given that he openly references this position in a CV, I infer that: this was publicly known within the industry or company; represents a systematized relationship between Huawei and MSS; and, is a position of increased responsibility or authority. It is important to note that in the Chinese Ministry of State Security is the primary entity responsible for espionage and counter intelligence. MSS has been implicated in a variety of activities, from human intelligence asset recruitment and information gathering to cyber warfare activities in network penetration. It should raise immediate concern that MSS assets are working on networking equipment as representative agents for Huawei.

Second, beyond specific titular responsibility, he engaged in behavior that describes planting information capture technology or software on Huawei products. On multiple projects covering both domestic and international in scope, he lists his responsibilities has building lawful interception capability into Huawei equipment. Additionally, technical work described on the CV matches the type of technical requirements needed to engage in interception of transiting information even with various safeguards, such as virtual private networks (VPN). In describing his work building information capture capability, he uses the same terminology whether it is for domestic or international networks and appears to refer to the same higher authority as the primary user of this information although it is not entirely clear. Given his relationship with MSS, it is reasonable to believe this capability is being provided to or directed by MSS. We do not have the requisite information to say whether Huawei is being directed or whether they are providing this access to MSS out of an abundance of caution, but the relationship clearly exists at an institutional level and has been systematized within Huawei.

Third, in addition to titular and experiential activity that ties Jingguo to state security activities, it is possible to tie work from his CV to reported cases of Huawei information gathering. It is not possible to directly tie his routers or his code to the specific products in question, but based upon the timeline, work described, and geographic responsibility, there is a clear match with work described on Huawei activity in Italy and network security with code being injected that would allow Huawei to access the network and traffic.[7] It is important to repeat that I cannot tie specific routers or code he developed to the described activity because the granular information that would be needed is not available. Based however on the timelines described in the Bloomberg news report (see Footnote 7), his CV, self-declared activity (such as technical work and geographic responsibility), and work matches the work described in news reports for Huawei Italy.

Jingguo appears to be involved in the exact type of work with links to Chinese state security that concerns governments. From the MSS to information capture and linking to specific cases where Huawei engaged in covert information gathering, this should be a major concern to Huawei network information clients.

CV #3-From Military Industrial Complex SOE to Huawei Network Manager

Wang Qiang studied network engineering at Zhejiang University of Science and Technology (ZUST) in the eastern Chinese city of Hangzhou. After graduating from ZUST, Qiang accepted a position at the China Aerospace Science and Technology Corporation (CASTC) in Beijing. A major state-owned enterprise that operates across a wide variety of sectors, CASTC and its subsidiaries and cross holdings have been involved in a variety of activities that have caught the attention of authorities worldwide from being placed on the US entity list to selling high and traditional weaponry to everyone from North Korea to Syria. A major supplier to the People's

[7] Please see https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment

Liberation Army and more recently the Strategic Support Force division handling advanced warfare capabilities, CASTC is a major concern involving state security and Chinese military projection globally. A primary focus is missile and space technology.

During his many years working for CASTC, Qiang worked on variety of civilian and military communication systems development. Work on military applications covered numerous communication methods between military installations and between command centers and naval or air force assets. This included key PLA units with major control of traditional and advanced warfare assets. His work on networks and communication systems covered highly secure networks and communication systems, fully private networks, and working with a wide variety of communication protocols. In civilian work, he designed and built communication and internet works in key Chinese client states with large investment and assistance programs.

Qiang left CASTC and went to China Unicom, where he worked on high security clients continuing his work on network design and protocols. We have relatively little information about his activities at Unicom, but he was employed there for just over a year.

Upon joining Huawei Technologies Co., Ltd. (hereafter “Huawei”), he took charge of major new projects to increase network capacity and big data projects. This included network expansion projects for China Telecom and a major data center completion for China Mobile. This was followed by an HDTV network project via fiber in Fujian. The work covered all aspects of networking for major clients using the Huawei router products and long distance transmission lines.

There are a number of notable aspects to Qiang’s specific work. While this CV is rich in project and client-type description, it contains less description about his skills and the technical work he undertook. Nevertheless, it is still possible to infer from what information is included. First, Qiang’s work for CASTC placed him in contact with some of the most sensitive aspects of all PLA operations and technologies. He would have intimate knowledge of not just of PLA asset deployment but communication systems and monitoring. This includes security, penetration, and monitoring. Prior to the recent evolution of internet monitoring in China into a more cohesive and defined structure, many companies or governmental units engaged in cyber activities. This work designates him not as a normal coder or network engineer but as state security asset trusted with intimate knowledge of PLA assets and all communication systems.

Second, Qiang's work for the PLA made him a logical choice to move into an SOE and, subsequently, Huawei in order to handle major network expansion and monitoring. Though focused more on network hardware, routers, and transmission, Qiang (given his background both technically and his company) would have intimate knowledge of what was expected from China on network monitoring. Though there is no description of his work focusing on international clients, what is notable is the strong link between key PLA or national security personnel Huawei personnel in key positions such as network design and router manufacturing.

Third, there is also some evidence Qiang was involved in replication or hacking of foreign hardware. During his time at the CASTC, Qiang specifically noted his expertise in Cisco and Nortel switches and the use of such switches for various networking projects he worked on. What makes this notable and suspicious is that during his time working for CASTC (a major Chinese military SOE with contracts for the PLA) there were large scale hacking or pirating of both Cisco and Nortel by Chinese state actors and or state-linked actors. In one case, fake Cisco routers with Chinese chips began appearing in US military hardware.[8] This roughly coincides with Qiang's time working with this networking gear, though it is not possible to tie him directly to this incident. It is notable however the overlap and subsequent work.

The career path of Wang Qiang tracks a very similar path of military-industrial complex, network monitoring and management, with a move into Huawei. Like with other CVs covered here, we cannot conclusively say what code was input into networks, hardware, or routers managed by Qiang. However, we can conclusively say that key Huawei personnel have close relationships with Chinese military and cyber activity entities and whose activities match key elements of what is publicly known about technology incidents of pirating or hacking. There are clear and serious questions raised about Huawei activity.

Conclusion

The exact relationship between Huawei and the Chinese state, military, and intelligence services has long been rumored to exist but with only minimal public evidence of such a relationship. The data uncovered provides direct, first person account of Huawei personnel activity,

[8] Please see https://www.theguardian.com/technology/blog/2008/oct/06/security.china

relationship to Chinese military and intelligence agencies, and evidence of worrying behavior. The analysis adhered closely to what could be documented or matched again known records. If we took a more expansive view of what we believe could be reasonably inferred from key words and associations, it would be possible to arrive at an even more worrying view.

There are four points about this data and analysis that are important. First, the data provided is direct, first-hand testimony about Huawei activities, the behavior of its personnel, and its relationships with other Chinese organizations. The data provided comes directly from Huawei employees testifying to their work and activities. Second, Huawei employees effectively confirm the rumored relationship between the Chinese state, military, and intelligence gathering services. Huawei employees confirm the fears of links and acting in concert with the Chinese state. Third, the relationship is clearly systematized given the public references to MSS unit representatives. In other words, this is not simply due to Huawei recruiting employees that used to work in the military by normal chance. Rather, there is a clear institutionalization where the Chinese state and intelligence gathering assets are placed in Huawei within a systemic organization designed to facilitate information flows. Fourth, the institutional relationship between Huawei and Chinese state security services directly contradicts Huawei claims that they have no relationship with these services. It should cause significant concern that Huawei employees provide evidence that directly contradicts public relations statements and claims.

It is important to note that the three profiles presented in this paper are meant to be unreplicable composites of real people. Information has been overlaid in an attempt to be as factually accurate for what could be a real person and to not embellish the factual information of the real people analyzed. If inconsistencies are discovered in the details provided, this is likely due to author mistakes in using a name that may not as perfectly matched an experience as expected. While great care has been taken to avoid any such errors, they are accidental and not intended to embellish or paint inaccurate personnel picture from the underlying data.

This paper has sought to answer whether there is evidence of Huawei acting in concert with the Chinese state, military, and or intelligence gathering services. After examining a unique dataset of employee provided work activity at Huawei, it is clear that there is an undeniable relationship between Huawei and the Chinese state, military, and intelligence gathering services. While data limitations prevent us from saying whether Huawei follows official commands, acts in concert with the state, or seeks to preempt greater control by acting in advance, there is significant direct evidence of Huawei personnel acting at the direction of Chinese state intelligence with multiple overlapping relationship links through the Chinese state. This should concern governments worried about Chinese intelligence gathering.