FEATURE

# Huawei "back doors"?

## Beijing may not need Huawei 'back doors'

Expert says National Security Agency never found Huawei back doors created for Chinese intelligence

By Frank Chen

Excerpted from https://www.asiatimes.com/2019/03/article/beijing-may-not-need-huawei-back-doors/
March 5, 2019


*A man walks past a Huawei store in Beijing. Huawei is being accused by the US of violating its sanction laws and implanting backdoor access to its gear sold overseas. Photo: AFP/Getty Images*

As the US and some of its allies get together to lock Huawei out of their telecommunications infrastructures, some cybersecurity experts in the West now openly question the rationale of singling out and penalizing the Chinese tech firm.

They say Huawei is "unlikely" to build so-called "back doors" into systems for fear of being exposed, especially considering that Beijing can already hack into foreign systems without any such help.

Washington is adamant that any nation deploying Huawei's gear in its next-generation wireless networks is giving Beijing a ready-made conduit for espionage. Americans say the Shenzhen-based tech behemoth's global stranglehold on 5G gear puts it at Beijing's beck and call, and that the firm acts as Beijing's surrogate.

US officials also cite a Chinese intelligence law which "compels their citizens

*Huawei's Chief Financial Officer Meng Wanzhou is now on bail in Vancouver after she was detained during a transit stop at the city's airport in December. Canada may extradite her to the US at the latter's request, for allegedly breaching US sanctions against Iran. Photo: Reuters*

and their companies to participate in intelligence activities".

But security experts told the Associated Press that the US government was probably exaggerating that risk. The reality is that Beijing does not need malware implanted in or clandestine access to Huawei routers, switchboards or wireless base stations to infiltrate overseas networks which already have "notoriously poor security", making them easily exploited.

Jan-Peter Kleinhans, a researcher at the Berlin-based think tank Neue Verantwortung Stiftung specialized in IT security and state surveillance, said that if the Chinese wanted to tap or eavesdrop global networks, "they will do so regardless of the type of equipment you are using" and that Beijing's army of state-sponsored, highly-accomplished hackers had shown no preference for one manufacturer's technology over another's.

Moreover, Huawei would already have been caught and banished years ago, had any such back doors installed on behalf of Chinese intelligence been discovered by overseas clients or government watchdogs.

Huawei has already moved to counter sue the US government for trumping up accusations without any proof of its alleged complicity.

European allies have been reluctant to embrace a blanket ban on Huawei equipment. For instance, Germany has signaled no intention to cut off Huawei's business there in toto, with a reported prerequisite of a mutual no-spying deal


*Huawei is being accused by the US of acting as Beijing's surrogate by allowing the latter backdoor access to its gear sold overseas. Photo: Weibo*

with China. Poland and the Czech Republic, both NATO members, have also allowed Huawei to make inroads into their respective telecoms and end user markets.

AP also quoted Priscilla Moriuchi, the US National Security Agency's former head of Far East operations, as saying that she was not aware of the NSA ever finding Huawei back doors created for Chinese intelligence.

One irony is that the US has knowingly committed what it now accuses Huawei of doing.

According to classified documents laid bare in 2013 by defected NSA contractor Edward Snowden, who fled to Hong Kong and was later granted asylum by Moscow, the US "planted surveillance beacons in network devices from companies like Cisco Systems and shipped them around the world".

The shocking revelations by the whistle-blower led to a ban by Beijing on Cisco products.

Despite the US' coordinated blockade, Huawei said it had entered into contracts with 30 carriers worldwide to test and trial 5G networks and wireless technologies.