Experts: US anti-Huawei campaign likely exaggerated

28 February 2019, by Frank Bajak

In this Jan. 24, 2019, file photo Richard Yu, CEO of Huawei Consumer Business Group, unveils the 5G modem Balong 5000 chipset in Beijing. Security experts say the U.S. government is likely exaggerating the threat it says the Chinese telecommunications giant Huawei poses to the world's next-generation wireless networks. Critics say the U.S. case is short on specifics and glosses over the fact that China doesn't need secret access to Huawei routers to infiltrate global networks. (AP Photo/Andy Wong, File)

Since last year, the U.S. has waged a vigorous diplomatic offensive against the Chinese telecommunications giant Huawei, claiming that any nation deploying its gear in next-generation wireless networks is giving Beijing a conduit for espionage or worse.

But security experts say the U.S. government is likely exaggerating that threat. Not only is the U.S. case short on specifics, they say, it glosses over the fact that the Chinese don't need secret access to Huawei routers to infiltrate global networks that already have notoriously poor security.

State-sponsored hackers have shown no preference for one manufacturer's technology over another, these experts say. Kremlin-backed hackers, for instance, adroitly exploit internet routers and other networking equipment made by companies that are not Russian.

If the Chinese want to disrupt global networks, "they will do so regardless of the type of equipment you are using," said Jan-Peter Kleinhans, a researcher at the Berlin think tank Neue Verantwortung Stiftung.

One of the most common U.S. fears—that Huawei might install software "backdoors" in its equipment that Chinese intelligence could use to tap into, eavesdrop on or interrupt data transmissions—strikes some experts as highly unlikely.

Priscilla Moriuchi, who retired from the National Security Agency in 2017 after running its Far East operations, does not believe the Huawei threat is overblown. But she called the odds of the company installing backdoors on behalf of Chinese intelligence "almost zero because of the chance that it would be discovered," thus exposing Huawei's complicity.

Moriuchi, now an analyst at the U.S. cybersecurity firm Recorded Future, said she was not aware of the NSA ever finding Huawei backdoors created for Chinese intelligence but also cautioned that it can be extraordinarily difficult, when backdoors are found, to determine who is behind them.

European allies have been reluctant to embrace a blanket anti-Huawei ban even as U.S. officials continue to cast the world's No. 1 telecom-equipment maker as little more than an untrustworthy surrogate for Beijing's intelligence services.

The top U.S. diplomat for cybersecurity policy, Robert Strayer, says Huawei is obliged to heed Chinese Communist Party orders by a 2017

intelligence law that "compels their citizens and their companies to participate in intelligence activities."

In this Jan. 24, 2019, file photo Richard Yu, CEO of the Huawei consumer business group speaks as he unveils the wireless router running with 5G modem Balong 5000 chipset in Beijing. Security experts say the U.S. government is likely exaggerating the threat it says the Chinese telecommunications giant Huawei poses to the world's next-generation wireless networks. Critics say the U.S. case is short on specifics and glosses over the fact that China doesn't need secret access to Huawei routers to infiltrate global networks. (AP Photo/Andy Wong, File)

Strayer provided no specifics when pressed by reporters Tuesday as to how Huawei gear might pose more of a security threat than other manufacturers' switches, routers and wireless base stations. The diplomat spoke at Mobile World Congress, the world's largest wireless trade show, in Barcelona, Spain.

The American rhetoric has included threats.

U.S. Secretary of State Mike Pompeo suggested in a TV interview last week any use of Huawei equipment could jeopardize U.S. intelligence sharing and might even be a reason to locate military bases elsewhere. The remarks may have been targeted at NATO allies including Poland and the Czech Republic where Huawei has made significant inroads.

A spokeswoman for the U.S. National Security Council declined to comment or to provide any officials to address specifics. A State Department spokesman referred The Associated Press to a press statement on Strayer's remarks in Barcelona.

Huawei, founded in 1987 by a former military engineer, overtook Sweden's LM Ericsson in 2017 as the lead company in the market for wireless and internet switching gear. It says it supplies 45 of the world's top 50 phone companies and has contracts with 30 carriers to test so-called fifth-generation, or 5G, wireless technology.

U.S. companies are not serious competitors in this market, having pulled back over the years. Huawei's major rivals are European—Ericsson and Finland's Nokia.

The U.S. has provided no evidence of China planting espionage backdoors in Huawei equipment despite as 2012 congressional report that led the U.S. government and top domestic wireless carriers to ban it and other Chinese manufacturers from their networks.

"The backdrop for this is essentially the rise of China as a tech power in a variety of domains" said Paul Triolo, tech lead at the Eurasia Group risk analysis consultancy. Now, he said, "there is a big campaign to paint Huawei as an irresponsible actor."

In January, U.S. prosecutors filed criminal charges against Huawei and one of its top executives, alleging the company stole trade secrets and lied to banks about embargo-busting company dealings with Iran. Canada earlier arrested that Huawei executive—who is also the daughter of the company's founder—at U.S. behest; she is currently awaiting extradition to the U.S. Huawei has denied wrongdoing.

In this Jan. 29, 2019, file photo, the logos of Huawei are displayed at its retail shop window reflecting the Ministry of Foreign Affairs office in Beijing. Security experts say the U.S. government is likely exaggerating the threat it says the Chinese telecommunications giant Huawei poses to the world's next-generation wireless networks. Critics say the U.S. case is short on specifics and glosses over the fact that China doesn't need secret access to Huawei routers to infiltrate global networks. (AP Photo/Andy Wong, File)

One irony of the situation is that the U.S. has actually done what it accuses Huawei of doing. According to top-secret documents released in 2013 by former NSA contractor Edward Snowden, the U.S. planted surveillance beacons in network devices and shipped them around the world.

The affected equipment included devices from Cisco Systems, a Silicon Valley company whose routers were blacklisted by Chinese authorities after the Snowden revelations.

Washington's closest ally has taken a different approach to any potential threats from Huawei. Britain's National Cyber Security Center (NCSC) long ago placed multiple restrictions on Huawei equipment, including disallowing it in any sensitive networks, agency director Ciaran Martin noted in a speech last week.

According to Kleinhans, who has studied the agency's practices, Huawei can't conduct any direct maintenance on mobile base stations in the U.K., and instead must allow local wireless carriers to handle the work. Those carriers can't use Chinese equipment to conduct any law enforcement wiretapping. The British agency also requires redundancy in critical networks and a variety of equipment suppliers to prevent overreliance on any single manufacturer.

In its annual review of Huawei's engineering practices published in July, the NCSC found "shortcomings" that "exposed new risks in the U.K. telecommunication networks." But none were deemed of medium or high priority.

Martin called the problems manageable and not reflective of Chinese hostility—though experts say it's often difficult to tell if vulnerabilities are simply coding defects or intentional.

"With 5G, some equipment needs to be more trustworthy than ever. But probably not all," NCSC technical director Ian Levy wrote in a blog.

Like the British, German officials have indicated they'll reject a blanket Huawei 5G ban.

In December, the head of Germany's cyber-risk agency, Arne Schoenbohm, said "for such serious decisions as a ban, you need evidence."

Last week, the nation's Interior Ministry told The Associated Press "the direct exclusion of a particular manufacturer from the 5G expansion is at the time not legally possible."