# Why the war on Huawei?

*By Elisa Barwick*

The Five Eyes intelligence sharing network's push for a global espionage apparatus is threatened by the growing domination of tech markets by Chinese company Huawei, and the spooks club will do anything to stop it: claim Huawei's hardware is rigged for spying; blame it for hacks which threaten national security; insist it is working for the Communist state; and try to ban the technology in as many nations as possible.

But who is the real threat? It is the Five Eyes spy alliance—the signals intelligence agencies of the USA, UK, Australia, Canada and New Zealand—not China, which is mobilising all possible allies and assets to establish unprecedented global police-state control, including an unrivalled spying capability. In the words of Australia's Home Affairs Secretary Michael Pezzullo, it is determined to create a "transnational model of security" to match a globalised world, redefining the state itself in order to provide a "unity of command, clarity of authority, and singularity of purpose" for our security architecture. ("Five Eyes plan global police state", *AAS,* 22 Aug. 2018.)

Any expansion of outside technology into US, European and other markets is a threat to this plan, as it will interrupt the US National Security Agency (NSA)-UK Government Communications Headquarters (GCHQ) monopoly over the digital technology used for spying—especially as 5G technology, which China dominates, becomes prevalent.

Veteran Brazilian journalist and correspondent for the *Asia Times*, Pepe Escobar, wrote in Consortium News on 4 February: "Huawei's sophisticated encryption system in telecom equipment prevents interception by the NSA. That helps account for its extreme popularity all across the Global South, in contrast to the Five Eyes … electronic espionage network."

Other sources report that Huawei protects user communications more tightly than other telcos, preventing them from getting into the hands of third parties. By contrast, in a letter to Google written in July 2018 the US Energy and Commerce Committee stated: "In June 2017, Google announced changes to Gmail that would halt scanning the contents of a user's email to personalise advertisements to 'keep privacy and security paramount'. Last week, reports surfaced that in spite of this policy change, Google still permitted third parties to access the contents of users' emails, including message text, email signatures, and receipt data, to personalise content."

In 2011 WikiLeaks began releasing its "Spy Files", exposing the global mass surveillance industry—from spyware delivered to your phone via updates, to unregulated international surveillance companies selling powerful data-analysing software to governments, to monitor people of interest or to match phone signals with voice prints for drone targeting. "Intelligence agencies, military forces and police authorities are able to silently, and *en masse*, and secretly intercept calls and take over computers without the help or knowledge of the telecommunication providers", WikiLeaks revealed.

US programs to "stop terrorism" are designed to scoop up and screen all possible data, despite experts like former NSA technical director William Binney advising that this would hamper efforts to prevent terrorist attacks, proposing instead a program which analyses patterns in metadata while protecting individual privacy.

### Evidence?

While NSA whistleblower Edward Snowden presented documents confirming the agency had breached Huawei's corporate servers in 2010 and had "so much data that we don't know what to do with it", the evidence of spying by Huawei is sketchy. ("Australia ups ante on Five Eyes campaign vs. China", *AAS,* 23 Jan. 2019.)

In an article for the *Financial Times* on 12 February, Robert Hannigan, director of GCHQ in 2014-17 reported on the UK's years-long evaluation of Huawei by its National Cyber Security Centre (NCSC). While the centre did not dismiss the existence of Chinese state-linked cyber espionage, Hannigan stated that "The key point here, obscured by the growing hysteria over Chinese tech, is that the NCSC has never found evidence of malicious Chinese state cyber activity through Huawei."

He explained that the UK does not allow Huawei access to the "core" of its networks, but "assertions that any Chinese technology in any part of a 5G network represents an unacceptable risk are nonsense". On 15 February MI6 head Alex Younger suggested the UK would take a softer line on the matter than the USA, where Trump is considering an executive order to bar US companies from using Huawei products.

Germany's IT watchdog, the Federal Office for Information Security, has criticised the lack of proof behind US demands for a ban on Huawei equipment, saying its experts had examined the company's products and components and found nothing. According to news reports, a major Italian telecom company asked by the US Embassy to stop using Huawei gear was not provided with any evidence, only allegations. Outside of sanctions breaches and related "conspiracies", the recent US criminal indictments of Huawei refer only to an incident of industrial espionage where Huawei engineers allegedly took photos of and stole parts from phone company T-Mobile's "Tappy", a robot for testing touchscreens.

During his recent trip to Europe, US Secretary of State Mike Pompeo threatened allies that using Huawei equipment might prevent Washington partnering with them. At the Munich Security Conference held 15-17 February in Germany, US Vice President Mike Pence cited China's National Intelligence Law which says private companies must assist in intelligence work. The USA, he said, has been "very clear with our security partners on the threats posed by Huawei and other Chinese telecom companies".

Chinese State Councillor Yang Jiechi, speaking in a Q&A session at Munich, specified that "Chinese law does not require companies to install a back door or collect intelligence"—something that certainly *is* required in Australia under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* passed in December 2018, which compels tech companies to build back doors into their platforms to enable government scrutiny. ("Don't let the Five Eyes spy on you!", *AAS,* 3 Oct. 2018)

On 18 February Australian Prime Minister Scott Morrison claimed that breaches of Parliament House's email network and the databases of major political parties earlier this month were conducted by "a sophisticated state actor". Occurring just a few months before an election is due, and with "Russian interference" in the 2016 US election already being evoked, the implication is unmistakable—China did it!

Founder of cyber security company LMNTRIX, Carlo Minassian, is not giving the government the benefit of the doubt in what he calls "this week's episode of The Australian Government Gets Hacked". In an 18 February *Australian Financial Review* article he accused the government of incompetence when it comes to the most basic cyber security standards, and slammed the (anti) encryption bill for opening back doors that can be exploited by hackers.