Global supply chain poses communications security risk

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

Disputes between the US and China over telecoms companies ZTE and Huawei have renewed focus on the security implications of using foreign technology in communications infrastructure. *Rob Pritchard* examines how countries seek to mitigate these risks

Key Points
- Government efforts to mitigate the risks raised by using foreign software and equipment in communications networks are likely to involve a combination of co-operation with technology companies and classified mitigation strategies.
- Efforts by Western democracies to compel or advise private companies not to make use of foreign products are likely to be ineffective and will not address challenges around foreign components in domestic supply chains.
- Countries with large domestic technology sectors may be better positioned to substitute the use of foreign technology products, but the supply chain risk will prove an enduring challenge for all countries.

In the first quarter of 2018, the United Kingdom's National Cyber Security Centre (NCSC) wrote to an unspecified number of UK telecommunications companies warning of the potential security implications of purchasing equipment from Chinese telecommunications company ZTE. The document has not been made public, but on 16 April details and quotations from the letter were published in the *Financial Times* . The newspaper reported that the letter had been sent to UK telecoms companies, the UK telecoms regulator Ofcom, and ZTE itself.

The NCSC subsequently stated on its website that the letter had been sent to a "limited number" of companies "where there could be national security concerns", and contained technical advice alongside the NCSC's assessment of the threat potentially posed by using ZTE equipment in critical UK communications infrastructure.

Risks inherent in the use of non-sovereign technology are not new, especially for governments and militaries. However, with the rise of China and others as technological powers, Western states have faced a new challenge – the deployment of equipment and software designed and manufactured by companies with close links to potentially adversarial governments onto networks and infrastructure that support critical services.

Concerns over Chinese technology

Huawei, the Chinese telecommunications giant, was founded in 1987 by Ren Zhengfei, a former People's Liberation Army (PLA) engineer. Although initially focused on enterprise infrastructure equipment – the area that has been the primary security concern for Western countries – Huawei has expanded to produce a range of equipment aimed at smaller companies and individual consumers, including smartphones.

Jane's understands that the rapid growth of Huawei has caused concern in intelligence agencies around the world, faced with the possibility of a Chinese company having unfettered access to core communications networks that would once have been considered at least somewhat trusted, even if not actually approved for classified conversations.

The concerns are that Huawei equipment could be used for interception of network traffic or the disruption of the network itself. In July 2013, former CIA and NSA director General Michael Hayden told *TheAustralian Financial Review* as that "at a minimum, Huawei would have shared with the Chinese state intimate and extensive knowledge of the foreign telecommunications systems it is involved with".

The ZTE logo is visible on a building in Beijing on 14 May 2018. In May, the US Department of Defense announced that Huawei and ZTE products would be removed from sale at shops on US military bases around the world. (Wang Zhao/AFP/Getty Images)

1710325

In May 2018, *The Sydney Morning Herald* reported that in papers filed in a Texas court case between ZTE and US company Universal Telephone Exchange, the latter had alleged that ZTE had been founded by "China's Ministry of Aerospace … as a front to send officers abroad under non-diplomatic cover". ZTE's formation in 1985 from organisations that were originally part of the Ministry of Aerospace Industry is a matter of public record, but the implication that it was to create cover for intelligence officers goes beyond previously reported assessments. *The Sydney Morning Herald* noted that ZTE had denied allegations that its staff had engaged in corruption or espionage.

State responses

One approach to this challenge is to ban the use of such products entirely. In May 2018, the US Department of Defense announced that Huawei and ZTE products would be removed from sale at shops on US military bases around the world, with spokesperson Major Dave Eastburn stating that the devices "may pose an unacceptable risk to the department's personnel, information and mission".

In March 2012, the Australian government banned Huawei from tendering for the new National Broadband Network, citing security concerns. In June 2018, Huawei denied claims, first reported by *TheAustralian Financial Review* on 13 June, that the company was "all but certain" to be excluded from participation in building Australia's fifth-generation (5G) wireless networks, on grounds of national security.

Also in June 2018, Prime Minister Malcolm Turnbull announced that Australia would jointly fund the construction of a submarine telecommunications cable linking the country with the Solomon Islands, after the Solomon Islands government terminated a 2016 contract with Huawei to build the cable. According to a July 2017 report in *The Sydney Morning Herald* , in June of that year the director-general of the Australian Secret Intelligence Service (ASIS), Nick Warner, had conveyed to the Solomon Islands government the Australian government's concerns over Huawei's involvement in the project.

The Indian government barred domestic suppliers from using Huawei and ZTE equipment in 2009, although the ban was ultimately short-lived. In an article in *The Sunday Guardian Live* newspaper in April 2018, unnamed Indian security officials expressed continuing concern about the reach of the two Chinese companies in India.

Chinese computer manufacturer Lenovo acquired IBM's personal computer division in 2005, and IBM's server arm in a second purchase in 2015. *The Wall Street Journal* , in May 2015, reported that the sale of the personal computer division had resulted in the US Department of State banning the use of Lenovo PCs and laptops on classified networks, and that the subsequent sale of the server business was causing the US Navy to review the use of former IBM servers in its weapons systems.

In other cases, countries have adopted a mitigation approach. The Intelligence and Security Committee of the UK Parliament (ISC, which provides oversight of the UK intelligence agencies) published the June 2013 report *Foreign Involvement in the Critical National Infrastructure* . The report detailed the history of Huawei's involvement with UK telecommunications company BT, alongside the security concerns of government officials and the inability of government to take any effective action.

The document provided a timeline: Huawei bid to be part of BT's 21st Century Network project (a significant modernisation initiative) in 2003, and was awarded a contract in December 2005, despite security concerns. The report detailed governmental process failings, but noted that it was not clear if the UK government realistically had the ability to prevent BT, or other companies, purchasing equipment from suppliers such as Huawei.

[Continued in full version…]

(950 of 2608 words)

For the full version and more content:

Jane's Military & Security Assessments Intelligence Centre

This analysis is taken from Jane's Military & Security Assessments Intelligence Centre, which delivers comprehensive and reliable country risk and military capabilities information, analysis and daily insight.

*IHS country risk and military capabilities news and analysis is also available within **Jane's Intelligence Review**. To learn more and to subscribe to **Jane's Intelligence Review** online, offline or print visit: http://magazines.ihs.com/*