

Chinese equipment not to be trusted

Written by Taipei Times Editorial
Thursday, 01 February 2018 06:57

Six years ago, on Jan. 29, 2012, Reuters reported on the completion of the African Union headquarters in Ethiopia's capital, Addis Ababa. The building was paid for by the Chinese, who even provided the furniture and IT experts to set up the center's telecommunications equipment.

While critics suspected the reasons for China's involvement in the continent's economic development, African leaders welcomed it. Then-Ethiopian prime minister Meles Zenawi made comparisons between China's rise and the "beginning of the African renaissance," which he at least partly attributed to Chinese investment in infrastructure, energy and telecom technology in Africa.

The article quotes the Democratic Republic of the Congo's then-ambassador to Washington, Faida Mitifu, as saying: "The good thing about this partnership is that it's give and take."

That was certainly an accurate description of the relationship, if an article last week in France's *Le Monde* is to be believed. The report said it was discovered in January last year that there was a nightly spike in the headquarters' server activity between midnight and 2am. Masses of confidential data were being transferred to servers in Shanghai. The following July, a sweep of the building found microphones in the furniture and in the walls.

The union has since replaced its telecom equipment and cleared the building of bugs. Still, that is five years of sensitive data that has been gathered. China has also completed projects in government buildings in other African nations, and recently signed deals to build and finance parliament buildings in Zimbabwe and the Republic of the Congo.

All nations collect data from each other, and Beijing is smart to cultivate African nations, given the continent's geopolitical and economic potential. However, alarm bells should be raised in nations across Asia, Africa and Europe that China is offering to invest in as part of its "One Belt, One Road" infrastructure project.

First, there is the length of time the spying on the African Union headquarters went on. Second, there is the fact that the Chinese got in through the back door under the guise of offering help.

Chinese equipment not to be trusted

Written by Taipei Times Editorial
Thursday, 01 February 2018 06:57

Third, there is the use of ostensibly benign telecommunications technology for the benefit of the Chinese state. Fourth, this was done in a nation Beijing was trying to foster friendly relations with, not a rival, such as the US, or a nation it harbors hostile intentions toward, such as Taiwan.

Concerns over China and cybersecurity have led US President Donald Trump's administration to consider establishing a secure 5G network. It is now exploring options with European and Asian telecom companies. Even private Chinese companies are not included in this, because there is concern that they might be Shanghaied by Beijing into including spy software in the components they use.

In particular, US lawmakers have singled out Huawei Technologies Co, the Chinese network equipment maker, which is expanding around the globe.

Huawei, founded by former Chinese People's Liberation Army officer Ren Zhengfei (任正非) in 1987, is known to have received significant sums in financial aid from the Chinese government and can compete on price with other international providers on this basis.

This is the reason that the US, Australia and Canada are suspicious of Huawei, and that the South Korean government replaced all its telecommunications equipment used to contact the US with that from other companies years ago. In Taiwan, the National Security Bureau bans the use of Huawei's equipment.

Given these revelations of China's willingness to spy and its long-term record of doing so, Taiwanese companies need to be all the more vigilant against using any Chinese telecommunications equipment.

Source: [Taipei Times - Editorials 2018/02/01](#)