Is China out to spy on us through drones and other tech? Perhaps that's not the question we should be asking

May 19 2023, by Dr. Ausma Bernot and Patrick F Walsh

Credit: AI-generated image (disclaimer)

Australian government agencies' use of Chinese-made technology has been making headlines again. This time, the potential threat comes from DJI drones produced by China-headquartered company Da Jiang Innovations.

A cessation order signed earlier this month will see the Australian Defence Force (ADF) suspend its use of DJI products, pending a six-month security audit of the force's supply chain. DJI drones were being used for training and military exercises.

DJI joins a growing list of Chinese technology producers spurring anxiety in Australia and among allies. But the disproportionate focus on Chinese-made technologies might not be doing Australia's national security much good.

A history of pointing the finger at China

It is important to note DJI does have links with China's ruling political party, the Chinese Communist Party (CCP), which has its own branch within the company. DJI also supports public security efforts in Xinjiang. Recent research has demonstrated how private surveillance companies in China will keenly adopt the CCP's language to position themselves advantageously in the domestic market.

All of the above has raised national security concerns in Australia—and not for the first time. In 2018, Malcolm Turnbull's government blocked Huawei from supplying Australia's 5G infrastructure to ensure the security of critical infrastructure. Turnbull said Australia must "defend our sovereignty with the same passion that China seeks to defend its sovereignty".

An ongoing case is also being made against TikTok, with critics pointing to the potential for the CCP to use the app to harvest data. The platform was banned from Australian government devices in April.

In another example, the shadow cyber security and home affairs minister, James Paterson, earlier this year called for the removal of all CCTV cameras at government sites supplied by China-based companies

Hikvision and Dahua. This came after an audit that involved counting the number of Hikvision and Dahua cameras being used on government premises (there were more than 900).

The problems, according to recent debates

Paterson's reviews of the use of TikTok, Chinese CCTV camera and DJI drones by government agencies have been accompanied by two key arguments.

The first considers Chinese companies' links to human rights violations. In 2022, the United Nations published an assessment that determined there was evidence of serious human rights violations against Uyghur and other predominantly Muslim-minority people in Xinjiang province.

The Australian Strategic Policy Institute has monitored Chinese technology companies and their sales in Xinjiang since 2019, and curated a list of 27 companies supplying surveillance infrastructure to the region. DJI, Hikvision and Dahua all compete for market share in China, and this includes sales to public security agencies in Xinjiang.

The second argument considers potential risks to Australia's national security. In the case of DJI, Australia has acted in tandem with the US since 2017, when DJI drones where first prohibited from use by the US military. The same year, Australian Defence Forces suspended their use of DJI drones for two weeks. A recommendation was then made to use them only in non-sensitive and unclassified contexts.

In 2019, the US Department of Defense banned the purchase and use of drones and their components produced in China, and in 2022 made DJI a blacklisted supplier—less than a year before the ADF announced its current security audit.

What should Australia be doing?

In a 2017 parliamentary hearing that included a discussion on DJI drones, the ADF's then deputy chief of information warfare, Marcus Thompson, noted "there were some concerns regarding the cyber security characteristics of the device". The conversation continued behind closed doors.

More recently, Australian Security Intelligence Organisation (ASIO) Director-General Mike Burgess responded to concerns about CCTV camera use by saying: "There's nothing wrong with the technology; it's that the data it collects and where it would end up and what else it could be used for would be of great concern to me and my agency."

These scenarios suggest, when it comes to China, there are risks of potential foreign interference, espionage and data leaks. Yet, at the same time, we don't have concrete evidence of Chinese government agencies accessing Australians' data via tech companies and their products.

Either way, starting a new debate on the use of Chinese technology every few months is not a sustainable security strategy, as much as it is a whack-a-mole tactical response. Nor is it very useful to conduct audits that merely count the number of Chinese-made devices in use.

Protecting Australia's national security interests will require in-depth security reviews of all foreign technologies used, as well as a review of our overall national security strategy. ASIO has a foreign interference task force, which could consider incorporating the vetting of imported tech. Such an approach would help avoid hypotheticals.

It would also clearly articulate roles and responsibilities within government for whatever new technology comes along next. It is not just China that poses risks to Australia's national security. Our politically

driven focus on China takes away from efforts to weed out potential harms from elsewhere, such as Russia, Iran and non-state actors.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Is China out to spy on us through drones and other tech? Perhaps that's not the question we should be asking (2023, May 19) retrieved 25 April 2024 from https://techxplore.com/news/2023-05-china-spy-drones-tech.html