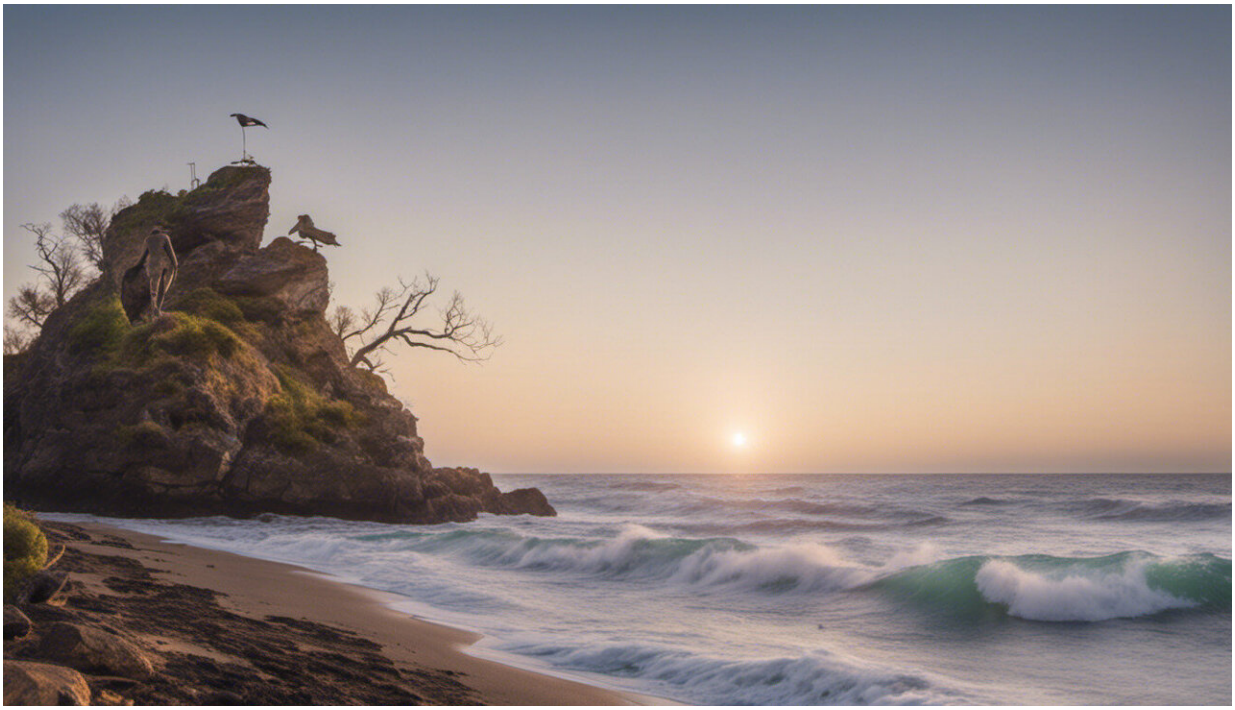
Whacking the mole: how Australia scrambles to regulate Chinese technology

September 12 2018, by Sarah Logan



Credit: AI-generated image (disclaimer)

Did you ever go to your local show as a child? Remember that infuriating game where to win you had to hit every mole which popped its head out of a hole? I imagine Australia's government feels like it's playing whack-a-mole in regulating Chinese information and communications technology right now.

A clearer policy on regulating information and communications technology in the context of national security threats may help. Though in this version of the game, the stakes are rather higher than cheap toys at the local show.

Last month, the Australian government effectively banned Chinese companies Huawei and ZTE from tendering for our national 5G network.

This week, the ABC revealed a range of secure locations using surveillance equipment made by Chinese companies which are likely to be banned from providing such equipment to government in the US.

One in particular, Hikvision (HIK), has very close links to the Chinese government—42% is owned by state-owned enterprises, and the company is associated with a technology lab inside China's Ministry of Public Security.

The ABC's investigations showed surveillance equipment being used in a range of locations, from an Australian defence base in South Australia, to Sydney's Central Station.

Critical supply chains

As a resource-driven economy, Australia is not used to being at the wrong end of critical supply chains. We are familiar with being at the base of the supply chain for critical infrastructure – producing the iron ore, rare earths and coal which make and fuel technology.

But recent concerns around regulating the risk from Chinese information and communications technology (ICT) have revealed exactly how uncomfortable it is at the pointy end of this particular supply chain. It's this user end of the supply chain that the US Department of Homeland

Security says is especially vulnerable to foreign espionage.

Chinese ICT companies are increasingly at the forefront of discussion about information security and cyber risk in Australia, following the strong US lead in this discussion.

In the broader sense, discussions about the risk from Chinese ICT firms are similar to discussions about Chinese investment in critical infrastructure – ports, for example, or gas pipelines. We want to ensure the safety of national assets from the attentions of interests which may not be compatible with our own. But ICT is different.

Four reasons ICT is different

First, the supply chain is murky. In the case of HIK, for example, its products are often rebadged and on-sold by third parties. And the problem is compounded when software is introduced into the mix. Who in government – state, federal or local – should be responsible for assuring the safety of these devices?

Second, where should regulation end? Who is to say whether four components made by a Chinese company in a device make an item vulnerable, but two do not? Can a local council use a HIK camera but a state government must not? Whose job is it to check?

Third, the private sector is directly implicated in ICT and cybersecurity more broadly. Purchasing decisions and cybersecurity practices at even the smallest private sector firm can have an impact on national security, especially given the increasing importance of internet-connected devices.

Finally, Chinese ICT companies are often the cheapest suppliers of equipment (in part, perhaps, because – like HIK – they have been fuelled by huge Chinese government contracts). This means banning them as

suppliers imposes a cost burden on government, the private sector and consumers.

Time for action

Unlike the US, whose lead we tend to follow on these issues, Australia has no domestic ICT manufacturing industry and so – for us – there are no domestic winners from regulating purchasing decisions like this.

Review of foreign investment in critical infrastructure has recently been upgraded.

But ICT has unique and diverse needs. A security camera in Central Station is not the same as a port in Darwin.

Government knows this: 2016's Cyber Security Strategy outlined as one of its goals: "develop guidance for government agencies to consistently manage supply chain security risks for ICT equipment and services."

But the 2017 update on progress in implementing the strategy lists developing such guidance as "not scheduled to have commenced".

Perhaps it should have by now.

Provided by The Conversation