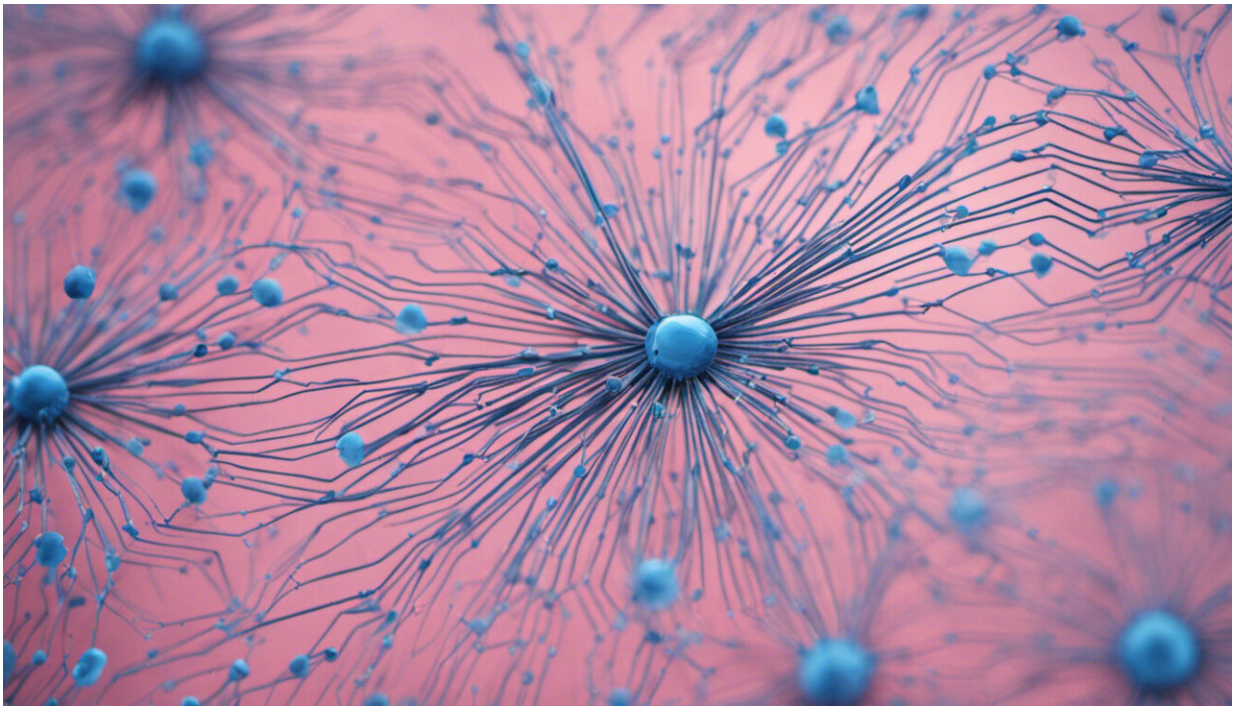
Australia is vulnerable to cyber threats, so what can we do about it?

October 12 2016, by Jill Slay



Credit: AI-generated image (disclaimer)

The Australian Cyber Security Centre (ACSC) 2016 Threat Report, released today, has some concerning details about the state of Australia's cyber security. The report highlights the ubiquitous nature of cyber crime in Australia, the potential of cyber terrorism, and the vulnerability of data stored on government and commercial networks.

Several factors are driving these vulnerabilities. And there is considerable work to do to address them.

The cause

A big driver is the maturation and "professionalisation" of cyber criminals. They have businesses, plans, and online fora (support services offered in many languages). There are even services a potential criminal can easily hire – with botnets used for DDoS attacks going for as little as A$50. DDoS stands for Distributed Denial of Service, and involves attackers sending swarms of bots to overwhelm networks. Recently, DDoS attacks have been getting extremely powerful.

Eugene Kaspersky, chief executive of security group Kaspersky Lab, recently explained that:

as the criminals mature in their operations, the criminals are now offering … "crime-as-a-service" … they are now moving to attacking transportation, and manufacturing … criminals are now hacking coal mine haulage trains, to steal coal or decreasing temperatures inside fuel tanks to steal 3% of fuel with every tank.

The internet is a weapon

We have reached the stage at which the internet has been weaponised. This word was previously only used to discuss events such as Stuxnet, which was a cyber attack on an Iranian nuclear facility thought to be carried out by the United States and Israel. I would suggest we can extend this concept and realise that the internet's corporate, personal and government systems now resemble weapons and weapon systems.

An old-fashioned criminal with a gun could hold up a bank and take

customers' money. Today's criminal, depending on the size of their network-based "weapon", can take our money, our data, our secrets, or disempower us by disabling our electricity, gas or water supply.

We are beyond a point of no return in our reliance on computers and networks, and the demand for innovation in technology is heightening our cyber security problem all the time.

So what should we do?

In a recent discussion paper, my colleague Greg Austin and I wrote:

When it comes to addressing threats from advanced technologies, since Australia is a free and open society facing few enemies, and none that are powerful, the country has been … behind the pace. Awareness in the broader community and even in leadership circles of the threats from advanced technology is quite weak.

We commended the Turnbull government, its innovation strategy, its Defence White Paper, and its Cyber Security Strategy. However, we also noted that:

…there is a large gap between US assessments of advanced technology threats and the Australian government's public assessments. These gaps have important policy implications, as well as negative impacts on the security and prosperity to Australians… The country's education and training policy needs to make giant steps, of which an enhanced STEM approach is only one, and one that will have no strong pay-offs in the next decade at least.

We are in a situation where Australia greatly lacks a trained and experienced cyber security workforce. Existing staff are fully stretched. We have only a trickle of students in the right disciplines in the VET and

Higher Education pipelines. We also lack a local cyber security industry and we find that cyber security solutions are largely supplied by the United States, Israel, Europe, and Russia. We are forced to believe the vendors' rhetoric rather than rely on local expertise.

A checklist for national cyber security

To remedy this situation we created a checklist for effective response to the cyber security situation that exists nationally:

1. The states and Commonwealth should commit to a fast track process to set up a national cyber crime fighting unit to capture and convict more cyber criminals. This should include research staff, funded to at least $20 million per year for ten years.
2. Australia needs to consider creating a National Cyber Security College to get focus and concentrate expertise. Such a body could help generate the following necessary actions:

- Establish nationally approved undergraduate curricula across a range of disciplines in cyber security, using rewards to ensure that teaching is carried out to some national established standard.
- Establish TAFE curricula at Certificate 1-6 since not all jobs are for graduates.
- Determine a transition plan so professionals from a range of specified disciplines can be upskilled and converted into cyber security professionals.
- Devise a dedicated, well-funded plan to generate the 8,000 to 10,000 cyber security professionals needed in the next few years.
- Consider developing a private system and sector-specific initiatives for hybrid education initiatives around the country.

We would not leave our houses unlocked and allow criminals to walk in and steal our possessions. We now need to come up with clever ways of

securing the cyber world and protecting Australians and our economy.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation