

This article is part of a series examining the Coalition government's record on key issues while in power and what Labor is promising if it wins the 2019 federal election.

The government's chief cyber security coordinator, Alastair McGibbon, [told an audience of specialists](#) in November 2018 that the prospect of a catastrophic cyber incident is:

the greatest existential threat we face as a society today.

Using a nautical metaphor, he said such an event was not far off on the horizon, but could be on the next wave. He cited what [one technology expert called](#) the most devastating cyber attack in history, the NotPetya attack in 2017. NotPetya was a random attack on a single day that cost one Danish global company more than A\$400 million dollars.

The latest dire warning from the government is appropriate, yet its policy responses have not quite matched the challenge – or their own commitments.

Read more: [**Should cyber officials be required to tell victims of cyber crimes they've been hacked?**](#)

Cyber security is everyone's business

The government is 16 months into a departmental reorganisation in order to deliver better cyber security responses, especially through the new Home Affairs Department. That department has been very busy with everyday skirmishes in the escalating confrontations of cyberspace – from

Huawei and 5G policy, to foreign cyber attacks on Australian members of parliament.

But Home Affairs is not the only department with a broad responsibility in cyber security policy. On the military side, the Defence Organisation has moved decisively and with discipline. In 2017, it announced the [creation](#) of a 1,000-strong joint cyber unit to be in place within a decade. It also announced increased funding to expand the number of people working in civilian defence roles on cyber operations.

Another department with potentially heavy responsibilities is the Department of Education, working with universities, the TAFE sector and schools. Unfortunately, it appears to be missing in action when it comes to cyber security.

Key plans have stalled

In April 2016, Prime Minister Turnbull [released](#) a National Cyber Security Strategy. It included commitments to grow the cyber workforce ([esp](#) [ecially for women](#)), expand the cyber security industry and undertake annual reviews of the strategy itself.

But in key places the ambitious plans appear to have stalled or fallen short. As a result of the Turnbull overthrow, the post of Minister for Cyber Security – which was only created two years previously – disappeared. The 2018 annual review of the strategy was not released, if it took place at all. The annual threat report of the Australian Centre for Cyber Security (ACSC) did not appear in 2018 either.

In November 2018, AustCyber, an industry growth centre that is one good outcome of the 2016 strategy, published its second [Sector Competitiveness Plan](#). Typical of government funded agencies, it reports much good news. Australia is indeed an international powerhouse of cyber security capability. What is unclear from the report is whether the government's 2016 strategy has much to do with that.

Read more: [*Why international law is failing to keep pace with technology in*](#)

[preventing cyber attacks](#)

Where we're falling short

One indicator that we're off-track is the fact the AustCyber report of 2018 has no data on the participation of women in the sector after 2016. Reports from the decade prior to 2016 showed a decline from 22% down to 19%, but the government does not appear to be tracking this important commitment after it was made.

In other bad news, the AustCyber report concludes that the education and workforce goals remain unfulfilled. It is hard to estimate how badly, since the initial strategy of April 2016 set no baselines or metrics. AustCyber now assesses that:

the skills shortage in Australia's cyber security sector is more severe than initially estimated and is already producing real economic costs.

On the government's commitment to increase the cyber workforce, AustCyber reports growth over the previous two years of 7% – roughly 3.5% per year. But it probably needs to be of the order of 10% per year for a full ten years if the gap identified by the report is to be met:

The latest assessment indicates Australia may need up to 17,600 additional cyber security workers by 2026 ...

The government has [provided \\$1.9 million](#) over four years to promote university cyber security education in two Australian universities. That amount is so small it might not even be called a drop in the ocean. As AustCyber suggests, though in muted language, Australia does have huge resourcing holes in our cyber security education capability.

The most important gap in my view is the near total lack of university degree programs or professional education in advanced cyber operations, the near total lack of technical education facilities to support such programs, such as advanced cyber ranges, and a weakly developed national capability for complex cyber exercises.

What we should be doing

In 2018, I [argued at a national conference](#) sponsored by the government that Australia needs a national cyber war college, and a cyber civil reserve force, to drive our human capital development. I suggested at the time the college should be set up with a budget of A\$100 million per year. Based on a recent [international research workshop](#) at UNSW Canberra, I have changed my estimate of cost and process.

Australia needs a cyber security education fund with an initial investment of around A\$1 billion to support a new national cyber college. It should be networked around the entire country, and independent of control by any existing education institutions, but drawing on their expertise and that of the private sector.

It would serve as the battery of the nation for cyber security education of the future.

Read more: [***The public has a vital role to play in preventing future cyber attacks***](#)

Labor isn't offering a better alternative

The Labor Party, through its cyber spokesperson Gai Brodtmann, [has been critical](#) of the government's failure to fill the gaps. But she is retiring from the House of Representatives at the next election.

Labor has no well developed policies, and no budget commitments, that can address the gaps. There is even reason to believe the party doesn't have a front bench that is engaged with the

Written by Greg Austin, Professor UNSW Canberra Cyber, UNSW

scope of the challenge. None of them seem to be as technologically oriented as Turnbull, the last cyber champion the Australian parliament may see for a while.

Greg Austin does not work for, consult, own shares in or receive funding from any company or organisation that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.

Authors: Greg Austin, Professor UNSW Canberra Cyber, UNSW

Read more <http://theconversation.com/australia-is-vulnerable-to-a-catastrophic-cyber-attack-but-the-coalition-has-a-poor-cyber-security-track-record-113470>