Over the next four years, Australia's federal government will invest more than A$230 million on cyber security. Put another way, A$57.5 million per annum will be taken from one part of the federal budget and spent instead on cyber security.

The government's long-awaited Cyber Security Strategy does not detail how these funds will be spent across the "five themes of action" included in the strategy.

Yet this information is curiously available from other sources. Some A$38.8 million is expected to be spent relocating the same Australian Cyber Security Centre where the cyber security strategy was initially announced two years ago.

Other large line items, not detailed in the strategy document but reported elsewhere, include A$5.3 million annually to increase the capabilities of Australia's Computer Emergency Response Team, A$11.8 million annually to establish joint cyber-threat sharing centres and an online threat sharing portal, and A$7.6 million to create a national cyber security innovation network. To boost the government's intelligence and investigative abilities, the Australian Federal Police will receive A$5.1 million and the Australian Crime Commission an additional A$4 million annually.

Some have referred to Australia's Cyber Security Strategy as " mature and nuanced " and compared it with that of our closest allies. A closer examination is warranted.

In the US, for example, there is no unified national strategy. Rather, a patchwork of plans exists including a Cybersecurity National Action Plan , a Cybersecurity Strategy and Implementation Plan (CSIP), a Comprehensive National Cybersecurity Initiative , and the Department of Defense’s Cyber Strategy , among many others. This reflects the fragmented way in which responsibility for cyber security policy is allocated across the US.

There is a large differential in spending between Australia and the US. In the 2017 US federal budget request, more than US$19 billion is requested for cyber security, representing more than a 35% increase over the previous year. The US thus spends US$43.48 per person annually and Australia plans to spend A$2.50 (US$1.92 per person annually.

Simply comparing the total spend between two countries does not equate with the effectiveness of that spending. This is because the effectiveness differs according to the different program design and implementation between countries. However, for a country with an annual GDP that is 10 times the size of Australia's (at current market prices), and a population that is 13 times larger than Australia's, this is an enormous differential.

Following America's lead, but why?

Many of the ideas in the Australian strategy are derived from the US, particularly the Comprehensive National Cybersecurity Initiative. Australia's plan calls for coordination of public and private research and development funding, connecting research centres, and expanding education.

Australia will have a new "cyber ambassador", a role similar to that of the Coordinator for Cyber Issues in the Department of State. The focus on the past year has been on the Cyber Security Information Sharing Act (or CISA), a law that allows for more information sharing between public and private organisations around cyber security threats. So too information sharing figures heavily in the Australian strategy.

This would be fine if we knew whether these programs worked. The issue is that almost none of the US programs or strategies have actually been evaluated. We just don't know how effective the tens of billions of dollars spent over the past decade have been. For instance, the Department of Homeland Security (DHS) operates a threat detection system called EINSTEIN. When the Government Accountability Office evaluated the US$6 billion program in January 2016 it found that, "none [of the metrics developed by DHS] provide insight into the value derived from the functions of the system".

Finally, the threat of cyber attacks and the economic damage they might entail are not well known. There's good reason to think that we spend

more on cyber security than we lose due to attacks
. The Australian strategy explicitly calls for analysis so as to generate better answers to these questions. The absence of answers to these foundations questions makes it hard to determine whether too much or little funding is being allocated to address the risks and how the funding should be allocated.

Go to the source

With so much attention being paid by policy makers to cybersecurity, why do neither of these strategies attempt to address the root causes of the problem?

For example, software containing bugs continues to be rushed to market, putting users of these products at increased and unnecessary risk. A more cost-effective way to improve cybersecurity through public policy would seek to incentivise companies to make more secure products before shipping them to market. This is what was done to improve the safety of automobiles in the 60s – by imposing product liability on car makers.

Instead, the strategies on offer suggest governments worldwide intend to continue to escalate a hacking arms race. Despite the clear intention to, “actively promote an open, free, and secure cyberspace”, the Australian strategy’s most revealing passages relate to the intention to, “deter and respond to malicious cyber activities”, through the use offensive cyber capabilities. The US Department of Defense likewise made an overt indication of its intention to use offensive capabilities in its cyber strategy last year. This arms race will thus continue to escalate and thus degrade the openness, freedom and security of cyberspace. Companies and individuals that are subject to or caught up in these attacks will continue to be the collateral damage.

It is astounding how fast the cyber security situation has evolved in just the past five years. This rate of change is not slowing down. Getting these strategies right requires the identification and correction of contradictions in cyber security policy. This in turn requires program evaluation to determine what worked and what did not. When another review is announced in five years time, it would be good to be in a position to answer these questions, which is something we are still unable to do, and which becomes so evident in the newly released strategy.

Benjamin Dean does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond the academic appointment above.

Read more http://theconversation.com/more-money-doesnt-guarantee-success-in-cyber-security-race-58146