Though mature and nuanced, the cyber security strategy delivered by Prime Minister Malcolm Turnbull last week matches neither the spending plan or the language of our closest cyber allies.

The plan promises to redress important deficiencies in the country's posture, but apart from mentions of terrorism, it does not openly discuss key sources of malicious activity, such as China and Russia. The strategy does not have a spending plan adequate to address the pace and scale of emerging threats to the digital economy and national security.

The core problem could be that we simply don't see the menace of cybercrime with the same sense of urgency as our allies do.

In Turnbull's preface to the strategy, he acknowledges:

The scale and reach of malicious cyber activity … is unprecedented. The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving.

The report says Australia needs to prepare for a "significant cyber event", with the scale of the effect unspecified.

And in 2015, the Australian Cyber Security Centre reported that "Australia has not yet been subjected to any activities that could be considered a cyber attack" (defined as an attack "seriously compromising national security, stability or prosperity".)

We can compare this persistently anodyne Australian script with the language of President Obama in March this year :

“Significant malicious cyber-enabled activities” from outside the country continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

He made this statement in formally declaring the continuance of a national security emergency in cyberspace that he had declared for the first time one year earlier. This is his admission that the most powerful country on the planet has consistently failed to secure its main cyberspace assets in the face of specific rampaging and escalating threats.

This discrepancy on threat presentation between Australia and the United States could be defended on the grounds that the Australian government has chosen to pursue a more diplomatic style in public, or that it prefers to keep a lower profile on cyber threat issues, while sharing identical perceptions of the threat with key allies.

Yet there are some strong indicators that this not the case.

One such indicator is the matching discrepancy between the new resources devoted to current and emerging threats by Australia compared with its allies.

In the Turnbull blueprint, the new funding commitment for the civil sector is A$230 million over four years. This compares with a recent US government commitment of A$24 billion (US$19 billion) under an emergency package of new cyber security measures largely for the civil sector just for FY 2017.

The UK has recently announced a supplementary five-year spend of A$3 billion (£1.9 billion) on cyber security measures. On an annualised basis and rough approximation, these two packages are, respectively, 400 times higher and 10 times higher than the newest Australian supplementary commitments (to the extent that they can be compared).

Measuring success

The strategy’s eight-page action plan, along with its indicators of success, is ambitious in its

scope. Novel measures include joint public-private threat assessment centres in the states and a series of new appointments, including an Assistant Minister, a Special Adviser (both reporting to the PM) and an ambassador for cyber affairs. There are radical commitments to widen the services of the Australian Signals Directorate in the Department of Defence to meet private sector customer needs.

But many of the new commitments are fairly generalised and lack granularity, such as the intent to increase numbers for cyber security graduates, women in the profession, and school kids “in the know”.

In the absence of quantification of such commitments, the good news is the government will report annually on its success.

In one year’s time, we will want to know from the government how many more cyber graduates we have compared with this year. In the medium term, we will need the government to provide some metrics on how many graduates in the field we actually need. We also need to see the baseline statistics for this year.

We might ask the government fairly promptly for some elaboration on just what levers it intends to use, in partnership with universities and the corporate sector, to pursue the cohort goals in cyber security and what sort of money it is prepared to put into it.

Australia has some way to travel before it graduates to a coherent national cyber security strategy fully informed by global realities and funded accordingly.

Greg Austin 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/australia-still-doesnt-see-a-cyber-attack-as-the-menace-our-allies-fear-57719