Time for the government — and media — to tell the truth about cyber hysteria

Bernard Keane, political editor, in Crikey.com June 22, 2020

The government has no right to lecture anyone about cybersecurity while it is party to making the world's IT networks less secure — all in the name of spying for western corporations.

(Image: AAP/Lukas Coch)

If the government were serious about protecting Australia's businesses and governing institutions from "sophisticated state-based cyber actors", there's a pretty simple thing it could do: instead of using security flaws in widely used software for commercial espionage, it could alert software manufacturers to them.

But it won't do that, because nonsense like Friday's cybersecurity media conference — in which a prime minister and his defence minister breathlessly announced the nation was under attack — are about theatre and distraction.

The follow-up to Scott Morrison's histrionics was today's warning that businesses would — in news that must have gladdened the hearts of every CIO in the country — be forced to invest in greater cybersecurity. Except, the government's latest cybersecurity strategy, being assembled by the Keystone Cops of the Home Affairs Department, is already months late.

In fact, Home Affairs itself is the worst-performing portfolio when it comes to meeting the basics of the government's own internal cybersecurity requirements — having been repeatedly chipped by the Australian National Audit Office and the Joint Committee for Public Accounts and Audit about its poor cybersecurity performance.

That's how seriously the government takes cybersecurity.

To be fair, Home Affairs is merely composed of bumbling, under-resourced, badly led bureaucrats.

Other sections of government are a direct threat to the cybersecurity of Australian business, institutions and individuals: the Australian Signals Directorate (ASD) and the sections of other security agencies engaged in signals intelligence.

As part of the Five Eyes and its intelligence-gathering infrastructure, Australian agencies like ASD routinely exploit security weaknesses in widely-available software used by business, governments and other institutions — exactly like China, Russia, every other intelligence service and criminal groups worldwide.

Together, they power a multi-billion dollar global industry based on rapidly identifying security weaknesses in software products from Microsoft, Apple and all other major IT providers, and then exploiting them before the manufacturers realise they are there and patch them.

A former senior NSA official told *Crikey* a couple of years ago that the NSA fails to tell manufacturers about around 10% of security flaws in widely used software, so that it can exploit them — and share them with allied agencies like ASD to be exploited.

That means that the Australian government is lecturing us all about making sure our IT systems are fully patched — but actually is party to withholding information from software manufacturers that would better enable them to quickly patch flaws.

Think that's just conspiracy theory? Three years ago, Microsoft criticised the NSA for doing exactly that, after a worldwide ransomware attack exploiting a Microsoft XP flaw.

To make matters worse, the NSA had had its trove of exploits — the software tools that exploit the security flaws — stolen, and one of them was the basis for the software behind the ransomware attack. The CIA later suffered a similar fate.

A recently released report revealed that the CIA's security around its software tools was "woefully lax" and that it was more focused on sharing its exploits around than security.

Given this, any Five Eyes government has no right to be lecturing companies about keeping their systems updated and patched. They're as big a part of the problem as the Chinese/Russians/criminals /insert bogeyman of the month here.

All this might be justified if outfits like ASD were pursuing terrorists, child abusers or organised crime. In fact, their priority is commercial espionage, like the Chinese.

Just ask ASD: they're the ones who spied on Indonesian trade negotiators while they were talking to their US legal firm during a trade dispute with the US. The "highly useful" information was used to benefit US corporations. That's just one of a long list of examples of Five Eyes agencies engaging in commercial espionage revealed by Edward Snowden.

How do we know commercial espionage is a priority over fighting terrorism et al for western intelligence agencies? Remember that when Alexander Downer and John Howard ordered the Australian Secret Intelligence Service (ASIS) to illegally bug the Timor-Leste cabinet in 2004, it was to advantage Woodside in Australia-Timor-Leste negotiations over resources access.

In doing so, they took precious resources away from counter-terrorism operations in Indonesia at a time when Islamist terrorism against Australia was surging.

Had ASIS been doing its counter-terrorism task rather than, at the direction of Howard and Downer, bugging the cabinet office of a micro-state, it's possible that eight people may not have perished in the September 9, 2004 car bombing targeting the Australian embassy in Jakarta. We can never know for sure. But the Australian government had indicated its priorities: the interests of an Australian corporation over stopping terrorism.

What a shame neither the government nor the media, given to breathlessly reporting Australia's alleged victimisation by Chinese hackers, ever bothers to provide the full story.