Beware Dutton’s new Cyber Security Strategy

Citing a great and evolving threat to Australian infrastructure, Home Affairs Minister Peter Dutton announced a consultation for a new Cyber Security Strategy to include high-level coordination between the government and corporate sectors to target cyber-crime.

The government’s 2016 Cyber Security Strategy established the Australian Cyber Security Centre within the Australian Signals Directorate (ASD), the agency responsible for foreign signals intelligence and military support operations. Joint Cyber Security Centres were set up in most state capitals to work with industry, and a 24/7 Global Watch body to respond to critical cyber incidents. An Information Warfare Division (!) was created within the Australian Defence Force in July 2017, which includes a cyber unit with responsibility for defensive and offensive cyber activities.

Home Affairs is taking submissions until 1 November 2019.

Dutton’s consultation paper states that while strong progress has been made, “the threat environment has changed significantly and we need to adapt our approach to improve the security of business and the community”. Cyber-crime is growing in scale and severity, the report alleges, and cyber criminals, including state actors, have been emboldened. Cyber-crime is estimated by the department to cost Australian business up to $29 billion per year.

The report’s authors decry having to operate “within a legislative framework that was established before the internet became a foundational element of our economy, and without a modern perspective on how malicious cyber activity crosses traditional geographical borders”. Despite some 75 new security laws passed since 9/11, the government is pushing for more. In a section titled “How can the government proactively address national cyber threats?”, the report says that currently “Government can only take direct action to prevent or respond to cyber security incidents with the permission of network owners (including other government agencies). This takes time and gives malicious actors an advantage. *In national emergency situations, it may be appropriate for Government agencies to take swifter action*.” (Emphasis added.) The government is considering “both stronger enforcement of existing laws and new requirements”.

The paper cites Europe’s Network and Information Security Directive, which is transposing a supranational directive into the law of all European states, with the UK a leading international example of how such measures “can be used to protect citizens”. The UK, however, has a reputation for threatening people’s rights in the name of protecting them from a terrorist scourge it has itself fostered (*Stop MI5/MI6-run Terrorism!*, CEC, June 2017). As per the UK model, the Australian government is calling for public-private coordination to target cyber threats. A new UK law passed in February, the *Counter-Terrorism and Border Security Act 2019*, amended existing legislation to allow the Home Office to share previously classified information on “subjects of concern” with local councils, businesses, social workers and teachers. The private sector is enlisted to report suspicious activity or purchases; social media hosts are called on to report and remove extremist or suspicious content. Surveillance warrants can be obtained merely to assess risk, including in the poorly-defined category of “hostile state actors”. It also strengthened powers to shut down the City of London financial centre to all foot and vehicular traffic in the event of a threat, which could conceivably include the reaction to a financial crisis. (“‘Techno-Stasi’ police state laws before UK parliament”, *AAS*, 27 June 2018.)

Will Australian agencies be similarly afforded expanded powers to spy on its own citizens? Asked at a 4 September Lowy Institute event if Australian spy agency ASIO had sufficient surveillance powers to deal with potential new threats, outgoing ASIO head Duncan Lewis left the door open to similar activity by the Australian Signals Directorate, which can currently only spy overseas.

While security and law enforcement agencies have seen a significant increase of their powers due to the growing cyber threat, said Lewis, “it is necessary to have a look at capabilities such as the ASD to see whether it can inform, or assist, or be deployed in the extreme in protecting Australians”. News Corp journalist Annika Smethurst’s home was raided in June over her 2018 article reporting on letters between Department of Defence head Greg Moriarty and Home Affairs department head Mike Pezzullo

discussing that very topic—legislative reform “to enable ASD to better support Home Affairs priorities”.

Targets: China, Russia

Reporting on the cyber security document on 6 September, the *Australian*’s Ben Packham wrote that “China and Russia are considered Australia’s top cyber adversaries”, and without presenting a shred of evidence, proclaimed China “the prime suspect” in the hack of Australian National University student records and the February attack on the IT system of Parliament House. Packham cited anti-China thinktank the Australian Strategic Policy Institute’s (ASPI) International Cyber Policy Centre (ICPC), with a scaremongering warning: “So far no one has died from a cyber-attack, but we are on the cusp of that changing”, said director of the outfit, Fergus Hanson. “Now we are getting more and more physical systems connected to the internet, it’s inevitable.”

Launched in 2013, ASPI’s cyber centre “has a capacity building team that conducts workshops, training programs and large-scale exercises both in Australia and overseas for both the public and private sectors”, its website states. The cyber centre receives funding from the ASD, in addition to cyber heavyweights like Microsoft, Amazon, Facebook and Google. Further funding flows from the government-funded Cyber Security Cooperative Research Centre at Edith Cowan University in Perth, which coordinates action between industry, government and the research sector. With ASPI sponsorship coming from defence giants Lockheed Martin, Raytheon, Thales and MBDA Missile Systems, it is no surprise it echoes the ambitions of the Anglo-American military-industrial complex. Why should the Australian government be funding, and presumably taking advice from, such an entity?

The ICPC has partnered with the industry body for information security professionals, the Australian Information Security Association (AISA). The body will co-host the Australian Cyber Conference 2019 on 7-9 October in Melbourne, with the ASD and Australian Cyber Security Centre. Sponsors of the “Change the rules, up the game”-themed conference include ASD, Microsoft, BAE Systems, and Big Four auditor PwC. The Home Affairs report alluded to the broader agenda of the global establishment that sets our foreign and economic policy, by stressing that “Australia already works closely with international partners to share information and build support for international rules and norms to govern the responsible use of cyber space.” This takes place through the Five Eyes spying alliance (USA, UK, Canada, Australia and New Zealand) which is establishing a *transnational* model for security, making terrorism and cyber-crime the latest excuse to transcend national sovereignty and target nations that resist the trend.

Australian Alert Service, 25 September 2019
