Spies on the rise as nation gets battle-ready

In October 2019 Secretary for Home Affairs Michael Pezzullo warned a Senate Estimates hearing that Australia faced a “cyber Pearl Harbor”—a devastating cyber-attack on critical national infrastructure—unless his department was granted sweeping new legal powers. The lynchpin of such a capability, according to Pezzullo, is giving the Australian Signals Directorate (ASD) access to privately run infrastructure which could be subject to attacks, from energy suppliers to banks. While Pezzullo claimed this would not be leveraged “into some kind of mass surveillance program on Australian communications”, detecting such a threat would require accessing data from the entity’s computer systems, bank records and email or text messages, just as News Corp journalist Annika Smethurst reported in the April 2018 *Sunday Telegraph* article which got her raided by the Australian Federal Police in June last year. (“Pezzullo hypes ‘cyber Pearl Harbor’ in push for more police-state powers”, *AAS*, 6 Nov. 2019.)

If you were watching the news on 19 June, you could have been forgiven for thinking PM Scott Morrison was announcing an actual—military not cyber—Pearl Harbor attack, as he sombrely opened a press conference by saying he would “read from a prepared statement”. He declared that Australia was “currently” under cyber attack by a sophisticated state actor, with a range of sectors being targeted, “including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure”. The Prime Minister noted that the ASD already has very close engagement with domestic private sector operators, to detect such threats, the collaboration involving “contact and disclosure”. The ASD is responsible for foreign signals intelligence and military support operations, and is not supposed to operate domestically except in specific emergency situations.

Morrison's 19 June press conference. Photo: Screenshot

Journalists who initially reported Morrison’s remarks verbatim, were later forced to clarify that there was no actual, new attack. It was almost a *War of the Worlds* moment,[1] designed to create a lasting impact on the population long after the realisation that there were no facts backing up the PM’s claims had been forgotten.

On 1 July at the Australian Defence Force Academy, Morrison launched a new Defence Strategic Update and Force Structure Plan, which brought Australia fully into line with new US and UK defence and security strategies released in 2017-18 which named competition with major powers Russia and China as the greatest strategic threats. Comparing the situation to the 1930s and 1940s, Morrison announced increased military spending in order to be “a better and more effective ally”. (“Morrison’s indefensible Defence plan recommits to Cold War with China”, *AAS*, 8 July 2020.) The planned expansion of Australia’s spying apparatus occurs in the context of this war footing.

Cyber strategy

The Home Affairs Department is currently overseeing consultations on the 2020 Cyber Security Strategy. Morrison foreshadowed in his 19 June press conference the release of the “new cyber security strategy in the coming months”. As part of a larger $15 billion investment in cyber and information warfare capabilities, on 30 June Morrison announced $1.35 billion for a cyber security upgrade. The new Cyber Enhanced Situational Awareness and Response (CESAR) package will include recruitment of five hundred extra ASD spies and will distribute funds to: the ASD to target cybercrime, both offshore and in assisting domestic authorities; creation of a new cyber threat-sharing platform for industry and government to share intelligence and block threats; development of a “national situational awareness capability” to help vulnerable entities mitigate threats; and new research laboratories and expansion of data science, technological and intelligence capabilities.

An extra 1,700 intelligence and cybersecurity jobs over ten years had been announced with the

launch of the 2016 Defence White Paper. This included a cyber unit, the Australian Cyber Security Centre, which now resides at the ASD; Joint Cyber Security Centres in most state capitals to work with industry; a 24/7 Global Watch body to respond to critical cyber incidents; and an Information Warfare Division within the Australian Defence Force, which includes a cyber unit with responsibility for defensive and offensive cyber operations.

The Australian Strategic Policy Institute (ASPI), which has its own International Cyber Policy Centre that receives funding from the ASD as well as tech companies like Microsoft, Amazon, Facebook and Google, has called for "a central hub in the Department of Home Affairs" to host cooperation between the private and public sectors in the defence of national security. "Corporations hold considerable data that may be of benefit to governments during and after incidents", wrote ASPI Senior Fellow Anthony Bergin in the 8 January *Australian Financial Review*. "The Office of National Intelligence is seeking to expand its links to the private sector through more active engagement with business groups", he added. Such coordination has already been adopted in the USA and UK, where it is known as the fusion doctrine. In Australia, private citizens or companies can already be compelled by intelligence agencies to hand over data or provide assistance to spies under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*. ("Don't let the Five Eyes spy on you!", *AAS*, 3 Oct. 2018.) In the expansion of its multi-tiered deep-state infrastructure, Home Affairs is also pushing for a new Countering Foreign Interference unit, to crack down on what our spies judge to be "fake news".

Banks sharing your data

According to the 13 January *AFR* Jacqueline Craig, a former chief of the Cyber Electronic Warfare Division at the Department of Defence and now fellow at the Australian Academy of Technology and Engineering, said that to avert catastrophe, "Banks, physical infrastructure and large industry need to be able to communicate information with the government in real-time." Under the pretext of the coronavirus health crisis, since April the banks have been facilitating just that: sharing data from consumer accounts with the government on a weekly basis, allegedly to inform crisis-response decisions. The information is reportedly "anonymised and aggregated", but due to the increase in digital banking it allows banks a "mind-boggling" window into daily money flows into and out of private accounts, which can be broken down by postcode. "The banks are working collaboratively with the government through the sharing of economic data covering consumer spending and credit trends during this period", Treasurer Josh Frydenberg told *AFR Weekend* 20 June. If the government had its way and cash were heavily restricted, there would be no way of escaping such surveillance.

Bank regulator the Australian Prudential Regulation Authority (APRA), which is in charge of all collection of financial information for the Reserve Bank, Australian Bureau of Statistics and government under the *Financial Sector (Collection of Data) Act 2001*, has been working closely with "the world's top intelligence agencies" to combat cyber-attacks, reported James Frost in the 10 January *AFR*. APRA head Wayne Byres told *AFR* the bank regulator was working closely with the ASD's Cyber Security Centre and the domestic spy agency ASIO (Australian Security Intelligence Organisation), as well as their international peers. With a global financial disaster worse than 2008 in progress, unless it is forced by the people to change its allegiance the government will utilise any and all powers in its arsenal to save the banking system: the distraction of war, "anti-terror", national security and foreign interference laws, extraordinary banking powers dictated by foreign agencies, cash bans and more.

Footnote:

[1] A 1938 US radio broadcast of the H.G. Wells book was so realistic, even interrupted by news bulletins, that it had people believing there was an alien invasion in progress.

By Elisa Barwick, Australian Alert Service, 15 July 2020

Printed from http://citizensparty.org.au/print/pdf/node/739, on 12 Dec 2023 at 06:12 am