Pezzullo hypes 'cyber Pearl Harbor' in push for more police-state powers

By Richard Bardon

4 Nov.—The Canberra defence and intelligence establishment may have finally reached the nadir of idiotic hyperbole in its latest bid to frighten Parliament into handing it yet another tranche of police-state powers. Exhibit A is the assertion by Secretary for Home Affairs Michael Pezzullo at a 21 October Senate Estimates hearing that Australia faces a devastating cyber attack on critical national infrastructure, a "cyber Pearl Harbor", unless his department is granted authority to deploy on home soil electronic spying agency the Australian Signals Directorate (ASD), which (officially) only operates abroad. But whilst Home Affairs' written statements on cyber security emphasise the protection of essential services such as electricity, water and communications, Pezzullo in his Senate testimony sought to expand his department's remit to the protection of *financial markets*—bearing out the Citizens Electoral Council's longstanding charge that Australia's intelligence agencies, like their sister agencies throughout the Five Eyes alliance (Australia, Canada, New Zealand, UK, USA), exist not to protect the people, but to preserve the rule of the corrupt Anglo-American financial oligarchy.

The idea of a domestic role for the ASD was officially floated this September, in a Home Affairs discussion paper on "Australia's 2020 Cyber Security Strategy". As the *Australian Alert Service* reported at the time,[1] the government's 2016 Cyber Security Strategy had provided a mandate to strengthen the nation's cyber security, resulting in the creation of the Australian Cyber Security Centre (ACSC) within 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 activities. The September discussion paper praised these efforts, but declared that "the threat environment has changed significantly and we need to adapt our approach…. The Government is most concerned about threats to Australian businesses that provide essential services, such as energy, water, telecommunications and transport."

Mission creep

Pezzullo told the Senate that these concerns were what had prompted correspondence between himself and Defence Secretary Greg Moriarty in February 2018, made infamous in an April 2018 *Sunday Telegraph* article by News Corp journalist Annika Smethurst, whose reporting got her raided by the Australian Federal Police (AFP) this June.[2] Smethurst reported that a top-secret proposal signed off by Pezzullo and ASD boss Mike Burgess sought then-Defence Minister Marise Payne's support for "legislative reform to enable ASD to better support a range of Home Affairs priorities", which would allow ASD hackers to "proactively disrupt and covertly remove" onshore cyber threats by "hacking into critical infrastructure", and empower the agency to access data such emails, bank records and text messages without a warrant, on the say-so of the Home Affairs and Defence ministers. At the time, Pezzullo justified these measures as being targeted at child exploitation and the online operations of transnational criminal and terrorist networks. Now, however, he has dropped the mask, effectively admitting in testimony to the Senate Legal and Constitutional Affairs Legislation Committee that Canberra is "most concerned" not about the essential services upon which the population's lives would depend in a crisis, but with preventing disruption to the financial system, which has come to be synonymous with the national interest so far as official Canberra is concerned.

The April 2018 article by Annika Smethurst which first exposed Home Affairs' plans to spy on Australians, and outraged "Iron" Mike Pezzullo. Photo: Screenshot

Already, the definition of terrorism under the *Security Legislation Amendment (Terrorism) Act 2002* includes any "action or threat of action … [which] disrupts, or if carried out would disrupt banking … or insurance"; and the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* criminalises the mere *possession* of information "likely to cause harm to Australia's interests", including "economic" interests.[3] These laws are enforced by AFP and domestic spy agency the Australian Security Intelligence Organisation (ASIO), but Home Affairs is now looking to deploy the ASD on the same pretext—even where no "national security interests" are involved. Asked by committee chair Sen. Amanda Stoker whether "a cyber attack with economy-wide ramifications" is a real risk, and if so what is being done about it, Pezzullo answered that the danger is imminent and that the government, ASD and the private sector are working together to "close this gap in sufficient time before that day, the equivalent of a cyber Pearl Harbor, comes." In addition to threats posed by (unnamed) "state actors", he said, there are also "what I would describe as very sophisticated non-state actors whose interests … may not be of a geopolitical or diplomatic motivation—that is to say, *to coerce us in terms of our national security interests*…. It could well be that in the not-too-distant future a capable non-state actor … may have motive, means and capacity to, for instance, *short a market to change market signals and take advantage of that from a profit point of view*. In years to come that might be as concerning to us as what certain state actors do." (Emphasis added.)

Smethurst's anonymous government source said of Pezzullo's March 2018 proposal, "There is no actual national security gap this is aiming to fill other than a political power grab." This is undoubtedly true—because the *Intelligence Services Act 2001* already permits the ASD to intervene, with Ministerial authorisation, on an emergency case-by-case basis to prevent "serious crimes" (i.e. one which carries a penalty of more than 12 months' jail) involving the movement of money, goods or people, transmission of data, or the use or transfer of intellectual property. Plainly, any cyber-enabled crime serious enough to qualify as a "cyber Pearl Harbor" would already be captured.

1. "Beware Dutton's new Cyber Security Strategy", *AAS*, 25 Sept. 2019.
2. "The Five Eyes war on truth", *AAS*, 12 June 2019.
3. "Is it a terrorist offence to warn Australians about the financial system? It could be!", CEC media release, 18 June 2019.