Australia ups ante on Five Eyes campaign vs. China

The Five Eyes intelligence agencies accuse all Chinese companies of being agents of the state, but the same agencies require all private companies in their own countries to do the bidding of their supranational, anti-democratic surveillance apparatus.

By Elisa Barwick

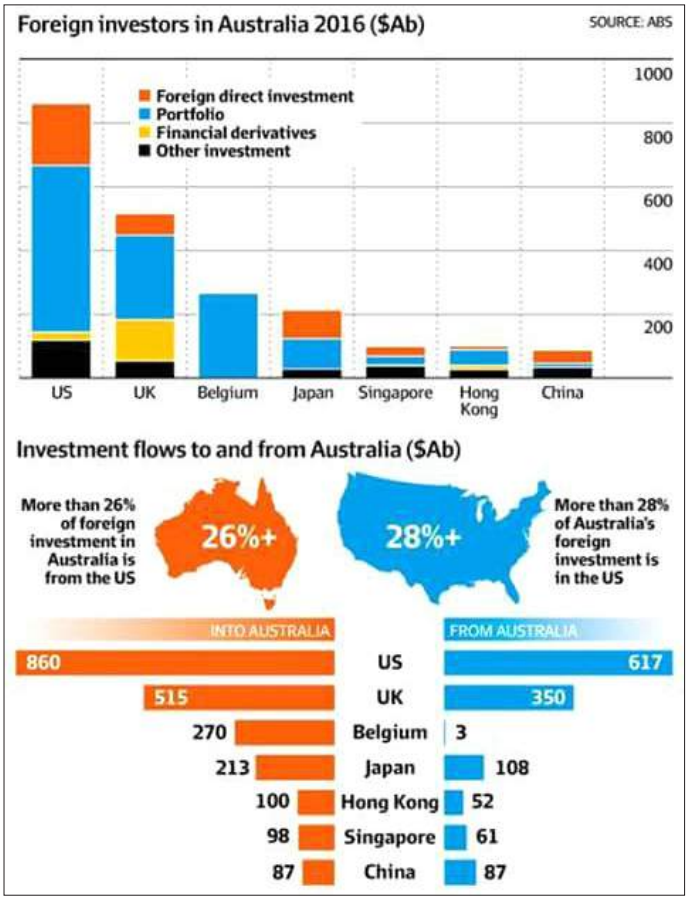
Two of Australia's top spy chiefs are leading the charge to implement an upgraded Five Eyes plan to counter China's foreign outreach. Over the last year, the Five Eyes spying alliance, comprising the UK, USA, Canada, Australia and New Zealand, has held special meetings to discuss China, in combination with its campaign to create a global security and spying infrastructure, a.k.a. a global police state **(box, p. 10)**. China's advanced, market-dominating digital and technological capabilities pose a threat to that plan.

According to the *Australian Financial Review* of 16 January, Australia's Foreign Investment Review Board (FIRB) now believes there is no such thing as a private company in China, in what is a snub to our largest trading partner and a threat to the 2014 China–Australia Free Trade Agreement (CHAFTA). The head of the FIRB, David Irvine, is a former head of ASIO, the Australian Security Intelligence Organisation (2009-14), and director-general of ASIS, the Australian Secret Intelligence Service (2003-09). He also served as Australian Ambassador to China (2000-03) and Papua New Guinea (1996-99).

Though thresholds cited on the FIRB's website remain unchanged, *AFR* cites "a senior figure with direct knowledge of the FIRB board's thinking" on the decision to effectively treat all Chinese companies as agents of the Communist Party of China; Irvine publicly refutes the claim. Under CHAFTA, thresholds triggering FIRB scrutiny of private Chinese investment were raised, in line with other countries with which we have trade agreements, while all state investments were still subject to review. According to *AFR*'s source, this will change and there will no longer be a distinction between Chinese state and private investors. All deals would be scrutinised, because "Chinese companies will do as they are told" by the government, the source said.

Irvine stopped Hong Kong company Cheung Kong from taking over gas distributor APA Group, and State Grid from taking over NSW electricity distributor Ausgrid (which the Citizens Electoral Council also opposed); but is he as scrupulous when it comes to foreign investment from the USA, UK, or Belgium, whose share in the foreign takeover of Australia is much greater than China's? (graphic) Crucial infrastructure should not be outsourced or sold off—*to anybody*; this should include healthcare giant Healius (formerly Primary Health Care), which would dissolve concerns over access to sensitive data.

As the FIRB shift was being reported, the head of Australia's peak intelligence body, Nick Warner, was in Vanuatu with Prime Minister Scott Morrison during his visit to that South Pacific nation and Fiji in an effort to coax Pacific Island nations to put Australia ahead of China when it comes to economic, military and security arrangements. While Morrison claimed his interest in the region was not in reaction to China's rising influence, his insistence that "We're here because ... they are our neighbours and family" was undermined by the fact that it was the first visit by an Australian leader to Vanuatu in 29 years, and the first to Fiji in 13.



These graphics show that Chinese investment in Australia is greatly exaggerated, and that Australia invests as much in China as China does here. Australian government policy is at fault when it comes to foreign investment, not China's. Source: *AFR*

Warner, who is director-general of the Office of National Intelligence, which oversees all Australian intelligence agencies, had played a key role in sinking Chinese telco Huawei's deal to build an undersea internet cable linking Papua New Guinea and the Solomon Islands with Australia, which was to have been funded by China's Exim Bank. This was achieved with the Australian government's rival offer to build the cable, paying two-thirds of the cost itself—after it suggested it would not allow Huawei to land a cable connection in Australia. According to journalist John Kehoe, writing in the *AFR* on 16 January, Warner was "instrumental in convincing the Coalition government" to take this road. Like Irving, Warner has specialised in the Pacific region. His near 20-year stint at the Department of Foreign Affairs and Trade (DFAT) included roles as High Commissioner to PNG, First Assistant Secretary for the South Pacific, and Special Coordinator of the Regional Assistance Mission to Solomon Islands (RAMSI). He also served as Secretary of the Department of Defence (2006-09) and was head of ASIS (2009-17).

China's National Intelligence Law

Author of the *AFR* article about the FIRB policy shift,

Angus Grigg, backed up his story with comments from Danielle Cave and Tom Uren of the anti-China Australian Strategic Policy Institute (ASPI), who assert that Beijing's National Intelligence Law, passed in June 2017 and amended in April 2018, makes Chinese companies beholden to the state. Article 7 of the laws states: "An organisation or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows."

This puts in black and white "what intelligence agencies around the world have long known, but struggled to articulate to parliaments or government departments", the pair told *AFR*. China's President Xi Jinping is, according to Grigg, using the private sector "to help fulfil the country's larger strategic and economic goals".

Unmentioned is that the Five Eyes uses exactly the same technique to achieve its strategic and economic goals, and it pioneered the method. In fact, responding to the 1 December 2018 arrest of Huawei Deputy Chair and Chief Financial Officer, Meng Wanzhou, China's Ambassador to Canada Lu Shaye revealed in an article for Ottawa's *Hill Times* that "When making laws for national security and

The secret plans of Five Eyes

• Reuters revealed in a 12 October 2018 article, "Exclusive: Five Eyes intelligence alliance builds coalition to counter China", that the Five Eyes alliance has been working with like-minded partners, including Germany and Japan, to expand a "broadening international front against Chinese influence operations and investments". Consultations on the topic "have been frequent and are gathering momentum", according to a US official cited in the piece. Several officials in four capitals spoke to Reuters. Another said the talks were taking place "below the radar", mainly in bilateral formats, and have included heads of government, diplomats and intelligence chiefs. The article stated that the Five Eyes summit in August 2018 in Queensland (below) had hinted at closer coordination and "global partnerships".

• A 13 December *Australian Financial Review* article, "Secret meeting led to the international effort to stop China's cyber espionage" by Chris Uhlmann and Angus Grigg, revealed details of Five Eyes meetings in Ottawa and Nova Scotia, Canada, in July 2018. "In the months that followed that July 17 dinner an unprecedented campaign has been waged by those present—Australia, the US, Canada, New Zealand and the UK—to block Chinese tech giant Huawei from supplying equipment for their next-generation wireless networks", reported the article. This culminated in the arrest of Huawei chief Meng, the authors went on. Allies like Japan and Germany were to be included in the effort.

Following the gathering, *AFR* continued, top spy chiefs made a series of rare public addresses about locking out Huawei from 5G. After Australian PM Malcolm Turnbull made a mid-August 2018 phone call to US President Trump to tell him Australia would exclude Huawei and ZTE from 5G development, Director-General of the Australian Signals Directorate (ASD) Mike Burgess became the first in his position to give a public speech regarding 5G on 29 October. Duncan Lewis (ASIO head) and Paul Symon (ASIS head) were there supporting him—all had been at the Canada meetings. New Zealand announced its ban on Huawei seven days after the Burgess speech; then on 6 December Canadian Security Intelligence Service head David Vigneault made his first public speech on the threat—like all the rest he didn't mention Huawei by name. The following day, MI6 boss Alex Younger gave a rare speech on the same topic. Later that day British telco BT Group announced it would not use Huawei technology in its 5G network. But a private British company would never be influenced by a state-directed intelligence organisation, right?

• Australian Home Affairs Secretary Michael Pezzullo spilled the beans prior to the Five Country Ministerial meeting (Five Eyes) held 28-29 August 2018 on the Gold Coast, that the Five Eyes countries were pushing for a global police-state capability, with a "transnational model of security". ("Five Eyes plan global police state", *AAS* 22 Aug. 2018)

Pezzullo laid out the Five Eyes plan in two speeches in Washington, DC in June and in Canberra in July in the lead-up to the otherwise top-secret forum. We "need to *re-think the paradigm that domestic security and law enforcement can be exclusively executed within national jurisdictions*", he said. (Emphasis in original.) Up until now this was "the prevailing paradigm", he said, "and understandably so in a world of nation states; the world that emerged in that same 17th century after the Peace of Westphalia." The transformation of the state itself would be required, he contended, as the world moved towards a global security model—obviously under the direction of the Five Eyes.

• At the Commonwealth Heads of Government Meeting (CHOGM) in London on 19-20 April 2018, PM Turnbull had signed Australia up to a new cyber security pact forged by the 53 member nations, extending the collaborative relationship between the Five Eyes (four of which are Commonwealth countries) into a broader network. On the sidelines of the meeting, Australia and the UK signed up to a new joint strategy to work together at the operational level to target cyber crime, piloting "new tactics, techniques and capabilities" and coordinating "global responses" to attacks. With the UK negotiating its exit from the European Union, the Commonwealth has been recognised as a crucial conduit of British influence across the globe, via its "Global Britain" plan. ("'Global Britain': an attempt to retain power as global balance is disrupted", *AAS* 16 January 2019)

• The *National Security Legislation Amendment (Espionage and Foreign Interference) Act* 2018, which passed the federal parliament on 28 June, established an unprecedented state-secrecy regime smothering freedom of speech, association and political communication, in the name of curbing so-called foreign influence. ("Resistance builds to Turnbull's totalitarian 'national security' laws", *AAS* 7 Feb. 2018; "Officials warn 'foreign influence' laws undermine parliamentary privilege", *AAS* 4 Apr. 2018) It was actually part of a globally coordinated campaign aimed at outlawing China's desire for international cooperation. London's *Financial Times* revealed on 27 June 2018, in "Australia leads 'Five Eyes' charge against foreign interference", that the push for foreign interference laws was occurring under the Five Eyes umbrella.

intelligence, China has drawn references from the relevant laws of the USA, Canada, and other Western countries. Something is considered as 'safeguarding national security' when it is done by Western countries. But it is termed 'conducting espionage' when done by China. What's the logic?"

Lu referenced the "PRISM program, Equation Group and Echelon-global spying networks ... engaging in large-scale and organised cyber stealing, and spying and surveillance activities on foreign governments, enterprises, and individuals." In addition, he said, the Five Eyes nations have pushed for all of the private businesses in their nations to ban rival Huawei equipment, "which is literally a government controlled action".

THE HILL TIMES | WEDNESDAY, JANUARY 9, 2019

11

Comment

Why the double standard on justice for Canadians, Chinese?

It seems that, to some people, only Canadian citizens should be treated in a humanitarian manner and their freedom deemed valuable, while Chinese people do not deserve that.

Lu Shaye

Meng Wanzhou

Recently, China's competent authorities took compulsory measures in accordance with the law against two Canadian nationals who are suspected of engaging in activities that endanger China's national security. Some Canadians and some in the Canadian news media, in disregard of China's judicial sovereignty, accused China of arbitrary detention and demanded their immediate release.

However, on the prior ground less detention of Chinese citizen Meng Wanzhou by Canada at the behest of the United States, these same people made utterly different comments. They insisted that Canada's detention of a Chinese citizen who was transferring planes at the airport was "acting in accordance with law," though Meng has not been charged with any violation of Canadian law.

It's understandable that these Canadians are concerned about their own citizens. But have they shown any concern or sympathy for Meng after she was illegally detained and deprived of freedom?

Without violating any Canadian law, Meng was arrested last month and put in handcuffs just as she was changing planes at the Vancouver International Airport. It seems that, to some people, only Canadian citizens shall be treated in a humanitarian manner and their freedom deemed valuable, while Chinese people do not deserve that.

When China called on the Canadian side to release Meng and ensure her legal and legitimate rights and interests, those elites claimed in the media that Canada is a country of rule of law and has an independent judiciary, and therefore it must comply with the judicial proceeding. However, in the case of detention of Canadian citizens in China who violated China's law, those elites ostentatiously dismissed China's law and presumptuously urged China to immediately release their citizens. It seems that, to those people, the laws of Canada or other Western countries are laws and must be observed, while China's laws are not and shouldn't be respected.

Something is considered as 'safeguarding national security' when it is done by Western countries. But it is termed 'conducting espionage' when done by China. What's the logic?

Some people in Canada, without any evidence, have been hyping the idea that Huawei is controlled by the Chinese government and poses security threats to Canada and other Western countries, and that Chinese law requires China's enterprises to collaborate with the government in espionage activities. However, these same people have conveniently ignored the PRISM Program, Equation Group, and Echelon—global spying networks operated by some countries that have been engaging in large-scale and organized cyber stealing, and spying and surveillance activities on foreign governments, enterprises, and individuals. These people also took a laissez-faire attitude toward a country that infringes on its citizens' privacy rights through the Patriot Act. They shouted for a ban by the Five Eyes alliance countries (Australia, Canada, New Zealand, the United Kingdom, and the United States) on the use of Huawei equipment by these countries' own enterprises, which is literally a government-controlled action.

When making laws for national security and intelligence, China has drawn references from the relevant laws of the U.S., Canada, and other Western countries. Something is considered as "safeguarding national security" when it is done by Western countries. But it is termed "conducting espionage" when done by China. What's the logic?

Canada, pulling a few individual countries such as the U.S. and the U.K. on its side, pressed China in the name of "the international community" to release its citizens. Do a handful of Western countries really represent the whole international community? To those would-be representatives of the international community, non-Western countries are not members of the international community and only their countries can call the shots on international affairs.

I have recently heard a word repeatedly pronounced by some Canadians: bullying. They said that by arresting two Canadian citizens as retaliation for Canada's detention of Meng, China was bullying Canada. To those people, China's self-defence is an offence to Canada. If someone slaps you on your left cheek, give him your right cheek, they told us. But I have never seen them doing as they said.

Huawei chief financial officer Meng Wanzhou, pictured at a 2014 investment forum in Russia, was arrested at the Vancouver International Airport last month and is awaiting potential extradition to the United States. *Photograph courtesy of the Kremlin*

The reason why some people are used to arrogantly adopting double standards is due to Western egotism and white supremacy. In such a context, the rule of law is nothing but a tool for their political ends and a fig leaf for their practising hegemony in the international arena. What they have been doing is not showing respect for the rule of law, but mocking and trampling the rule of law.

Lu Shaye is the Chinese ambassador to Canada.

The Hill Times

Chinese Ambassador to Canada Lu Shaye's article in the *Hill Times*; Huawei Deputy Chair Meng Wanzhou.
Photos: Chinese Embassy Canada; AFP/Eyepress News

One of the most explicit efforts to allow governments to co-opt their citizens to spy was Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, a.k.a. the encryption bill, which became law on 6 December 2018. The details almost put the Chinese law to shame! Intelligence agencies can compel any citizen or company to act on their behalf, whether by hacking, re-engineering apps or programs, or simply unlocking a mobile phone, to allow unprecedented covert and overt access to data. The order would remain secret, and not only does the person co-opted to the task have to keep it secret, the penalty for disclosing it is five years' imprisonment. Should someone refuse to comply with an order, they can be jailed for 5-10 years! ("Home Affairs encryption bill: A political tool made in Britain", *AAS* 5 Sept. 2018; "Don't let the Five Eyes spy on you!", *AAS* 3 Oct. 2018)

The bill is a copy of a 2016 UK law known as the "Snoopers' Charter". The UK version even mandates that companies take reasonable steps to develop and maintain a capability to respond to security agency requests, and allows companies to violate existing laws to comply with them.

Concerns about government back doors into communications systems thus no longer exclusively applies to firms like Huawei. Leading Australian cyber security and technology experts have slammed the encryption law for tainting Australian vendors with the same questions alleged of Huawei.

Another mechanism used by the Five Eyes is the supply of disinformation to the media. In Australia it is common knowledge that our intelligence agencies feed material to the media to create a suitable climate for incubating desired policies. Former 4 Corners executive producer Peter Manning told the University of Technology Sydney's Australia-China Relations Institute (ACRI) conference on 12 November 2018 that it is common practice for media to use intelligence agencies as sources, so what we end up with in our press is the "line" they want put out. "I wish [the media] would go to the experts, rather than the loudest voices" such as ASPI, observed ACRI Deputy Director Prof. James Laurenceson at the same conference. Former Whitlam and Fraser government official John Menadue has said ASIO is pretty much running our China foreign policy, briefing journalists regularly on the "China threat". This activity has the same imprimatur as the Integrity Initiative, another project under the purview of the Five Eyes (Washington Insider, p. 12).

FVEY cartel to exclude rivals?

There is no solid evidence of Huawei engaging in espionage, but unsurprisingly there *is* evidence of espionage being committed against it by the USA. According to documents released by whistle-blower Edward Snowden in his 2013 exposure of the National Security Agency's (NSA) extensive global surveillance operations, the NSA had successfully hacked Huawei back then, accessing even the source codes of Huawei products. One NSA document admitted it was for the purpose of advancing US spying capabilities, saying that "many of our targets communicate over Huawei produced products, we want to make sure that we know how to exploit these products". The NSA admitted spying on former Chinese President Hu Jintao, the Chinese Trade Ministry, banks and private companies.[1]

The question of who is really conducting intellectual property theft is squarely raised by this information, particularly given that Huawei is far in advance of its competitors in developing 5G telecommunications technology, from which the Five Eyes (sometimes shortened to FVEY) is now trying to exclude it. Huawei is projecting deliveries of new hardware at least nine months ahead of any competitors at less than half the price.

Mainstream media has widely reported that the Five Eyes has taken the lead in banning Huawei from construction of 5G network infrastructure. The USA in particular has pushed its allies, beyond just the Five Eyes network, to do so. Australia and New Zealand led the way with a ban, and while the UK, Canada, Japan, France, Germany and others are reportedly in agreement, actual bans are still pending. Head of the Canadian Security Intelligence Service spy agency from 2009 to 2013, Richard Fadden, called for Huawei to be banned from Canada's 5G network on 22 January. As for the USA, it has restricted technology transfers to China and prevented Chinese investment in US tech companies, and the Congress is now considering expanding the reach of those laws. US President Donald Trump is also reportedly considering issuing an executive order that would ban US purchases of products manufactured by Huawei and the smaller ZTE Corporation.

1. "NSA Spied on Chinese Government and Networking Firm", Spiegel Online 22 Mar. 2014; "NSA Breached Chinese Servers Seen as Security Threat", *New York Times*, 23 Mar. 2014