Understanding China's Threat to Australia's National Security

Speech to *Confronting and Countering the Threats from Espionage, Foreign Interference and Terrorism*, 16th National Security Annual Summit, Canberra, 8 May 2019

Clive Hamilton[1]

As long at the Communist Party rules China it will pose a persistent and serious threat to Australia's national security. Over the last two years we have made considerable progress in setting up defences against Beijing's subversion and covert influence. But we have only just begun a decade-long project, at least, of undoing the influence networks that the CCP has already established.

Momentum is being slowed by institutional inertia, and Beijing has mobilized its "friends of China" among Australia's elites to push back, including attempts to erode public confidence in our intelligence agencies.

Beijing is exploiting our democratic processes, our legal system, and our free press. It's also exploiting multiculturalism as a cover for its influence activities. The accusation of Sinophobia or anti-Chinese prejudice is a powerful silencing device. Those whose voices have been most quieted are of course Chinese-Australians who want to speak out for human rights in China, or against the injustices in Tibet and Xinjiang.

We are only now becoming aware that Beijing's interference in our political system goes well beyond the activities of wealthy, Party-linked donors. In recent years, the Chinese Communist Party, through its global United Front network, has been actively encouraging trusted members of Chinese communities in countries like Australia to become directly involved in running

[1] Professor of public ethics, Charles Sturt University, Canberra.

for political office, a policy known as *huaren canzheng* (pronounced "hua wren t's-an jung").

The policy, literally meaning "ethnic Chinese political participation," also involves mobilising overseas Chinese community organisations to "form one unified voice," and supporting mainstream candidates who have a "correct understanding of Chinese people and China."

Political organizations with names like the Chinese Labor Association and the Chinese Liberal Club are now operating inside Australia's two main political parties. Some members of them are using their growing influence to promote Beijing's interests. This approach is related to the "mixing sand" (*chan shazi*) tactic advocated by Mao Zedong, that is, planting trusted people in the enemy's ranks in order to weaken them.

Unlike Russia, which carried out an ambitious campaign of interference intended to benefit Donald Trump in the 2016 U.S. presidential election, the CCP is bipartisan in its activities in Australia. It aims to build influence across the political spectrum, and be able to sway whomever wins.

Huaren canzheng has been actively promoted by Huang Xiangmo, the real estate mogul and political donor who in February was excluded from Australia because of ASIO's concerns about his CCP links. When in 2015 he was president of the Australian Council for the Promotion of Peaceful Reunification of China, the core United Front organisation, Huang wrote an article titled "On the new age of *huaren canzheng*". It's vital, he wrote, to rally ethnic Chinese forces to use their ballots, make political donations and master the rules of the political game.

In recent years, United Front groups in Australia have been holding training seminars to encourage trusted Chinese-Australians to participate in politics.

They're aimed particularly at young Chinese-Australians who are more integrated into Australian society. Huang Xiangmo wrote of the need to nurture those with bilingual skills "who can walk through the revolving door of politics, business and academia with ease."

In addition, for some years CCP agencies have been organizing so-called Discovery Trips to China for overseas Chinese.[2] There they meet senior Chinese government leaders, listen to speeches given by experts, attend discussion forums and build networks. This program is part of the CCP's broader *qiaowu* program, which CCP expert James Jiann Hua To describes as a massive operation aimed at co-opting overseas Chinese and "managing their behaviour and perceptions through incentives or disincentives to suit the situation and structural circumstances that the CCP desires."

In short, both the training seminars in Australia and the Discovery Trips to China are elements of a CCP program designed to groom young Chinese-Australians to serve the interests of the Party-state.

Some candidates currently standing for election to federal parliament have participated in these training programs and the Discovery Trips to China. They also have close links with United Front organisations and influential figures from the Chinese diaspora who act on behalf of the Chinese Communist Party.

Over the last 18 months, some 15 federal politicians have been disqualified because of their dual citizenship. They fell afoul of Section 44 of the Constitution, which rules ineligible anyone who is a citizen of another country. Now the parties are doing their due diligence by forensically checking each potential candidate for dual citizenship.

[2] The trips are organised by the Overseas Chinese Affairs Office and China Overseas Exchange Association, both agencies of the Chinese Communist Party's United Front Work Department (UFWD), a powerful branch of the CCP tasked with influencing and controlling groups outside the party, including groups located abroad.

But the same clause of Section 44 also disqualifies any person who "is under any acknowledgment of allegiance, obedience, or adherence to a foreign power." The political parties ought to be doing their due diligence to rule out any potential candidates who are engaged in United Front activity. As the CCP's *huaren canzheng* policy begins to bear fruit federally, as it already has done in state parliaments and local councils, sooner or later I expect to see an MP challenged in the High Court.

We know that ASIO is gathering more detailed information on Beijing's attempts to co-opt Chinese-Australians and has expressed concern about CCP-linked individuals entering parliaments. (In Canada, where the process of penetration has gone further, CSIS has done likewise, although its warnings have been dismissed by a compromised political class.)

Such a High Court challenge would be disastrous for future representation of the Chinese-Australian community in federal parliament, so the parties must start thinking much more carefully about this problem. It should be stressed that Chinese-Australians are under-represented in Australian political office and more should be encouraged to enter politics, but not if they are liable to be disqualified under Section 44.

***

Our intelligence and law enforcement authorities have, by all accounts, been highly effective at identifying and arresting actual and potential terrorists. By contrast, they have been reluctant to prosecute individuals engaged in economic espionage and spying. In recent years, the United States has launched a series of high-profile prosecutions of Chinese spies and agents of influence who have engaged in unlawful activity. Even Canada, which is more in thrall to Beijing than Australia, has put spies before the courts.

Yet in Australia there have been none. This is not for want of malign activity, as recent ASIO reports have made clear, but for lack of political will. Fear of Beijing's ire is allowing its program of data theft, information gathering and cyber-hacking to proliferate.

And with the passage last year of the Espionage and Foreign Interference Act there is a new crime to tackle. Foreign interference is a crime if it involves activity that is covert, directed or funded by a foreign principal, and "is intended to influence a political or governmental process or the exercise of a democratic or political right …". Such activity has been rampant in Australia, as a reading of my book will reveal.

State police forces have, or ought to have, a large share of the responsibility for uncovering and prosecuting individuals engaged in unlawful foreign interference. Most of it takes place at a local level. Yet state police forces have not committed the resources to understanding the nature and extent of foreign interference that is taking place in their backyards.

Admittedly, it's a daunting task. They must first develop a comprehensive map of United Front actors and organisations, and then work out what kind of activity might be unlawful. It means penetrating a world that is opaque and unfamiliar. The *modus operandi* of the CCP is like nothing we have experienced before; certainly the old rules of the Cold War are not of much use, and viewing it through a le Carré lens only obscures things. Fortunately, there are members of the Chinese-Australian community very willing to help.

But there is another strong reason for state police forces to put themselves at the forefront of investigating foreign interference. Just as the Kremlin uses criminal gangs to carry out some of its work, and oligarchs have business partnerships with organised crime bosses, there has always been a nexus between the Chinese Communist Party's overseas influence activities and criminal gangs.

In Canada, the media has exposed evidence of enormous sums of dark money from China being laundered through Vancouver casinos and real estate. Some of the criminals have political links, both in China and in Canada. The provincial and federal governments have been reluctant to face up to the problem and do something about it. The reasons are complex: it looks overwhelming, the crooks have friends in high places, the crippling fear of accusations of xenophobia, and billions of dollars flowing into government coffers from gambling.

I am asking myself whether Australia is in the same boat, ignoring major crimes that are mixed up in political influence activity?

FBI Director Christopher Wray recently commented on another aspect of the merging of crime and politics. He said the FBI is focusing on what he called "a blended threat where cybercrime and espionage merge together in all kinds of new ways." He described how China, above all, poses a severe intelligence threat because it's stealing U.S. assets like advanced technology and commercial innovations, and collecting information for political use.

And then he said something that we in Australia are reluctant to admit.

> "China [by which he meant the CCP] has pioneered a societal approach to stealing innovation in any way it can from a wide array of businesses, universities and organizations. They're doing it through Chinese intelligence services, through state-owned enterprises, through ostensibly private companies, through graduate students and researchers, through a variety of actors all working on behalf of China."

The term "blended threat" refers to nation states using criminal hackers; but here I am describing something slightly different, criminals becoming agents of influence for nation states, and nation states willingly using them.

All of this is being played out in Australia too; yet we do not want to admit it, for fear of being accused of racial profiling or because of our anxieties about annoying Beijing. ASIO has a good idea of the landscape, and has been writing about it in recent annual reports. The Director-General Duncan Lewis put it succinctly when he wrote that "foreign actors" are aggressively seeking access to privileged and classified information on Australia's alliances, on our diplomatic, technological, economic and military secrets and on our energy and mineral resources. These foreign actors, he wrote:

> are also attempting to clandestinely influence the opinions of members of the Australian public and media, Australian Government officials, and members of Australia-based diaspora communities.

Yet the Director-General would not name China as the party overwhelmingly responsible for this subversion and espionage. In fact, China is not mentioned once in ASIO's report. Russia is, several times; even earning an index entry "Russian intelligence activity in Australia." There's no entry for China even though China's intelligence activity is a hundred-fold greater.

This is exactly how Beijing wants it: a thorough program of espionage and subversion that we are too afraid to talk about.

The same coyness was on display in February when it was revealed that a "sophisticated state actor" had hacked into the computer systems of both of our main political parties. The government would not reveal the source of the attack, although it knew it was China. Again, the government was intimidated into silence by Beijing. The message we are sending is that if you do it again we will not call you out.

The contrast with the United States could not be sharper. There, in addition to forthright statements from the FBI and the CIA directors, the US-China

Economic and Security Review Commission recently issued a report to Congress describing China's subversive activities, as far as they are known. A bill is moving through Congress that would legislate for an annual report detailing China's interference activities.

***

Sunlight is the best disinfectant against Beijing's covert, coercive and corrupt activities in Australia. Yet, the Australian government is keeping us in the dark, leaving the task of pulling back the curtains to a handful of journalists and academics, who must then take the blowback. The best source of information on Beijing's activities is of course the Chinese-Australian community itself. They do much more than we know; yet they live in fear of material retribution from the CCP and its agents. And, it's sad to say, they don't believe that the Australian government will adequately protect them.

If we are to prevail in this new era of political warfare, to use the CCP's term, a whole-of-society threat requires a whole-of-society response; but that cannot happen if the public is kept in the dark. At the moment, the government is signalling that there is a serious threat to our sovereignty and our democratic system. Yet it seems to be saying "leave it to us, we will take care of it."

Even a determined government cannot respond adequately to this new kind of threat. U.S. authorities are further down the track. They have been engaged in a major outreach exercise to American companies and universities, to explain the nature of the risks they face from China's network of influence and technology theft.

Something like this has been taking place in Australia on a smaller and more tentative scale, but so much more needs to be done. It's clear that our universities, in particular, are resistant to hearing the message and continue to

expose themselves to a range of risks. For example, some Australian universities have entered into partnerships with Chinese companies and universities that are likely steal their intellectual property.

The universities claim they do due diligence on the Chinese companies they partner with. But the companies they pay to carry out due diligence do not know what to look for or how to look. Work by Alex Joske has exposed many instances of Australian universities happily hosting Chinese scientists who turn out to be officers of the People's Liberation Army specialising in weapons research and other military-related research.

Not only are universities unaware but, when it's pointed out, some don't appear to be unduly worried. To borrow a metaphor from one authority on the CCP (Frank Dikötter), they are like Boy Scouts up against Don Corleone.

In the cyber domain, I think the public, along with government organizations and private companies, have been persuaded that they need to do more to protect their information from cyber attackers, including sophisticated state actors. But it's a mistake to think that all they need to do is harden their perimeter defences against outside threats. Possibly the greater threat comes from within, insider threats, or "malicious insiders" as ASIO has called them. As you know, all it takes is for someone with access to a computer network to stick into a port a USB that then downloads malware.

It would be incorrect to think that the risk is from MSS moles being sent in. That's le Carré thinking. Far more likely is an employee who comes under great pressure to engage in malicious activity. It's a much harder problem to respond to sensitively, but the starting point is to frame it correctly, and that is that most Chinese-Australians are the victims here.

Lastly, building on its almost total domination of Chinese-language media in Australia, Beijing has weaponised Chinese-language social media. WeChat is used heavily by most Chinese-Australians. Many rely on it as their main source of news and opinion. Now, accounts are being doctored and fake news stories are being spread to shape opinions in electorates with large diaspora populations.

WeChat is owned by Chinese conglomerate Tencent, which is controlled by Ma Huateng (Pony Ma), China's richest man and a firm supporter of the Party. WeChat cannot be regulated by Australian authorities, but it is subject to censorship in Beijing. This means that Australian politicians using WeChat to communicate with voters are censoring themselves, or rather their Mandarin-speaking staff members censor their posts so as not to attract the attention of Beijing's censors.

The Labor Party has written to Tencent to complain about fake news stories on WeChat. WeChat is not subject to pressure like Facebook or Twitter, so it's a futile exercise, if a necessary one. I would urge those politicians to challenge the censors by sending out posts condemning the outrages in Xinjiang or praising the Dalai Lama, as a way of standing up for free speech in Australia. Beyond that, we must come up with innovative responses to Beijing's exploitation of free speech.

My essential message then is that we are faced with a new kind of adversary that practices espionage and political interference in ways that are alien to us as experts. They are practices that subtly exploit the openness of our institutions and the boundaries we place around them. They operate in the grey zone. We are being forced to take a crash course in a new world of *huaren canzheng*, citizen spies and blended threats. To respond will require great flexibility in the way we think and a willingness to adapt our institutions.