Australian National University

February 2022

Public Submission - Review of Administration and Expenditure No. 20 (2020–21) – Australian Intelligence Agencies - Issues Affecting Long Term Strategies

Submission made on behalf of
Dr. William A. Stoltz, Senior Adviser for Public Policy, ANU National Security College
Mr. Sam Williamson, Research Assistant, ANU National Security College

Introduction

The authors would like to thank the Committee for the opportunity to make this submission to this important inquiry. For the avoidance of doubt, the views conveyed in this submission are those of the authors alone and should not be taken to represent an institutional position on behalf of the National Security College, nor the Australian National University.

This submission specifically relates to the Committee's interest in "shifting operational priorities from emerging threats that alter the longer term strategies" that guide Australia's intelligence agencies.[1] In particular this submission seeks to highlight two high-level trends that are likely to reshape the strategic priorities and operations of Australia's intelligence agencies. These are:

- The likely increase in demand for intelligence agencies to undertake and support covert action outside of Australian Defence Force (ADF) operations and in response to increasing interference operations by the People's Republic of China (PRC) in Australia's region; and
- The creation of a less-permissive operating environment for foreign intelligence collection across the threat landscape as a result of the convergence of disruptive technologies.

The authors assess that these trends will challenge future Australian governments to either:

- accept a higher degree of strategic and operational risk in relation to agencies' activities, or
- force an downwards adjustment in expectations of what agencies can feasibly achieve within existing resources and operational postures.

Should the Australian government continue to expect the same or greater operational results from Australia's intelligence community, not only will greater funding likely be required to incorporate new technologies, but historic relationships with the private sector and the Australian public will need to evolve quickly.

[1] Parliament House, 'Review of Administration and Expenditure No. 20 (2020–21) – Australian Intelligence Agencies' 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AandENo20.

Thank you for the opportunity and for the time taken by the Committee and the Secretariat team to consider this submission.

Should it benefit the Committee's consideration of this submission, the authors would be happy to participate in any subsequent hearings the Committee may wish to have.

Sincerely,

Dr. William A. Stoltz
Senior Adviser for Public Policy
National Security College, ANU

Mr. Sam Williamson
Research Assistant
National Security College, ANU

Covert Action

Precipitous great-power competition between the People's Republic of China (PRC) and the United States unfortunately makes the forecast for the Indo-Pacific's foreseeable strategic future cold and grey. Cold because the balance of power in the region between authoritarian and liberal-aligned states looks set to be determined by a 'cold war' led by the United States and China respectively. And grey, because the skirmishes of this cold war appear likely to play out in a so-called 'grey zone' not so much characterised by the state-sponsored insurgencies and proxy-wars of the Cold War of yesteryear, but rather in even greyer arenas of competition: international commerce, technology research, and the internet-enabled global information domain. **The implication of this competition for Australia's intelligence community is a likely increase in demand for agencies to support covert action operations, namely as a means of response to the PRC's subversive tactics.**

The PRC has long embraced grey zone options as a means to bridge apparent limitations in its military and diplomatic capabilities, however China's methods of clandestine interference are becoming sharper and less restrained by previous desires to be regarded as a friendly actor amongst the states it targets. Since approximately 2017, the PRC has embarked upon an ever more disruptive campaign of subversive 'active measures' with a particular focus on small and developing states across the Indo-Pacific as the frontier of great-power competition with the United States. This campaign is impacting upon Western countries' access and influence in South East Asia and the Pacific, especially for Australia and the United States.[2]

US allies like Australia and other Five Eyes countries, have historically benefitted from America's comparatively expansive use of covert statecraft, meaning they themselves have not needed to sustain as comprehensive, and risky, covert action programs. However, the PRC's well-resourced, persistent and unscrupulous campaign of influence and subterfuge will require an allied response, and one in which the US may need to play "deputy sheriff" to its allies, as Kurt Campbell has explained.[3]

A recent report by Paul Charon and Jean-Baptiste Jeangène Vilmer of the Institute for Strategic Research outlines in detail how the PRC's approach to influence operations is undergoing a 'Machiavellian moment' where Beijing has decided it is better – or at least easier – "to be feared than

[2] P. Charon and J.-B. Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', (Institute for Strategic Research (IRSEM), October 2021), https://www.irsem.fr/report.html.
[3] David Brunnstrom and Kirsty Needham, 'Pacific May Be Most Likely to See "strategic Surprise" -U.S. Policymaker Campbell', *Reuters*, January 2022, https://www.reuters.com/world/asia-pacific/us-most-likely-see-strategic-surprise-pacific-official-2022-01-10/.

loved."[4] Operationally, they suggest China's posture is undergoing a 'Russification' whereby the PRC's methods of influencing are increasingly emulating Soviet-style covert action with an emphasis on:

> "disinformation, counterfeiting, sabotage, discredit operations, destabilizing foreign governments, provocations, false-flag operations and manipulation aimed at weakening social cohesion, the recruitment of "useful idiots," and the creation of front organizations."[5]

As one publication explains from the National University of Defense Technology (an institute of the CCP's Central Military Commission) the ultimate objective of the PRC's active measures is to:

> "manipulate a country's values, national spirit/ethos, ideologies, cultural traditions, historical beliefs, etc. to encourage them to abandon their theoretical understanding, social system, and development path and hence to achieve strategic objectives without fighting." [6]

As the PRC's activities are taking place in third countries, they are difficult for Western states to directly or swiftly address with 'overt' tools of military or diplomatic statecraft. This is especially the case for Australia which is observing heightened interference by the PRC in neighbouring South Pacific countries.[7] Enduring PRC methods of so-called debt-trap-diplomacy[8] and diplomatic pressuring[9] are being complemented by information operations, elite capture and corruption,[10] and an expanded deployment of Chinese security forces. Pacific leaders are worried that their sovereignty is now "sandwiched" by PRC behaviour in the region which they recognise as motivated by "superpower rivalry".[11]

Long term military and economic investments to bolster Western power in the Indo-Pacific will doubtless eventually prove valuable in countering Chinese influence. But the facts of foreseeable strategic circumstances will likely demand the considered use of covert action by liberal middle

[4] P. Charon and J.-B. Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', 15.
[5] P. Charon and J.-B. Jeangène Vilmer, 34.
[6] 黄昆仑 (Huang Kunlun), "夺取未来战争 制脑权" ("Seizing Mind Superiority in Future Wars"), 解放军报 (PLA Daily) (16 Jun. 2014). Cited in P. Charon and J.-B. Jeangène Vilmer, 31.
[7] Jonathan Pryke, 'The Risks of China's Ambitions in the South Pacific', *Brookings* (blog), 20 July 2020, https://www.brookings.edu/articles/the-risks-of-chinas-ambitions-in-the-south-pacific/.
[8] Roland Rajah, Alexandre Dayant, and Jonathan Pryke, 'Ocean of Debt? Belt and Road and Debt Diplomacy in the Pacific', n.d., https://www.lowyinstitute.org/publications/ocean-debt-belt-and-road-and-debt-diplomacy-pacific.
[9] Barbara Dreaver, 'Fears over China's Involvement in Kiribati's Ditching of Marine Reserve', 1 News, n.d., https://www.1news.co.nz/2021/11/11/fears-over-chinas-involvement-in-kiribatis-ditching-of-marine-reserve/.
[10] Pryke, 'The Risks of China's Ambitions in the South Pacific'.
[11] Mar-Vic Cagurangan- For Variety, 'In the Shadow of Geopolitical Conflicts: How China Triggers Domestic Division in Pacific Island Nations', Marianas Variety News & Views, January 2022, https://mvariety.com/news/in-the-shadow-of-geopolitical-conflicts-how-china-triggers-domestic-division-in-pacific-island-nations/article_57445b06-7225-11ec-9191-3bb2a1c961b1.html.

powers, including Australia, as a means of response, but also to supplement other statecraft in proactively shaping the political, cultural, and economic behaviour of those foreign countries at the forefront of the contest for the Indo-Pacific. This is because **to rapidly mobilise effective responses to the PRC's current subversive activities requires undertaking in-kind measures to counter China on the same plain of covert and unacknowledged activity that they themselves are seeking to 'win without fighting'.**

An Expanded Covert Action Posture

Based on the differing legal and policy permissibility of covert action over the years Australia's approach to covert action has been characterised by three distinct eras:

- the 1950s to the 1970s in which covert action supported allied propaganda, paramilitary and counter-insurgency programs;
- 1985 to 2001 in which covert action was confined to Australian Defence Force-led operations; and
- 2001 to the present in which covert action outside of ADF special operations has primarily focused on the task of disrupting active national security threats, with the main agencies for this activity being ASIS and the cyber-focused Australian Signals Directorate.

As such, for the past twenty years Australia's approach to covert action has been calibrated to focus on disruption of national threats, often undertaken in support of otherwise declared military operations, with examples including counter-terrorism activities, interference with people smuggling, and the recovery of hostages.[12] This focus on disruption has meant that so-called 'special operations', and more recently 'offensive cyber operations', have been the dominant forms of covert action undertaken by the Commonwealth in recent times. As described, current and emerging strategic trends will likely force a historic shift in this otherwise limited and restrained covert action posture.

To counteract the impact of the PRC's unrestrained interference in third countries, Australia and other Five Eyes nations will likely need to undertake covert actions that include:

- information campaigns to promote favourable messages and discredit pro-Chinese Communist Party (CCP) actors;
- providing financial and other support to political candidates and organisations who are anti-CCP and pro-democratic; and

[12] Australian Strategic Policy Institute, 'The ASIS Interviews', accessed 27 January 2022, https://www.aspi.org.au/report/asis-interviews.

- sabotaging the PRC's interference operations, including via digital and economic means.

In addition to being a means of response to the PRC's influence operations, covert action will likely also have a wider utility to Western nations as a means to avoid escalation to military conflict with the PRC and other aggressive states. High-end modern warfare between peer-adversaries, especially between nuclear-armed states like the United States and China, is highly undesirable not least of all because from a strategic point of view the outcome of such warfare is increasingly difficult to predict. **The integration of new technologies and the opening up of new warfighting domains - cyber and space - means that many countries, large and small, now possess militaries capable of unprecedented and therefore somewhat unknown levels of violence and disruption.** Just as the newly industrialised militaries of Europe couldn't entirely anticipate the scale of mechanised violence wrought by the Great War, strategists today are conscious that it is difficult to fully comprehend the speed, escalation, and violence of any future high-end conflict. Given this, covert action as a means to shape facts on the ground below a threshold of violence may present favourable alternatives for states seeking to manage escalation and limit the prospects of high-end warfare between modern militaries.

While an increased demand for Australian covert measures appears to be apparent, this does not mean that such actions should be considered a complete solution in and of themselves and it will be important for agencies to manage the expectations of government as to what they can achieve. As Rory Cormac as explained in the context of the UK's approach to covert action, the utility of such measures for liberal middle powers is "as a force multiplier… a means of closing or at least concealing the growing gap between responsibilities and resources."[13] It is in this context that covert action presents additional options for Australia to shape and influence international affairs in a manner that overt capabilities might not be proportionately able to achieve. However, it needs to be emphasised that covert action, to be effective, must be strategically coordinated with other international activities[14]. In the case of successfully countering PRC influence operations the use of covert action by Australia will also need to be highly coordinated with other Five Eyes members. Indeed, any effective covert campaign in this regard will likely need to be designed and carried out as a concerted Five Eyes effort.

Amy Zegart has outlined that the Central Intelligence Agency's (CIA) extensive covert action and special operations activities have placed pressure on the analytical and intelligence collection portions

[13] Ibid, pg 3.
[14] Rory Cormac, *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy*, First edition (Oxford ; New York: Oxford University Press, 2018).

of the agency.[15] She explains that not only must the traditional intelligence segments of the CIA compete for resources and recognition, but that they also face the repurposing of collection and assessment capabilities away from addressing complex intelligence problems towards supporting covert operations. As Zegart writes, "no organisation can do it all. The more CIA people are hunting, the less they are gathering… too much attention to today's priorities leaves the nation vulnerable to nasty surprises tomorrow."[16] Similar challenges may well soon arise for Australia's intelligence community as the conditions of a persistent cold war increases demand from policymakers and politicians for agencies traditionally focused on intelligence collection to directly support and undertake a higher tempo of covert action operations. There are risks too for assessment agencies whose traditional arm's length from policymaking may be hard to maintain when they are being asked to advise on the probable success or likely outcome of alternative options for intervention in foreign targets.

Transparency with Parliament, and in particular this Committee, will be vital to ensuring any expanded approach to covert action does not create political divisions that could be damaging to the national interest. An expanded approach to covert action, perhaps akin more to that of the United Kingdom, will likely require new or reformed structures of coordination within government to ensure such activities are contestable, accountable, and aligned with wider international objectives. It will also require a careful recalibration in the public engagement activities of some intelligence agencies in order to manage public trust and understanding.

[15] In the American system, special operations conducted by the military are not regarded as covert action, while in the UK and Australian systems they are.
[16] Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton ; Oxford: Princeton University Press, 2022), 194.

Technological Disruption of Foreign Intelligence Collection

In addition to the new anticipated operational demands generated by covert action, the primary business of Australia's intelligence agencies - espionage - is being profoundly affected by technological change. The confluence of a range of new and emerging technologies is disrupting how Australian intelligence agencies undertake foreign intelligence collection. In turn, this is also affecting the business of counterintelligence. The issues presented in this submission are most pertinent to the disruption of human intelligence collection (HUMINT) and signals intelligence collection (SIGINT).

Core and longstanding elements of intelligence tradecraft are being disrupted by the rapid uptake and innovative application of new technologies. Advances in biometrics have made it significantly more difficult for HUMINT agencies to make use of assumed identifies for intelligence officers and their agents as a means to move across borders and evade detection. Such biometric innovations include the widespread use of biometric passports and visas which are linked to facial and fingerprint records; faster and cheaper DNA testing; and the increasing use of iris scanners. The integration of artificial intelligence (AI) tools with CCTV systems in public spaces can also help track and identify individuals in real-time based on indelible features such as a person's facial features, height, and gait.[17]

This will likely increase the instances in which Australia's intelligence officers abroad, namely those of ASIS, will need to operate with so-called 'deep' or unofficial cover, where instead of making use of traditional official cover, officers must make use of the cover provided by non-government affiliations or employment. Such an approach will be time consuming and may reduce intelligence officers' access to enabling government logistics and diplomatic immunities, therefore increasing risks associated with their deployment abroad.

Despite the challenges, such technologies have by no means made HUMINT collection obsolete. HUMINT activities can still yield impressive, strategically valuable results despite hostile, hard to crack adversaries, as demonstrated by the recent joint CIA-SIS effort to successfully extract a defecting Chinese rocket scientist.[18] However, for the Australian government technological disruption likely means that higher degrees of risk - to operational success and even personal safety - will need to be

[17] Aaron Holmes, 'Facial Recognition Is on the Rise, but Artificial Intelligence Is Already Being Trained to Recognise Humans in New Ways — Including Gait Detection and Heartbeat Sensors', *Business Insider Australia* (blog), October 2019, https://www.businessinsider.com.au/ai-training-beyond-facial-recognition-gait-detection-heartbeat-sensors-2019-10.
[18] Marco Giannangeli, 'Global Tensions Grow as Chinese Rocket Scientist Defects to the West', Express.co.uk, January 2022, https://www.express.co.uk/news/world/1554695/China-rocket-scientist-defects-West-MI6-global-tensions.

tolerated more often if the government-of-the-day is to expect HUMINT agencies to continue to produce valuable, actionable intelligence insights.

It is also obvious that successful HUMINT operations in a technology dense operating environment will also not be possible without close integration with and coordination with other Australian intelligence agencies. This may impact how nimble and independent individual agencies can be in undertaking operations and it will likely make the role of the Office of National Intelligence evermore critical as an intermediary that can triage the competing priorities and missions of Australia's agencies in their respective domains of foreign intelligence collection.

In the context of counterintelligence activities, for every technology that hinders Australia's foreign collection efforts, that same technology could be greatly beneficial to Australia's own efforts to fortify itself to foreign espionage. For example, a historic method of counterintelligence to identify foreign agents stealing information is to employ a “canary trap” by disseminating information that is almost entirely untouched save for small details that have been uniquely altered to allow a document and its carrier to be traced. AI can greatly aid this tactic with tools such as the WE-FORGE system – which is capable of swiftly developing at-scale information “sufficiently similar to the original to be plausible, but sufficiently different to be incorrect".[19] Tools like this, often created to protect intellectual property, will likely allow intelligence agencies to conduct broad “contact tracing” of leaked material, or to more easily disseminate false or misleading information to disrupt and hinder foreign intelligence collection efforts.[20] AI will also continue to aid intelligence analysis by helping agencies to detect connections between otherwise disparate data more effectively, a process which is increasing the value of open source data as a complementary enabler of intelligence insights otherwise supported by secret collection.

It is important to note here that, like WE-FORGE, many of the transformative technologies impacting upon intelligence collection and counterintelligence will continue to be developed by private firms or in universities for typically non-intelligence purposes. It is for this reason that the Chief of the UK's Secret Intelligence Service, Richard Moore, recently explained that his organisation and the wider UK intelligence community is in the process of reconfiguring its approach to collaborating with private firms, stating that "we cannot match the scale and resources of the global tech industry, so shouldn’t

[19] Dartmouth College, ‘Cybersecurity Researchers Build a Better “Canary Trap” – Using AI to Generate Fake Documents’, *SciTechDaily* (blog), October 2020, https://scitechdaily.com/cybersecurity-researchers-build-a-better-canary-trap-using-ai-to-generate-fake-documents/.
[20] Ibid.

try. Instead, we should seek their help".[21] Australia's own agencies will likewise have to continue to deepen their own collaboration with trusted private firms in a manner that resembles a closer collaborative partnership, rather than a limited transactional client relationship. This will be a difficult cultural change for agencies that will require continued encouragement and oversight from government. It may in time require legislative reform to clarify the extent and limitations of what intelligence activities private firms can support and how they report to government and the public about their engagement with the intelligence community.

A central challenge to effectively adopting AI is the development of sufficient data sets to train AI programs and the limited volume available of reliable, classified data. To overcome this, it will be essential that intelligence agencies cooperate to ensure such AI programs are not built on overly "siloed" data sets. In this regard, the sharing of data between Australian agencies and Five Eyes counterparts will help ensure that AI deployed for the purpose of intelligence is built on sufficiently diverse and reliable data. To train AI tools such as artificial neural networks, enormous volumes of pre-classified data are fed to the program, allowing it to perform tasks such as drawing connections between data and distinguishing one object from another in an image with (relative) accuracy.[22] In commercial applications of AI, this data is available with relatively few barriers, save for the logistical considerations of amassing such a database. This is not necessarily the case for the field of intelligence, where data sets required to train such a tool may be more difficult to obtain. Furthermore, such a data sets are excellent targets for foreign manipulation and subversion. Introducing misleading or diversionary content into an adversary's training or reference data would frustrate any intelligence collection and assessment relying on the program's output.

Other technologies that are critically impacting upon the collection of foreign intelligence include: the proliferation of encrypted communications, advances in quantum computing, and the increasingly pervasive Internet of Things (IOT). As with biotechnology and artificial intelligence, these technologies are double-edged swords for Australian agencies.

The proliferation of end-to-end encryption hinders the ease and accuracy with which communications can be intercepted and understood. Devices like bespoke encrypted handsets can also offer malicious groups closed networks for secure communications that can often only be infiltrated with the use of human sources. Of course, such technologies can also help improve the security of communications

[21] Richard Moore, 'Human Intelligence in the Digital Age - Speech by Richard Moore, Chief of the UK's Secret Intelligence Service', IISS, 2021, https://www.iiss.org/events/2021/11/human-intelligence-digital-age.
[22] Adrian Mackenzie, "The Production of Prediction: What Does Machine Learning Want?" European Journal of Cultural Studies 18, no. 4–5 (August 2015): 433. doi:.1177/1367549415577384.

for Australian agencies. This is what makes the prospects of sophisticated quantum computing a vexed issue for SIGINT agencies, because if some research initiatives continue apace encryption as we know it could be made far less uncrackable than previously thought.[23]

The ever-expanding integration of more devices and systems into the Internet of Things is similarly complicating. While the networking of more devices and systems over the internet gives SIGINT agencies more points of interception in relation to given targets, this same trend is opening up more Australian systems, including critical infrastructure, to digital infiltration and interference, as the problem of ransomware highlights. The result is more ways to surveil targets abroad and a greater array of infrastructure and critical systems needing protection at home. Understandably, this has placed pressures on both Australia's electronic surveillance regime,[24] and the Commonwealth's legal framework for protecting critical infrastructure held by the private sector.[25]

Conclusion

While this is a regularised, annual inquiry the Committee's decision on this occasion to specifically consider issues affecting the long term strategic planning of Australia's intelligence agencies is a prudent and timely one. Australia's agencies are transitioning out of an era primarily dominated by support to ADF operations in the Middle East and counter-terrorism activities. And they are moving into a new era more closely resembling the early years of the Cold War, where foreign intelligence activities became central to managing escalation, signalling deterrence, and providing vital strategic insight in times of international crisis. Meanwhile, this new era will feature rapidly disruptive technological change that will transform agencies' operations both positively and negatively.

In the years to come this Committee will exercise an indispensable function in scrutinising the suitability of Australian laws and institutions to meet this era of change. It will also have a critical role to play in demystifying for Parliament and the public what agencies are doing and the nature of their operating environment. To this end we trust that the Committee will continue to be creative and proactive in its use of inquiries such as this one as a means to inform and facilitate healthy debate.

---

[23] Cade Metz, 'Google Claims a Quantum Breakthrough That Could Change Computing', *The New York Times*, October 2019, sec. Technology, https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html.

[24] Department of Home Affairs, 'Reform of Australia's Electronic Surveillance Framework Discussion Paper', 2021, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/reform-of-australias-electronic-surveillance-framework-discussion-paper.

[25] Commonwealth Parliament, 'Security Legislation Amendment (Critical Infrastructure) Bill 2021', text, n.d., Australia, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657.

About the Authors

Dr. William A. Stoltz

Dr. Stoltz is the Senior Adviser for Public Policy at the National Security College, ANU. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.

Dr. Stoltz's own research explores options for Australia to shape and influence international security, as well as Australia's policy responses to a breadth of domestic national security challenges.

He holds a PhD and Advanced Masters of National Security Policy from the Australian National University as well as a Bachelor of Arts from the University of Melbourne.

Mr. Sam Williamson

Mr Williamson is a Research Assistant at the National Security College, ANU, with a focus on the intersection of intelligence and policy.

He holds a Bachelor of Criminal Justice from the University of Queensland and is completing his Masters of National Security Policy at the National Security College.