‘How is Research Dangerous?’: A Study of Australian Universities and Research Security Incidents

Brendan Walker-Munro[*] and Abi Young[**]

The performance of scientific and technological research has always been done openly, collaboratively and with the widest scope of international cooperation. However, recent moves by autocratic nations to exploit the standards of openness displayed by Western universities and research institutions has fuelled the emergence of ‘research security’, a domain invoking the protection of sensitive, classified or economically valuable knowledge and technologies from espionage, theft, interference and illicit transfers. Australia — once considered a ‘first mover’ by criminalising foreign interference and university espionage in 2018 — has since languished in legal and policy restrictions on research security. In some part, this is due to an unwillingness by academia to recognise that national security threats to the research enterprise are real. Therefore, this paper seeks to empirically examine live cases of research incidents from Australian institutions obtained from Freedom of Information requests. Building on those case studies, the paper then seeks to argue that Australian (and indeed global) academia is still a fundamental target for foreign adversaries seeking to expand or mature their technological and industrial bases through illicit means.

I Introduction

In 2017, Australia faced a significant national security problem. The nation was confronting a sophisticated espionage campaign on an ‘extensive, unrelenting’ scale,[1] so much so that it threatened to overwhelm the resources of its domestic intelligence agency (the Australian Security Intelligence Organisation, or ‘ASIO’).[2] ASIO was under so much pressure it was co-opting academics to provide evidence on espionage activities.[3] According to a classified report commissioned

[*] Faculty of Business, Law and Arts, Southern Cross University.

[**] Research Fellow, University of Western Australia.

[1] Jane Norman, ‘ASIO Says Espionage in Australia “Extensive, Unrelenting, Increasingly Sophisticated”’, *ABC News* (online, 17 June 2017) <https://www.abc.net.au/news/2017-06-17/espionage-australia-extensive-unrelenting-asio-says/8626072>.

[2] Andrew Greene, ‘ASIO Overwhelmed by Foreign Spying Threats Against Australia in Past Year’, *ABC News* (online, 18 October 2017) <https://www.abc.net.au/news/2017-10-18/asio-overwhelmed-by-foreign-spying-threats-against-australia/9061728>.

[3] Stephen Dziedzic, ‘Academic Says Australian Spy Agency Asked Her to Report on Chinese Students’, *ABC News* (online, 15 November 2024) <https://www.abc.net.au/news/2024-11-15/china-academic-asked-to-report-on-students-criticises-spy-agency/104601814>.

DOI: 10.38127/uqlj.v44i3.16015

by the Department of the Prime Minister and Cabinet and completed by consultancy firm McGrathNicol, Australia was at dire risk of becoming a haven for foreign spies.[4]

On 7 December 2017, then-Prime Minister Malcolm Turnbull introduced one of the most significant pieces of legislation to impact Australia's national security environment: the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) ('EFI Bill'). The Bill sought to comprehensively rewrite some of the most fundamental provisions of the *Criminal Code 1995 Act* (Cth) sch 1 ('*Criminal Code*'),[5] refreshing the decades-old definition of espionage and providing a suite of new offences for engaging in foreign interference, supporting to a foreign intelligence agency and theft of trade secrets. The amendments also sought to define wholly new classes of entity subject to potential regulation — 'foreign principals', 'foreign government principal' and 'foreign political organisation'.[6] The EFI Bill was passed by both Houses and became law on 29 June 2018.

But following the legislative flurry of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) ('*EFI Act*'), Australia has largely languished on research security law and policy. Legislative efforts in 2018 have since been eclipsed by allies in the Five Eyes: the United States ('US'),[7] Canada,[8] the United Kingdom ('UK'),[9] and New Zealand.[10] A critical analysis of the cyber domain demonstrated that Australian universities continue to struggle to protect themselves from attack.[11] The Australian policy guidelines for countering foreign interference in the university sector have remained unrefreshed since

[4] Stephanie Borys, 'China's "Brazen" and "Aggressive" Political Interference Outlined in Top-Secret Report', *ABC News* (online, 29 May 2018) <https://www.abc.net.au/news/2018-05-29/chinas-been-interfering-in-australian-politics-for-past-decade/9810236>.

[5] *Criminal Code 1995 Act* (Cth) sch 1 ('*Criminal Code*').

[6] Ibid ss 90.1–90.3.

[7] Erin N Grubbs, 'Academic Espionage: Striking the Balance Between Open and Collaborative Universities and Protecting National Security' (2019) 20(5) *North Carolina Journal of Law and Technology* 235. The US already criminalised 'standard' espionage at 18 USC § 793 (1948) but also 'economic espionage' at 18 USC § 1831 (1948).

[8] Government of Canada, *Safeguarding Research in Canada: A Guide for University Policies and Practices* (Web Page, 16 May 2024) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/guidance-research-organizations-funders-and-universities/safeguarding-research-canada-guide-university-policies-and-practices>. See also *Foreign Interference and Security of Information Act*, RSC 1985, c O-5.

[9] National Protective Security Authority, *Trusted Research Guidance for Academia* (Web Page, 18 July 2025) <https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia>. See also *National Security Act 2023* (UK).

[10] Brendan Walker-Munro, 'Land of the Long White Lab Coat: Aotearoa New Zealand and the Laws of Trusted Research' (2025) 31 *Canterbury Law Review* 1. See also Crimes (Countering Foreign Interference) Amendment Bill 2024 (NZ).

[11] Ivano Bongiovanni, 'The Least Secure Places in the Universe? A Systematic Literature Review on Information Security Management in Higher Education' (2019) 86 *Computers and Security* 350; Jin Li, Wei Xiao and Chong Zhang, 'Data Security Crisis in Universities: Identification of Key Factors Affecting Data Breach Incidents' (2023) 10(1) *Humanities and Social Sciences Communications* 270.

2021.[12] The changes wrought by the *EFI Act* itself are now under review by the Independent National Security Legislation Monitor, who has identified a significant number of issues in both the drafting and implementation of its measures.[13] And in August 2025, the Director-General of Security Mike Burgess used the annual Hawke Lecture at the University of South Australia to warn Australians that espionage is estimated to be costing the country around $12.5 billion annually.[14]

What remains unclear is the precise scope and scale of the threats posed to universities, and Australian universities in particular. Globally, academics continue to feature in news stories around the world for their involvement in acts of espionage, foreign interference and trade secret theft. Notable examples include:

- the arrest of a Brazilian university professor in Norway for acts of espionage, with allegations that he was a Colonel in the *Glavnoye Razvedyvatelnoye Upravleniye* ('GRU'),[15] the wing of Russia's military intelligence directorate with a mandate to engage in foreign spying;[16]
- an investigation into associations between Chinese academics at Stanford University detailing credible allegations that the university's research programs had been infiltrated by officials of China's Ministry of State Security;[17] and
- a parliamentary researcher and academic arrested and charged (then sensationally acquitted) by UK police for allegedly 'providing prejudicial information to a foreign state'.[18]

In the Australian context, public reporting of these types of issues is spotty. A report released by the Australian Parliament's Joint Committee on Intelligence and Security ('PJCIS') in 2022 found that 'incidents of foreign interference, censorship and intimidation were occurring on [Australian] university

[12] University Foreign Interference Taskforce, *Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, 17 November 2021).

[13] Independent National Security Legislation Monitor, *Review of Australia's Espionage, Foreign Interference, Sabotage and Theft of Trade Secrets Offences* (Issues Paper, 12 May 2025).

[14] HawkeCentre, '2025 Annual Hawke Lecture delivered by Mike Burgess AM, Director-General of Security, ASIO' (YouTube, 6 August 2025) <https://www.youtube.com/watch?v=tkKecsvhMNc>, citing Anthony Morgan and Alexandra Voce, *The Cost of Espionage* (Special Report, 1 August 2025).

[15] Thomas Nilsen, '"José" Turns Mikhail. GRU Colonel Admits Being Russian National', *The Barents Observer* (online, 14 December 2023) <https://www.thebarentsobserver.com/security/jose-turns-mikhail-gru-colonel-admits-being-russian-national/164095>.

[16] 'Main Intelligence Administration (GRU): Glavnoye Razvedyvatelnoye Upravlenie (GRU)', *GlobalSecurity.org* (Web Page, 30 July 2021) <https://www.globalsecurity.org/intell/world/russia/gru.htm>.

[17] Garret Molloy and Elsa Johnson, 'INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford', *The Stanford Review* (online, 7 May 2025) <https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/>.

[18] Joint Committee on the National Security Strategy, *Espionage Cases and the Official Secrets Acts* (House of Lords Paper No 223, House of Commons Paper No 1414, Session 2024–26).

campuses'.[19] A Queensland PhD student was refused a student visa for allegedly being 'directly or indirectly associated with the proliferation of weapons of mass destruction', but was still permitted to finish his PhD studies and return to China.[20] And a researcher — one of the few persons charged with foreign interference offences — is still yet to face trial, with delays reportedly arising from failures to obtain the consent of the Attorney-General,[21] the convoluted nature of the charges involved,[22] and national security concerns over a jury.[23]

Thus, precise numbers or empirical data on research security incidents (especially in Australia) remains elusive. That evidential shortfall is potentially damaging: in 2021, during the formulation of guidelines on the handling of foreign interference risks, Universities Australia Chief Executive and Board Director Catriona Jackson was lampooned in the media for being unable to articulate particular case studies.[24] Therefore, using documents obtained under the *Freedom of Information Act 1982* (Cth), this paper seeks to address that shortfall. Helpfully for this paper, one of the mechanisms established in the Australian government is a National Countering Foreign Interference Coordinator ('NCFIC'), supported by the Countering Foreign Interference Coordination Centre ('CFICC'). These two entities oversee much of the implementation of Australia's policy in research security, though it is couched in terms of 'countering foreign interference'.[25] The CFICC was the target of Freedom of Information ('FOI') requests related to documentation

[19] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector* (Report, March 2022) 117 [6.13] ('*PJCIS National Security Risks Affecting Higher Education Report*').

[20] Jamie Walker, 'CSIRO Cuts China WMD Academic', *The Australian* (online, 19 May 2024) <https://www.theaustralian.com.au/nation/csiro-cuts-chinese-wmd-researcher-loose-pressure-on-qut/news-story/c105edcc2d88fa643b2e40b9dc6fc1a7>. See also *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2024] FedCFamC2G 411, cited in Brendan Walker-Munro, 'Risks of Espionage in Our Universities? Lessons on Research Security from *Li v Canada*' (2024) 45(3) *Adelaide Law Review* 635.

[21] *Criminal Code* (n 5) s 93.1(1). See also Jamie McKinnell, 'Foreign Interference Charge Against Businessman Alexander Csergo Awaiting Attorney-General's "Consent", Court Told', *ABC News* (online, 4 October 2023) <https://www.abc.net.au/news/2023-10-04/nsw-businessman-alexander-csergo-accused-of-foreign-interference/102933340>.

[22] Jamie McKinnell, 'Crown Drops Allegation Businessman Alexander Csergo Prejudiced Australia's National Security', *ABC News* (online, 20 March 2024) <https://www.abc.net.au/news/2024-03-20/nsw-alexander-csergo-foreign-interference-court/103609608>.

[23] Nathan Schmidt, 'Sydney Businessman Charged with Foreign Interference Fronts Court for the First Time after 14 Months in Custody', *The Australian* (online, 19 August 2024) <https://www.theaustralian.com.au/breaking-news/sydney-businessman-charged-with-foreign-interference-fronts-court-for-the-first-time-after-14-months-in-custody/news-story/3959f3878a4d7fa6fb50996365da393b>.

[24] Lisa Visentin, 'University Peak Body Unsure Which Countries Are a Foreign Interference Risk', *Sydney Morning Herald* (online, 13 September 2021) <https://www.smh.com.au/politics/federal/university-peak-body-unsure-which-countries-are-a-foreign-interference-risk-20210913-p58r81.html>.

[25] 'Countering Foreign Interference', *Department of Home Affairs (Cth)* (Web Page) <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference>.

involving research security incidents at Australian universities. This paper reports and analyses the results of those enquiries.

Following this Introduction, Part II will examine the current position of research security in Australia, including both governmental and non-governmental responses since the first criminalisation of foreign interference in 2018. Part III involves presentation, examination and analytical critique of the FOI case studies — empirical evidence that Australia continues to be a high-profile industrial and intelligence target for foreign adversaries. Before concluding, Part IV will propose three legal and policy measures which Australia needs to consider both in meeting the current geopolitical and strategic environment and bringing the country up to speed with its contemporaries and allies.

II What is the Current State of Australian Research Security?

As an opening observation, it is important to recognise that Australian law and policy guidance does not explicitly use the term 'research security', which for present purposes can be considered as 'safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference'.[26] Instead, Australian frameworks make repeated reference only to the last of these three themes — 'countering foreign interference' — a far narrower proposition which explicitly excludes certain lawful and quasi-lawful activities that nonetheless pose national security risks to higher education settings such as, student/staff exchanges, cybersecurity, intellectual property disputes, and breaches of export controls.

Therefore, a more cohesive and coherent national policy on research security is a crucial starting proposition. The Australian government, through its funding institutions, administers not only the funds which universities need to survive, but also the competitive grants by which they demonstrate their value to society and the international economy. As will be seen in the exposition below, each element of the triumvirate — government, universities and funding agencies — have specific roles to play to support the protection of research from national security risks.

A *The Role of Government in Research Security*

Following the passage of the *EFI Act*, the Commonwealth government established the NCFIC and the CFICC at the same time as the Universities Foreign Interference

[26] Brendan Walker-Munro, 'A Missed Opportunity: Amending the *Defence Trade Controls Act 2012* (Cth) and Research Security' (2024) 2 *Journal of Strategic Trade Control* 1.

Taskforce ('UFIT') in 2019.[27] Unlike its counterpart in the Countering Foreign Interference Taskforce ('CFIT') — an enforcement-centric taskforce comprised of the Australian Federal Police, ASIO, the Australian Transaction Reports and Analysis Centre ('AUSTRAC'), and others[28] — UFIT was intended to 'collaboratively support and build an environment of trust and resilience, and to guide a university's decision-making based on proportionate risks, so Australian universities can continue to produce world-class research'.[29]

However, the role of UFIT has been criticised in recent years for not producing guidance of substance for the university sector. In the wake of the public release of generative artificial intelligence ('AI') platforms and their potential implications for national security in research, UFIT stayed completely silent.[30] Publication of the 'measures to safeguard Australia's sensitive research' in 2021 came not from UFIT, but the Group of Eight, a peak body representing Australia's eight most research-intensive universities.[31] In an Implementation Review in 2023 and a Pulse Check in 2024 (both of which were commissioned by the Department of Education),[32] universities expressed worries related to the communication and dissemination of information about UFIT initiatives and forward work plans. The specific concerns raised included 'a lack of clarity about what sort of foreign interference has relevance to the university sector'[33] and 'concerns about effectively communicating foreign interference considerations to staff, students and partners'[34] — precisely the types of clarity UFIT was meant to provide.

CFIT on the other hand appears to have been more successful in combatting foreign interference. Although prosecutions have been few and far between,[35] the Director-General of ASIO indicated in 2024 that CFIT had completed 'more than 120 operations to mitigate threats ... [and i]n a sign of how the threat has grown, successful

[27] 'University Foreign Interference Taskforce', *Department of Education* (Web Page, 11 June 2025) <https://www.education.gov.au/countering-foreign-interference-australian-university-sector/university-foreign-interference-taskforce>.

[28] Senate Select Committee on Foreign Interference through Social Media, Parliament of Australia, *Foreign Interference through Social Media* (Report, August 2023) 57 [4.29]–[4.30].

[29] 'University Foreign Interference Taskforce', *Department of Education* (n 27).

[30] Matthew Clarke, Jeanette Fyffe and Peter Murphy, 'Use of AI in Research Raises Knotty Issues', *The Australian* (online, 2 July 2023) <https://www.theaustralian.com.au/higher-education/universities-need-to-provide-more-guidance-for-use-of-ai-in-research/news-story/a77a4d353fe67f6853b9c91a794fcb73>.

[31] Group of Eight Australia, *Measures to Safeguard Australia's Sensitive Research* (Report, 19 March 2021) <https://go8.edu.au/wp-content/uploads/2021/03/Go8-Measures-to-Safeguard-Australias-Research.pdf >.

[32] Department of Education (Cth), *Pulse Check on the Implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, 23 October 2024) ('*Pulse Check*'); Department of Education (Cth), *Report on Implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector* (Report, 24 August 2023) ('*Report on Implementation')*.

[33] Department of Education (Cth), *Report on Implementation* (n 32) 7.

[34] Department of Education (Cth), *Pulse Check* (n 32) 11.

[35] Summarised in Independent National Security Legislation Monitor (n 13) 16.

disruptions have increased by 265 per cent, and continue to increase exponentially'.[36] The Director-General's evidence to Senate Estimates in 2025 was illuminating:

> One course of action could well be that the matter is handed over to the Federal Police for their lead on a prosecution. It could be that it's an intelligence led disruption by my organisation or the Australian Federal Police. That could look like an interview with the individual who is under investigation. It could be, subject to warrant, an overt entry-and-search operation or asking for a voluntary interview. It could be the use of compulsory questioning warrants. In our experience, when we declare our hand to individuals that are looking like they are either preparing or doing it, it has a deafening effect. Of course, when we've got a solid case — and that's a matter for the Federal Police — they take it on and they can do their prosecution.[37]

Further, there is evidence that the ambitious legislative regime introduced alongside the *EFI Act*, namely, the establishment of public registers to capture foreign lobbyists and influencers, also did not achieve the impact for which it was enacted. The *Foreign Influence Transparency Scheme Act 2018* (Cth) was supposed to 'provide the public with visibility of the nature, level and extent of foreign influence on Australia's government and politics'.[38] However, a statutory review conducted by the PJCIS in 2024 found that:

> Much of the evidence provided to the Committee in this review has argued that the Scheme's operation has been constrained, its effectiveness has been limited, and its implications are inhibited transparency outcomes despite a high regulatory compliance burden.
>
> In essence the Scheme has failed to achieve its intended purpose with little of consequence apparent.[39]

Likewise, the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* (Cth) reposed a power in the Minister for Foreign Affairs to cancel arrangements between Australian entities and foreign entities — such as under university research or funding agreements — that could adversely affect Australia's foreign relations and/or that are inconsistent with Australia's foreign policy.[40] Though some considered this legislation's 'capacity to politicise research and educational activities and increase regulatory burden risks undermining the core

[36] Mike Burgess, 'ASIO Annual Threat Assessment 2024' (Speech, Australian Security Intelligence Organisation Headquarters, 28 February 2024).

[37] Evidence to the Legal and Constitutional Affairs Committee, Parliament of Australia, Canberra, 27 March 2025, 111 (Mike Burgess).

[38] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the Foreign Influence Transparency Scheme Act 2018* (Report, March 2024) 1 [1.3] ('*PJCIS Foreign Interference Report*'), quoting 'Foreign Influence Transparency Scheme', *Attorney-General's Department (Cth)* (Web Page), <https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme>.

[39] *PJCIS Foreign Interference Report* (n 38) 75 [4.6]–[4.7].

[40] *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* (Cth) ss 17(3), 24(3), 35(2), 36(2).

academic mission of public universities',[41] the Minister never publicly exercised that power, despite at least one instance involving Australian researchers that arguably warranted it. In 2022, the PJCIS heard evidence relating to a research contract being entered into between Monash University and Chinese government-owned Commercial Aircraft Corporation of China ('COMAC'), which 'has been linked to a global industrial cyber espionage campaign and been sanctioned by the US government'.[42] The PJCIS recommended the Minister exercise the power to cancel that arrangement, which the government politely demurred in its response nearly a year later, saying 'Monash University has advised that all currently active research projects between Monash and COMAC will conclude in the first half of 2023, and no further activity is planned'.[43] A similar incident in 2025 occurred at Macquarie University, where a cybersecurity collaboration with Nanjing Normal University 'raised "alarm bells" among security experts and prompted Minister for Foreign Affairs Penny Wong to order an 'urgent' review'.[44]

Another legislative framework, the *Security of Critical Infrastructure Act 2018* (Cth) ('*SOCI Act*'), was expanded to higher education institutions in 2022 by the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (Cth). This imposed the substantial compliance obligations of the *SOCI Act* — including registration of critical infrastructure assets with the government, reporting of cyber security incidents, and the development of the Risk Management Program — to universities, who were strongly opposed to the changes.[45] However, almost immediately following the expansion of the obligations to the higher education sector, both the Queensland University of Technology and the University of Wollongong were subject to cyberattacks that impacted campus systems.[46] Since that time, both Western Sydney University and the Australian National University

[41] Bill Cai, 'The Sword of Damocles: Implications of the Foreign Arrangements Scheme for the Academic Freedom of Australian Public Universities' (2022) 25 *International Journal of Law & Education* 1.

[42] *PJCIS National Security Risks Affecting Higher Education Report* (n 19) 123 [6.37]–[6.38].

[43] Australian Government, *Australian Government Response to the Parliamentary Joint Committee on Intelligence and Security report: National Security Risks Affecting the Australian Higher Education and Research Sector* (Report, February 2023) 6.

[44] John Ross, '"Red flags" over Teaching Partnership with Chinese University', *Times Higher Education* (online, 6 November 2025) <https://www.timeshighereducation.com/news/red-flags-over-teaching-partnership-chinese-university>.

[45] Universities Australia, Submission No. 148 to Department of Home Affairs (Cth), *Protecting Critical Infrastructure and Systems of National Significance Consultation* (September 2020)2 .

[46] Alexandria Utting, 'More than 11,000 Employees, Students and Former Staff Affected by Cyber Attack, QUT Says' *ABC News* (online, 3 February 2023) <https://www.abc.net.au/news/2023-02-03/qut-cyber-attack-university-staff-students-affected/101929302>; Richard Chirgwin, 'University of Wollongong discloses data breach', *ITNews* (online, 11 December 2023) <https://www.itnews.com.au/news/university-of-wollongong-discloses-data-breach-603358>.

have also been impacted by cyberattacks,[47] the latter potentially assisting the government to more readily pass ransomware reporting changes to the *SOCI Act*.[48]

B *How Australian Universities Have Dealt with National Security Issues*

Like their global counterparts, Australian universities face something of an invidious challenge in the modern environment. They must balance a fundamental ethical commitment to openness, the pursuit of knowledge as a public commodity and commitment to public discourse, whilst also being forced to operate as businesses by the true financial costs of academic research.[49] As the Australian government limits research and development funding to only 1.86% of Australian GDP (compared to 3.59% in the US and 3.41% in Sweden and Japan),[50] researchers are inevitably incentivised to look abroad for funding sources. However, overseas collaborations inevitably come with the risk that either the entities providing the funding and/or the partners to that funding might subvert or sequester the research in a way that harms Australia's interests.[51] Further, changes in foreign governments can wreak havoc on funding sources if they relate to areas of research no longer considered 'appropriate' by the incoming government — for example, President Donald Trump's orders relating to excluding funding for programs incorporating diversity, equity and inclusion initiatives.[52]

[47] 'Public Notification: Western Sydney University Cyber Incident', *Western Sydney University* (Web Page, 31 July 2024) <https://www.westernsydney.edu.au/news/cyber-incident>; Mitchell Langley, 'Australian National University Faces Cyber Attack, FSociety Ransomware Threatens Data Leak', *Security Daily Review* (online, 17 February 2025) <https://dailysecurityreview.com/security-spotlight/australian-national-university-faces-cyber-attack-fsociety-ransomware-threatens-data-leak/>.

[48] *Cyber Security Act 2024* (Cth) pt 3, amending the *Security of Critical Infrastructure Act 2018* (Cth) ('*SOCI Act*') and authorising the *Cyber Security (Ransomware Payment Reporting) Rules 2025* (Cth).

[49] Natasha Bita, 'Australia Must Ramp Up Research Spending in an Age of Hi-Tech Warfare, Nobel Laureate Warns', *The Australian* (online, 28 May 2025) < https://www.theaustralian.com.au/higher-education/australia-must-ramp-up-research-spending-in-an-age-of-hitech-warfare-nobel-laureate-warns/news-story/45a1371ce2a7cc937dc8bc61b56ef5c3>; Brendan Walker-Munro, 'Nobel Laureate Brian Schmidt is "Scared" about Australia's Research Capacity: This Is Why', *The Conversation* (online, 28 May 2025) <https://theconversation.com/nobel-laureate-brian-schmidt-is-scared-about-australias-research-capacity-this-is-why-257717>.

[50] 'Research and Development Expenditure (% of GDP)', *World Bank* (Web Page, 5 April 2025) <https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?most_recent_value_desc=true>.

[51] Radomir Tylecote and Robert Clark, *Inadvertently Arming China? The Chinese Military Complex and its Potential Exploitation of Scientific Research at UK Universities* (Research Report, 24 February 2021); Brendan Walker-Munro, David Mount and Ruby Ioannou, *Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education* (Research Report, 30 October 2023).

[52] Eddy Ng et al, 'The Anti-DEI Agenda: Navigating the Impact of Trump's Second Term on Diversity, Equity and Inclusion' (2025) 44(2) *Equality, Diversity and Inclusion* 137; Herman Aguinis et al, 'Voices from the Academy: A Response to President Donald Trump's Anti-DEI Policies' (2025) 44(2) *Equality, Diversity and Inclusion* 151.

At the same time, university involvement in national security discourse seems to be on the decline. In the 2024 Pulse Check on the UFIT Guidelines, the Department of Education noted that '49% of [Australian] universities reported experiencing new or emerging barriers to implementation [of] the Guidelines'.[53] Given that the UFIT was specifically designed to provide guidance on those matters, and no changes to the UFIT Guidelines appear forthcoming, this raises the question of precisely what role the UFIT seeks to play in a contemporary research security environment. At the same time, the Pulse Check also revealed that 'universities would benefit from greater dissemination of information to practitioner-level staff',[54] suggesting that the currently top-heavy membership of the UFIT (ie, involving senior management executives such as Vice-Chancellors) is in fact one of its greatest restrictions on achieving a proper degree of communication on research security issues.

The wider discussion around universities and national security has also led to broader questions about the precise role and nature of universities in society, and what form such institutions should take in the future. Internationally, Tommy Shih and Caroline S Wagner wrote that '[p]olicymakers should recognize that security alone cannot strengthen Western economic or scientific leadership; international collaboration has become an essential ingredient to scientific and technological advancements'.[55] From the Australian context, Wesley observes:

Australia's universities now occupy an uncomfortably central role in Australia life. They are the focus of individual aspirations and societal ambitions; the sites of acrimonious disputes over what and who we value; pivotal to competing conceptions of what knowledge is for and why it is valuable. Over the past thirty years, as they have moved from the periphery to the centre of Australian life, universities have become subject to a host of competing and contradictory social, policy and academic expectations. They must drive social mobility and inclusion while being committed to individual excellence and meritocratic reward. They should be widely available but socially prestigious. They must deliver high-quality higher education to a large number of Australians but at limited cost to the taxpayer. They need to be institutionally effective and efficient but remain collegial and grounded in non-material academic values. They should be a dynamic export sector that prioritises local, and the engine of the new economy that still supplies the skills needed by the old.[56]

What has become apparent is that universities cannot be reasonably expected to shoulder all the regulatory burden for the risks flowing from research security issues. This echoes the PJCIS's conclusion from 2022 that 'the sector must move

[53] Department of Education (Cth), *Pulse Check* (n 32) 11.

[54] Ibid 10.

[55] Tommy Shih and Caroline S Wagner, 'The Trap of Securitizing Science' (2024) 41(1) *Issues in Science & Technology* 100.

[56] Michael Wesley, *Mind of the Nation: Universities in Australian Life* (Latrobe University Press, 2023) 196–7.

from a benign operating environment for our adversaries to a hardened environment … the sector, with government assistance, should create an environment where hostile activity is unfeasible, too expensive or too risky to undertake'.[57]

C *Funding Bodies and National Security Issues in Research*

Funding bodies also have a significant role to play in administering and responding to national security threat. In Australia, research is largely supported by the National Competitive Grants Program ('NCGP'), administered by a statutory body known as the Australian Research Council ('ARC').[58] Industry-specific funding can be sourced from the Commonwealth Scientific and Industrial Research Organisation ('CSIRO'), whilst medical and biological sciences are usually supported by the National Health and Medical Research Centre ('NHMRC'). Both CSIRO and NHMRC are statutory bodies, operating as Commonwealth entities with mandates that include funding administration and provision of support and guidance to Australian researchers.[59]

Of the three, the ARC has seemingly had the most exposure to national security issues. Under previous versions of the ARC's enabling legislation, the Minister for Education held a 'veto' power to refuse funding applications even in the face of recommendations from the ARC, its Board and/or its College of Experts appointed from academia.[60] This created something of a crisis of faith between academics and the Minister,[61] leading to an independent review of the ARC which concluded in 2023 that 'in every iteration, Ministerial interventions have drawn international attention, and placed at threat the capacity of Australian researchers to form research links with international university and industry collaborators'.[62] The ARC's legislation was subsequently amended to remove almost all aspects of the Minister's veto, *except* on grounds of national security, where the Minister retains that power:

[57] *PJCIS National Security Risks Affecting Higher Education Report* (n 19) 115 [6.4].

[58] *Australian Research Council Act 2001* (Cth) ('*ARC Act*').

[59] *Science and Industry Research Act 1949* (Cth); *National Health and Medical Research Council Act 1992* (Cth).

[60] *ARC Act* (n 58) ss 51(1), 53(1), 52(4) (as immediately prior to the entering into force of the *Australian Research Council Amendment (Review Response) Act 2024* (Cth) on 1 July 2024).

[61] Stephen Matchett, 'La Trobe VC Challenges ARC over Research Cancellation', *Campus Morning Mail* (online, 29 October 2018) <https://campusmorningmail.com.au/news/la-trobe-vc-challenges-arc-over-research-cancellation/>; Natassia Chrysanthos, 'Eminent Researchers Condemn Government's "Political and Short-sighted" Funding', *Sydney Morning Herald* (online, 11 January 2022) <https://www.smh.com.au/national/eminent-researchers-condemn-government-s-political-and-short-sighted-funding-20220110-p59n2i.html >.

[62] Margaret Sheil, Susan Dodds and Mark Hutchinson, *Trusting Australia's Ability: Review of the Australian Research Council Act 2001* (Final Report, March 2023) 27.

> Ministerial approval of grants of financial assistance for designated research programs
>
> (1) The Minister may, on behalf of the Commonwealth and in writing, approve the making of a grant of financial assistance to an organisation for a research project in relation to a designated research program.
>
> ...
>
> (6) The Minister must refuse to give an approval under subsection (1) if the Minister considers that, for reasons relevant to the security, defence or international relations of Australia, the approval should be refused.[63]

Concomitant with the amendment of its legislation, the ARC also published a new 'Research Security' webpage[64] as well as an updated *Countering Foreign Interference Framework*.[65] These resources should be considered as 'conditions precedent' to the operation of the Ministerial veto, as the ARC Board retains — consistent with both its enhanced research security focus and their *Framework* — a power to refuse to accept applications (or to refuse to supply such applications to the Minister for consideration for funding) which do not meet the rules of the funding program and/or the eligibility criteria.[66]

The NHMRC and CSIRO have not publicised how they counter research security risks. The NHMRC publishes no public resources on research security and does not routinely appear to operate any awareness or education programs for researchers (a curious position to take given the recognised national security risks to the life sciences).[67] The CSIRO has produced a research security tool for applicants and is collaborating internationally with its counterparts; however, those efforts have been undertaken confidentially to prevent subversion or avoidance of the program.

There are other agencies in Australia that fund research with national security implications. While those bodies are intrinsically more adept at handling issues of likely risk, they seem less likely to publicise instances of research security threat. For example, the Office of National Intelligence ('ONI') — established to coordinate Australia's National Intelligence Community[68] — administers the National Intelligence Community Research Program, comprising

[63] *ARC Act* (n 58) ss 48(1), 48(6).

[64] 'Research Security', *Australian Research Council* (Web Page) <https://www.arc.gov.au/funding-research/research-security>.

[65] Australian Research Council, *ARC Countering Foreign Interference Framework* (Report, December 2023).

[66] *ARC Act* (n 58) s 47(4).

[67] For example, see the issues of 'gain-of-function research' conducted by Ron Fouchier which led to him needing an export control licence before publishing his research publicly: Roy D Sleator, 'Ferretting Out the Facts behind the H5N1 Controversy' (2012) 3(3) *Bioengineered Bugs* 139. The US has since banned all forms of 'gain-of-function' research: *Executive Order 14292: Improving the Safety and Security of Biological Research*, 90 Fed Reg 19421, 19611 (5 May 2025).

[68] *Office of National Intelligence Act 2018* (Cth) s 7(1)(a).

both the National Intelligence Discovery Grants ('NIDG') and the National Intelligence Post-Doctoral Grants ('NIPG').[69] The Department of Defence, under programs such as Defence Cooperative Research Centres and the Strategic Policy Grants Program also funds research.[70] Neither ONI nor the Department of Defence are likely to publicise details on research security incidents to the broader community. The result is a significant gap in the communication of funding outcomes with potential national security implications to anyone other than the immediate applicant and (perhaps) their employing university — far from the 'hardened environment' envisaged by the PJCIS.

III FOI Case Studies

A full version of the documents supplied by the Department of Home Affairs are summarised in Table 1 below.[71] It is important to note that these incidents are very recent as they must, in order to have been provided to the NCFIC and CFICC, have occurred since 2019 when those agencies were established. These case studies have then been supplemented in Table 2 by case studies already listed by the Commonwealth Department of Education on their website.[72] It is unclear whether these latter case studies in Table 2 are based on real events that actually occurred, or have been created to foster discussion in the higher education sector (as there are some that show clear overlap of themes) — hence they have been labelled as 'hypothetical' below.

[69] 'National Intelligence Community Research Program', *Office of National Intelligence* (Web Page, 2024) <https://www.oni.gov.au/news/national-intelligence-community-research-program-grant-applications>.

[70] 'Grants', *Department of Defence (Cth)* (Web Page) <https://www.defence.gov.au/about/governance/grants>.

[71] A copy of this document was obtained under Freedom of Information from the Countering Foreign Interference Coordination Centre and is held by the author.

[72] 'Countering Foreign Interference in the Australian University Sector: Resources', *Department of Education (Cth)* (Web Page) <https://www.education.gov.au/resources/countering-foreign-interference-australian-university-sector>.

Table 1: Summary of case studies involving research security incidents in Australia

Case Study Summary	Threat Raised	Response
A researcher specialising in maritime defence policy and anti-piracy was the subject of a targeted spear phishing campaign. Subsequent investigations determined the researcher had previously worked in cooperation with the Royal Australian Navy.	• Cybersecurity • Conflicts of interest	Consultation with affected researcher.
A foreign academic requested 'visiting academic' status for one year, which would have enabled access to domestic resources. Their host institution was assessed as high risk on publicly available due diligence resources.	• Critical technologies (cryptography)	Proposal for visiting researcher was refused by university.
A lecturer was asked by international students in a discussion forum to remove Taiwan from the list of countries from an assignment task, because China held sovereignty over Taiwan and it was not a 'country'. There were allegations students 'intimidated' the lecturer and possibly other students.	• Foreign interference • Transnational repression • Academic freedom	Lecturer conceded to demands and removed Taiwan without discussion with other staff. Full investigation concluded that education of Faculty was necessary.
A university received several requests from PhD students to visit Australian campuses as part of their studies. All these students were part of the same research group and institute, at a foreign university which had institutional links to defence and aerospace sectors.	• Espionage • Foreign interference • Critical technologies (defence & aerospace)	Proposal for visiting researchers was refused by university.

A university student published articles with pro-democracy messaging. She was subject to a number of unwelcome and threatening acts, including: • suspicious emails; • negative reviews of her articles; • attempts to hack her social media; and • an interview with a foreign visa official conducted in the student's home.	• Foreign interference • Transnational repression	Unknown (case study did not provide this information).
An academic whose work has potential military applications (dual-use) is pressured by a senior former colleague from their home country to accept a visiting PhD researcher, paid for by a foreign government. The visiting researcher has a CV disclosing links to a university with strong defence and military links.	• Critical technologies (dual-use) • Espionage • Foreign interference	Proposal for visiting researcher was refused by university.
A foreign company offered to establish an exaflop AI supercomputer at an Australian university campus, maintained by on-campus staff employed by that foreign company. The foreign company was established and run by several persons with ties to the foreign country's 'military-industrial complex'.	• Critical technologies (AI/supercomputing) • Espionage • Foreign interference	Proposal was refused.

A foreign PhD student applied to a university to stay in Australia for two years on a scholarship paid for by the foreign government to study metamaterials. The supervisor of this student was a highly regarded academic who had received numerous defence and intelligence-centric grants. The student also requested that the letter of support not mention any critical technologies.	• Critical technologies (metamaterials) • Espionage • Foreign interference	Proposal for visiting researcher was refused by university. Attempt to 'bypass' visa scrutiny was referred to 'relevant stakeholders in the Commonwealth Government'.
A visiting academic proposed to conduct unspecified 'field work' into the use of social media by their country's ethnic minorities. The Australian university was requested only to provide visa support, office space and library access.	• Transnational repression • Foreign interference	Proposal for visiting researcher was refused by university.
A group of students published an article critical of a foreign government's repressive practices. Messages were then received from persons claiming to be from the foreign country, making threats of a personal and professional nature.	• Transnational repression • Foreign interference	Provision of support services to students. Additional training to coursework students regarding academic freedom and reporting. Increased monitoring of communications and digital safety.
An academic employee researching an area with dual-use implications was alleged to be involved in a dual appointment with a foreign university, as well as a commercial company in that country. Both allegations were substantiated after the employee had left the university's employment.	• Espionage • Critical technologies (dual-use) • Talent recruitment programs	Mandated annual disclosures for academic staff. Subsequent investigation into paid foreign appointments evidenced by publications resulted in 'a small number of staff' resigning.

A foreign doctoral candidate proposed a joint PhD between an Australian university and foreign entity. Checks showed the candidate was (then) employed by one of the foreign government's ministries (unspecified), and had appeared on state-controlled news articles on military and strategic technologies, including 'killer robots, the role of AI tools in assassinations, cyber warfare and weaponising technologies'. The candidate was also already engaged in PhD and Masters studies at two different institutions in two different countries at the time of the application.	• Espionage • Critical technologies (dual-use) • Talent recruitment programs	Unclear what action was taken –– a permit application was submitted to Defence Export Control.[73]

Table 2: Summary of Case Studies from Department of Education Resources

Case Study Summary	Threat Raised	Response
An academic writes an article critical of a foreign government and receives threats and pressure to publish more favourable views of the foreign government.[74]	• Academic freedom • Transnational repression	Discussing behavioural expectations and consequences of misconduct with students and student associations. Providing guidance to staff on facilitating these discussions at the start of the course, and throughout.

[73] As required by the *Defence Trade Controls Act 2012* (Cth).

[74] This table is copied directly from the source material provided by the Department: Department of Education (Cth), *Countering Foreign Interference Case Studies* (14 October 2024) <https://www.education.gov.au/download/18667/countering-foreign-interference-case-studies/39354/document/pdf>.

‘Following a class discussion on the issues raised in the academic’s paper, some students receive harassment and intimidation from fellow students, threatening to report them to the foreign country’s embassy and share their personal details online. Some of the affected students fear reprisals on their family overseas from a foreign government.’[75]	• Foreign interference	Secure contact mechanisms (eg, encrypted email) for reporting. Allowing staff to report issues on behalf of students. ‘No wrong door’ approach, enabling students to report to a trusted figure in the university. Formal investigation and report to ASIO.
‘A PhD student at an Australian university is undertaking a research project in the field of chemical engineering. The topic of their research has a sensitive dual-use application relating to chemical toxic agents.’[76]	• Export controls	Due diligence on research proposal.
A professor researching ‘swarm’ technology is identified as participating in an overseas talent recruitment program as well as holding an appointment as a professor at a foreign military university.[77]	• Critical technologies (drones) • Talent recruitment programs	Due diligence on academic appointments. Full investigation, leading to termination of employment.
An academic researching advanced batteries for clean energy is offered an adjunct role (including payment of research and travel costs for three months of the year) by a foreign university.[78]	• Critical technologies (clean energy) • Talent recruitment programs	Due diligence on academic appointments. Consideration of whether university conflict of interest policies and procedures are adequate.

[75] Ibid.

[76] Ibid.

[77] Department of Education (Cth), *Case Studies: Due Diligence, Risk Assessments and Management* (11 June 2025) <https://www.education.gov.au/download/19016/case-studies-due-diligence-risk-assessments-and-management/41096/document/pdf>.

[78] Ibid.

A university is encouraged to invite offers from a foreign venture capital fund (controlled by a foreign government) for that university's planned campus development works.[79]	• Foreign investment	University declined to go ahead with the investment.
Following a public protest, media reports that numerous students who attended a demonstration have received online messages from fellow students calling them traitors and threatening to report them to a foreign country's consulate.[80]	• Foreign interference • Transnational repression •	Investigation. Contacting affected students with support. Publishing a statement in support of academic freedom and democratic, lawful protest.
'An academic issues a reading list to students which is comprised of articles expressing a range of positions on a topic with strong opposing views. Some of the students enrolled in the course complained to the academic that some of the articles were offensive and demanded that those articles be removed from the list.'[81]	• Academic freedom • Transnational repression •	Provision of support to lecturer to retain reading list. Supporting the academic's response to the complainant.
Students report engaging in self-censorship in class discussions and assessments, reporting other students threatening to report them to the consulate.[82]	• Academic freedom Transnational repression • Foreign interference	Reinforce commitment to academic freedom. Providing students alternative modes of participation.

[79] Ibid.

[80] Department of Education (Cth), *Case Studies: Governance and Risk Frameworks* (11 June 2025) <https://www.education.gov.au/download/19010/case-studies-governance-and-risk-frameworks/41105/document/pdf>.

[81] Ibid.

[82] Ibid.

An academic expressing views contrary to those articulated by a foreign autocratic government receives a large volume of abusive messages and realises their personal contact details have been shared without their permission.[83]	• Cybersecurity (‘doxing’)84	Cybersecurity measures. Formal investigation and referral to law enforcement. Publishing a statement in support of academic freedom.
A university is considering establishing a foreign campus in a country suffering violent political protests and outbursts; however, the partnership agreement would give the foreign entity access to Australian student data.[85]	• Cybersecurity • Privacy	Personnel and physical security measures. Limiting offshore access to student data. Any reporting requirements obliged by Australian law.
An academic who supervises students at a foreign campus is approached by someone alleging to be a researcher interested in their project, which involves quantum physics.[86]	• Critical technologies (quantum) • Espionage	Report incident to University/ASIO. Consider engaging consular support.
A PhD candidate is invited to participate in research by one of her supervisors, located at a foreign university. This research occurs outside the scope of her PhD work, and is not supervised by her supervisor at the Australian university. She is confronted by the University Academic Integrity Officer, alleging a potential breach of their Misconduct Policy.[87]	• Lack of supervision • Reputational implications	Consideration of appropriate supervision guidelines. Assessment of whether university’s conflict of interest policies and procedures are adequate.

[83] Ibid.

[84] Doxing is defined by Australia’s e-safety Commissioner as ‘intentional online exposure of an individual’s identity, private information or personal details without their consent with the intent of causing harm’: ‘What is doxing?’, *e-Safety Commissioner* (Web Page, 28 May 2025) <https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing>.

[85] Department of Education (Cth), *University Foreign Interference Taskforce Transnational Education Working Group: Transnational Education Case Studies* (11 June 2025) <https://www.education.gov.au/download/19007/case-studies-transnational-education/41132/document/pdf>.

[86] Ibid.

[87] Ibid.

A *What the Case Studies Mean for Australian Research Security*

Both actual instances in FOI documents and the 'hypothetical' versions promulgated by the Department of Education demonstrate several lessons to Australian universities that are worth observing.

The first lesson is that the case studies reiterate warnings by Burgess in public Annual Threat Assessments since he commenced in the role of Director-General of ASIO in 2019, namely, that Australia was, is and will remain a site of intense intelligence and foreign interference interest into the future. Specific warnings borne out in the case studies include:

> We've seen visiting scientists and academics ingratiating themselves into university life with the aim of conducting clandestine intelligence collection. This strikes at the very heart of our notions of free and fair academic exchange.[88]
>
> Foreign spies are constantly seeking to penetrate … academia … to steal classified information, military capabilities, policy plans and sensitive research.[89]
>
> Following my previous address, our disruption of a 'nest of spies' got a lot of attention. But dismantling spy networks is business as usual for ASIO. We did it again last year. … Australians who were targeted by the foreign intelligence service included current and former high-ranking government officials, academics, members of think-tanks, business executives and members of a diaspora community.[90]
>
> Foreign intelligence services from multiple countries are aggressively seeking secrets about our … academic and think tank research … This applies equally to other professions that are traditionally targeted by foreign intelligence services: academics invited to an off-shore symposium …[91]
>
> [S]pies pose as consultants, head-hunters, local government officials, academics and think tank researchers, claiming to be from fictional companies… We have seen [the 'A-Team' spy network] try to recruit students, academics, politicians, businesspeople, researchers, law enforcement officials and public servants at all levels of government.[92]
>
> [N]ation states will want greater insights into their enemies –– and some of their friends –– to better understand strategic intent and capability. In a more complicated,

[88] Mike Burgess, 'ASIO Director-General's Annual Threat Assessment' (Speech, Australian Security Intelligence Organisation Headquarters, 24 February 2020).

[89] Mike Burgess, 'Director-General's Annual Threat Assessment' (Speech, Australian Security Intelligence Organisation Headquarters, 17 March 2021).

[90] Mike Burgess, 'Director-General's Annual Threat Assessment' (Speech, Australian Security Intelligence Organisation Headquarters, 9 February 2022).

[91] Mike Burgess, 'Director-General's Annual Threat Assessment' (Speech, Australian Security Intelligence Organisation Headquarters, 21 February 2023).

[92] Burgess, 'ASIO Annual Threat Assessment 2024' (n 36).

> competitive world, regimes will seek to exert more influence and control over diaspora communities.[93]

The second lesson is that both the FOI documents and hypothetical case studies do not fully demonstrate the scope of potential national security threats to the Australian research security enterprise, nor the ways that they are evolving and adapting to changes in the geopolitical environment. For example, recent reports have highlighted that North Korea has leveraged its entire nation-state intelligence apparatus towards generating a 'shadow workforce' impersonating IT workers and is *inter alia* involved in stealing research from Western academics.[94] Talent recruitment programs — such as the infamous Thousand Talents Program run by China — are explicitly banned by US law and funding conditions,[95] but not otherwise regulated in Australia. Similarly, a generalised academic naivety remains a significant challenge to the formulation and application of research security policy. Despite Xiaolong Zhu being refused a student visa by the Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs for potential risks of the diversion of his research into weapons of mass destruction, his university continued to support the appeal of his visa, with his PhD supervisor claiming his work on drone navigation in contested environments was 'not applicable to military purposes'.[96] The Minister disagreed and stood by its determination that he posed a risk.[97] That decision was affirmed by the-then Administrative Appeals Tribunal, the Federal Circuit and Family Court of Australia, and the Full Court on appeal.[98]

The third lesson is that the fundamental challenge facing universities is one of *information*: both obtaining information to inform due diligence investigations and risk assessments (either before an activity is undertaken, or in response to a complaint or tip-off), and then being able to share that information with other members of the higher education sector in Australia (either to 'warn off' specific named threat actors, or to raise the profile of specific methodologies by threat actors). The PJCIS heard evidence relating to this exact limitation during their 2022 inquiry but made no specific recommendations about information-sharing or amending the various secrecy provisions which gave rise to the limitation.[99]

[93] Mike Burgess, 'Director-General's Annual Threat Assessment' (Speech, Australian Security Intelligence Organisation Headquarters, 19 February 2025).

[94] Daryna Antoniuk, 'News Media, Foreign Affairs Experts are Targets of North Korean Group's Latest Campaign', *The Record* (online, 25 January 2024) <https://therecord.media/scarcruft-apt37-north-korea-espionage-south-korea-media-academia>; Michael Barnhart, *Exposing DPRK's Cyber Syndicate and Hidden IT Workforce* (Report, 2025).

[95] See, eg, 42 USC § 10632 (2022).

[96] *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* [2024] FedCFamC2G 411, [14], [29].

[97] Ibid [15].

[98] *Zhu v Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs* (2025) 311 FCR 237, [30]–[36].

[99] *PJCIS National Security Risks Affecting Higher Education Report* (n 19) 96 [4.81].

Finally, these case studies show that the Australian university sector is — in the words of a similar study on US institutions — simply 'too big, too distributed, too complex, and too exposed across too many sectors for a top-down, federally controlled approach to the research security challenge'.[100] One might argue that there is too much 'bad blood' or distrust between government and universities, with 'problems of authority, information, and trust, which on the one hand prevent the government from intervening or interfering in university research arbitrarily, and prevent properly informed collaboration between those two entities in response to national security risk on the other'.[101] This distrust can mean that universities adopt a hyper-cautious approach, refusing a collaboration, approach, visit or offer that had risks too high to mitigate. Although refusal could have been the appropriate decision in the circumstances, the line between 'refusal for risk' and 'racial profiling' is razor-thin and has on occasion been crossed with little benefit to Australia's reputation or interests.[102]

B *International Experiences of Research Security Threats*

Australia's experience is in line with other Western nations. In 2023 it was announced that the University of Amsterdam and the Free University of Amsterdam would partner with Huawei to build an AI laboratory in the Netherlands. However, Huawei was a poor choice of partner — in addition to having been banned from supplying 5G telecommunications infrastructure in a number of countries,[103] Huawei technology was also implicated in allegations of racial profiling of Uyghurs in Xinjiang.[104] Despite those issues, the lab was allowed to continue operating, concluding quietly at the end of 2025.

On the other hand, the Dutch government drew the ire of the research sector by proposing to implement a mandatory screening law (*Wet screening*

[100] Melissa Flagg and Zachary Arnold, *A New Institutional Approach to Research Security in the United States: Defending a Diverse R&D Ecosystem* (CSET Policy Brief, January 2021) 14.

[101] Brendan Walker-Munro, '(Professor) Hadrian's Wall: The Role of the Australian Research Council in Securing University Research' (2025) 48(1) *UNSW Law Journal* 348, 351–352.

[102] For example, in 2024 the Australian Defence Force Academy campus (University of New South Wales) indicated that 'collaborative research projects involving academics affiliated with Chinese universities will not be supported' -- a risk control based on nationality rather than specific risk factors: Andrew Greene, 'Chinese Academic Visits Banned at Canberra's Australian Defence Force Academy', *ABC News* (online, 21 August 2024) <https://www.abc.net.au/news/2024-08-21/adfa-bans-chinese-academic-visits/104247384>. Cf John Ross, 'Excluding Nationalities from Research Collaboration "Ineffective"', *Times Higher Education* (online, 24 August 2024) <https://www.timeshighereducation.com/news/excluding-nationalities-research-collaboration-ineffective>.

[103] Noah Berman, Lindsay Maizland and Andrew Chatzky, 'Is China's Huawei a Threat to US National Security?' *Council on Foreign Relations* (Web Page, 8 February 2023) <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security>.

[104] David Snetselaar, 'Dreams Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations' (2023) 32(2) *European Security* 233, 235.

kennisveiligheid)[105] which would require universities to submit all researchers — both local and international — whose research would touch on a sensitive technology area to 'security screening' (similar to a security clearance process). Those screenings would be performed by a departmental agency (*Screeningsautoriteit Justis*, a body that already conducts screenings for *vertrouwensfunctie* [position involving confidentiality]),[106] because Dutch intelligence agencies *Algemene Inlichtingen- en Veiligheidsdienst* ('AIVD') and *Militaire Inlichtingen en Veiligheidsdienst* ('MIVD') had declined to do so.[107] These investigations must be completed in no less than four weeks, or eight weeks for complex cases. Early estimates suggested *Screeningsautoriteit Justis* would perform 8,000 screenings per year (ie, completing around 30 screenings every working day);[108] however, that number has now risen to 10,000 per year and is likely to only increase.[109]

Germany likewise has recent experience with intelligence operatives at its universities. In April 2024, three persons were arrested by German authorities on suspicion of espionage, after they used academic contacts to obtain dual-use data on bearings in high-pressure machines and details of engines suitable for deployment on combat vessels. They also exported a laser to China in violation of German export laws.[110] On the other hand, students from China's Scholarship Council ('CSC') have been blocked from enrolments at German universities because they are required to give a 'loyalty pledge' to China's government that contravenes Germany's *Basic Law*.[111] CSC-funded students must also regularly

[105] 'Screening for Researchers Wising [sic] to Handle Sensitive Knowledge', *Government of the Netherlands* (Web Page, 7 April 2025) <https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge>.

[106] 'The Security Screening', *Netherlands General Intelligence and Security Service* (Web Page) <https://english.aivd.nl/topics/security-screening/the-security-screening>.

[107] 'Dutch Government to Screen Thousands of Researchers over Espionage Fears', *NL Times* (online, 8 April 2025) <https://nltimes.nl/2025/04/08/dutch-government-screen-thousands-researchers-espionage-fears>.

[108] 'The Netherlands to Screen Academics to Stop Knowledge Leaks', *DutchNews* (online, 8 April 2025) <https://www.dutchnews.nl/2025/04/the-netherlands-to-screen-academics-to-stop-knowledge-leaks/>.

[109] Daniel Hurst, 'ASIO to Take Over Issuing High-level Security Clearances due to "Unprecedented" Espionage Threat', *The Guardian* (online, 29 March 2023) <https://www.theguardian.com/australia-news/2023/mar/29/asio-to-take-over-issuing-high-level-security-clearances-due-to-unprecedented-espionage-threat>; Andrew Greene, 'Defence Struggling to Process Staff Security Clearances Needed Ahead of AUKUS Rush', *ABC News* (online, 31 March 2023) <https://www.abc.net.au/news/2023-03-31/defence-struggle-security-clearances-aukus-staff-rush/102167842>.

[110] Ido Vock, 'Germany Spying: Three Suspected Chinese Agents Arrested', *BBC News* (online, 22 April 2024) <https://www.bbc.com/news/world-europe-68873836>; Markus Weisskopf, 'Chinese Scientific Espionage in Germany: What Next?', *Science Business* (online, 2 May 2024) <https://sciencebusiness.net/universities/chinese-scientific-espionage-germany-what-next>.

[111] *Grundgesetz für die Bundesrepublik Deuschland* [Basic Law for the Federal Republic of Germany]. Articles 5(1) and (3) state: '(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures and to inform himself without hindrance from generally accessible sources … (3) Arts and sciences, research and teaching shall be free.'

submit a 'situation report' to the relevant Chinese embassy or consulate.[112] Thus, hosting institutions can clearly see in the CSC contract a concern for research security, beyond the obvious ethical and legal implications.

For some time now, the UK has taken a more collaborative approach to its research security challenges by framing the threat in terms of 'trusted research' and establishing the Research Collaborative Advice Team ('RCAT'), a body inside the Department of Science, Innovation and Technology which serves as 'a first point of contact for official advice about national security risks linked to international research'.[113] The RCAT operates alongside more traditional research security controls including the Academic Technology Approval Scheme ('ATAS'), a migration scheme requiring a certificate from the Home Office before foreign scholars in certain technological fields can travel to the UK.

In the US, allegations of espionage at Stanford University have resulted in both Departmental and Congressional investigations into funding from foreign entities.[114] Simultaneously, US authorities have recently brought charges against researchers for allegedly attempting to smuggle biological material into the country. In the first case, two researchers were apprehended with samples of a fungus known as head blight alleged to be a 'potential agroterrorism weapon' causing 'billions of dollars in economic losses worldwide each year'.[115] Another case involved the detention of a PhD candidate bringing samples of round worms into the US after allegedly deleting the content of her electronic devices prior to apprehension.[116]

Canada has taken a policy journey on opposite tracks to Australia. Canada has focused on research security since 2016,[117] but has more recently pivoted to a foreign interference focus in response to alleged interference in Canadian electoral

[112] UK-China Transparency, *China Scholarship Council 'Rules': Translation and Notes* (15 November 2023) <https://ukctransparency.org/wp-content/uploads/2023/11/China-Scholarship-Council-Rules-translation-and-notes-1.pdf>.

[113] 'Trusted Research Guidance for Academia', *National Protective Security Agency* (Web Page, 18 July 2025) <https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia>; 'Research Collaboration Advice Team: About Us', *Gov.UK* (Web Page) <https://www.gov.uk/government/organisations/research-collaboration-advice-team>.

[114] Molloy and Johnson (n 17); Sophia Chu, 'Congress Requests Information about Chinese National Students, Cites National Security Concerns', *Stanford Daily* (online, 1 April 2025) <https://stanforddaily.com/2025/04/01/congress-chinese-stude-information/>; Phelim Kine and Eric Bazail-Eimil, 'Congress Worries about Chinese Spies on College Campuses', *Politico* (online, 9 May 2025) <https://www.politico.com/newsletters/national-security-daily/2025/05/09/congress-worries-about-chinese-spies-on-college-campuses-00339754>.

[115] Department of Justice (US), 'Chinese Nationals Charged with Conspiracy and Smuggling a Dangerous Biological Pathogen into the US for Their Work at a University of Michigan Laboratory' (Press Release, 4 June 2025).

[116] Department of Justice (US), 'Alien from Wuhan, China, Charged with Making False Statements and Smuggling Biological Materials into the US for Her Work at a University of Michigan Laboratory' (Press Release, 9 June 2025).

[117] Public Safety Canada, 'Parliamentary Committee Notes: Research Security in Canada', *Government of Canada* (Web Page, 26 August 2024) <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240813/03-en.aspx>.

processes.[118] The Canadian university and research sector has been rocked by a number of national security scandals, including providing alleged 'background cover' (ie, a false employment connection) to the GRU Colonel arrested in Norway,[119] as well as possibly allowing two Chinese scientists with links to military microbiology labs to export potentially lethal biological weapons to China.[120]

C *Responding to Threats: The 'Blanket No'*

The FOI documents and hypothetical case studies suggest that Australian universities are more risk-averse than their international counterparts in instituting research security controls. Six of the 12 case studies in the FOI documents demonstrated that the university involved 'refused' to allow the relevant research or collaboration to proceed — suggesting, in effect, a 'blanket no' response. For context, a 'blanket no' response is one where the institution flat out refuses the research, collaboration or association, with no possibility of risk mitigations or management.

That result is surprising, given that research security protocols are often motivated by the desire to approve the conduct of the research, even if the research itself is subject to the imposition of regulatory controls or conditions.[121] Chief of Research Security Strategy and Policy at the US National Science Foundation, Dr Rebecca Kaiser, summarised this stance it recently in saying:

> We want to continue to fund the best research here in the United States, and if we decline proposals because we think they're too risky, then researchers might seek that funding elsewhere. We also want to focus on mitigation, rather than decline, and get to 'yes'.[122]

Given that international perspective, a finding that Australian universities are overwhelmingly tilting towards a 'blanket no' response is supported by the literature on risk management in higher education settings. Universities conduct substantial amounts of research across a vast swathe of fields, covering areas of law that carry national security implications including foreign direct investment,

[118] National Security and Intelligence Committee of Parliamentarians, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* (Report, 22 March 2024).

[119] Guillaume Corneau-Tremblay, 'Did a Russian Spy Operate out of Two of Canada's Universities?', *Policy Options* (online, 6 December 2022) <https://policyoptions.irpp.org/magazines/december-2022/russian-spy-canadian-universities/>.

[120] Catharine Tunney, 'Lies and Scandal: How Two Rogue Scientists at a High-Security Lab Triggered a National Security Calamity', *CBC News* (online, 2 March 2024) <https://www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7130284>.

[121] Yoran Beldengrun, Carthage Smith, 'What is research security and why does it matter for global science?' *OECD* (blog, 21 November 2025) <https://www.oecd.org/en/blogs/2025/11/what-is-research-security-and-why-does-it-matter-for-global-science.html>.

[122] Clare Zhang, 'Getting to "Yes": NSF Pilots Research Security Assessment for Grants', *American Institute of Physics* (Forum Post, 26 November 2024) <https://www.aip.org/fyi/getting-to-yes-nsf-pilots-research-security-assessment-for-grants>.

export controls and dealing with sanctioned countries and entities.[123] To mitigate those risks, states create new laws and impose new or modified duties to limit or prevent risk-taking behaviour.[124] Given that universities are generally considered one of the most highly regulated environments in the world,[125] one might assume that university research is an overwhelmingly dangerous exercise. Although that conclusion is clearly nonsense, it does highlight the obvious cultural tension between universities as austere and conservative bastions of free intellectual inquiry, and universities as protectors of knowledge that is in the nation-state's security or economic interests. Empirically too, universities continue to demonstrate that they are far more risk-averse in pursuit of research and development, innovation and commercialisation opportunities, unable to properly mimic the achievements of the private sector.[126]

Research security programs are also supposed to demonstrate 'country-agnosticism', that is, they apply to scholars and students irrespective of their nationality. Both the European Commission's recommendation on research security[127] and Canada's Sensitive Technology Research and Affiliations of Concern ('STRAC') policy[128] explicitly incorporate that notion. Yet country-agnosticism is harder to enact than it looks, with nationality (especially for Chinese scholars and students) often used as a proxy for actual risk.[129] Further, the impositions of certain countries' domestic laws can create difficulties in enacting country-agnosticism as a policy position.

[123] Brendan Walker-Munro, *Shifting the Needle: Making Australia's Research Security Ecosystem Work Smarter* (Policy Brief, 30 June 2025) ('*Shifting the Needle*').

[124] Michael Power, 'The Risk Management of Everything' (2004) 5(3) *Journal of Risk Finance* 58; Olga Hrynkiv, 'Legal and Policy Responses to National Security Measures in International Economic Law' (2022) 54(2) *Georgetown Journal of International Law* 165.

[125] Ann Brewer and Ian Walker, 'Risk Management in a University Environment' (2011) 5(2) *Journal of Business Continuity and Emergency Planning* 161; Ivano Bongiovanni, Karen Renaud and George Cairns, 'Securing Intellectual Capital: An Exploratory Study in Australian Universities' (2020) 21(3) *Journal of Intellectual Capital* 481; Group of Eight Australia, *Essential Decisions for National Success: Reducing the Regulatory Overload on our Universities* (Report, 2 May 2022); Marcus Smith and Patrick Walsh, 'Security Sensitive Research: Balancing Research Integrity, Academic Freedom and National Interest' (2023) 45(5) *Journal of Higher Education Policy and Management* 495.

[126] Keiko Yokoyama, 'The Rise of Risk Management in the Universities: A New Way to Understand Quality in University Management' (2018) 24(1) *Quality in Higher Education* 3; Ana Paula Beck da Silva Etges and Marcelo Nogueira Cortimiglia, 'A Systematic Review of Risk Management in Innovation-Oriented Firms' (2019) 22(3) *Journal of Risk Research* 364; Anil K Narayan and John Kommunuri, 'New Development: The Behavioural Effects of Risk Management in Higher Education' (2022) 42(6) *Public Money & Management* 414.

[127] *Council Recommendation of 23 May 2024 on Enhancing Research Security* [2024] OJ C 2024/3510, art 1(g).

[128] Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern* (Report, 9 January 2024).

[129] Sapna Marwaha, 'The Challenge of Pursuing Research Security when Nationality Becomes a Shorthand for Risk', *Wonkhe* (Blog Post, 10 June 2024) <https://wonkhe.com/blogs/the-challenge-of-pursuing-research-security-when-nationality-becomes-a-shorthand-for-risk/>.

To give one example, we can turn to the EU where (in the name of protecting academic freedom) many Chinese academics are functionally blocked from research because of the conditions attached to their source of funding. In Germany, the Friedrich Alexander University of Erlangen-Nuremberg ('FAU') decided to 'suspend collaboration with holders of scholarships awarded by the [CSC] indefinitely'.[130] Faculties of several Netherlands institutions have also suspended or stopped their collaboration with CSC because of the infringements on academic freedom involved.[131] In Sweden, Aarhus University stopped admitting PhD students with CSC funding, while Uppsala and Lund Universities 'imposed a temporary bar'.[132]

Having a 'blanket no' approach to CSC-funded academics is a clear policy position allowing universities to redirect limited resources elsewhere, short-cutting the due diligence process. But not all universities have the capacity to make the same decision. For many institutions, appointing CSC-funded PhD students is financially beneficial due to the stipends paid through the scholarship. In Australia, cost-efficient PhD completions improve a university's block funding from the government, with the result that a large part of the expansion of a university's research capacity is usually the result of cross-subsidised or externally funded researchers.[133] However, universities should not have to accept greater threat to research security to maintain financial stability.

IV How Research Security in Australia Could (and Must) Change

Australian society has long recognised that the imperative to protect the sanctity of university teaching and research is not just a legal obligation, but a moral and ethical one as well. As the High Court of Australia articulated:

> The maintenance of high standards of teaching and research, and the furtherance of the export of university services by Australian universities, make it essential that public regulation of universities be scrupulously maintained, in accordance with the law enacted to achieve that objective. It also makes the defence of academic standards

[130] Yojana Sharma, 'German University Ends Ties with China Scholarship Scheme', *University World News* (online, 20 July 2023) https://www.universityworldnews.com/post.php?story=20230720113914406>.

[131] These include the Free University of Amsterdam, the University of Amsterdam, the Erasmus School of Social and Behavioural Sciences and the Erasmus School of Economics, as well as the Technical University Delft and Utrecht University: Yojana Sharma, 'Universities Urged to Plan for Loss of China's PhD Students', *University World News* (online, 20 March 2024) <https://www.universityworldnews.com/post.php?story=20240321003823472>.

[132] Louis Beck Petersen, 'AU Stops Admitting PhD Students from China Who Have Signed Allegiance to the Chinese Communist Party', *Omnibus* (online, 27 March 2023) <https://omnibus.au.dk/en/archive/show/artikel/au-stopper-optaget-af-kinesiske-phd-studerende-der-har-underskrevet-troskabsed>.

[133] Universities Australia, *Investing in PhD Candidates in Australia* (Report, December 2024).

> and of the integrity of degrees or awards and university research a vital part of the functions of such statutory bodies.[134]

Universities have acknowledged that some level of risk-taking is involved (and, perhaps, even required) to achieve rigorous academic debate and the precipitation of innovation. Research security is imperative to enable international engagement, protect the staff and students, and protect the university itself. However, unnecessary bureaucratic burden can impede opportunities for researchers to pursue or engage in higher-risk activities in the first place. Further, levels of risk to which each university is exposed — and their relative appetites to accept residual risk — differ wildly across the university sector, owing to differences in research foci, student and staff demographics, local and global strategies, and competing market forces for grants and student enrolments.

A *Increased Research Security Prominence in Australian Policy*

Australia needs a federal research security policy that subsumes or replaces the existing UFIT Guidelines with a more cohesive and collaborative form of guidance. This will require that Australia capitalise on its earlier 'first-mover' advantage in passing the *EFI Act* by establishing a clear, flexible and balanced research security policy and provide whole-of-government clarity on precisely 'what research security entails, its purpose, and the standards expected consistently across the sector'.[135] That in turn will oblige the Australian government to consider which of the various regulatory approaches taken by comparable institutions is best suited to protecting our national interests — whether that is in the form of the EU's 'as open as possible, as closed as necessary' principle, or the more collaborative and advisory approach typified by the UK's RCAT.

As a contemporary example of what such a policy could look like, the recently released UK National Security Strategy announced expansion of the RCAT and the upcoming publication of the UK's first Research Security Strategy. According to the publication, academia is considered a strategic defence asset and require that '[t]he UK defence industrial base [will be] redefined to include academia, dual-use civilian-military companies, financial services, technologists and trade unions'.[136]

Australia's research security policy will need to move beyond the traditional political lens of countering foreign interference, a term derived in large part from the changes wrought by the *EFI Act*. That political lens is no longer fit-for-purpose, as Australia's limited prosecutions for the offence no doubt demonstrate: the charges of 'recklessly engaging in foreign interference' filed against Alexander Csergo have either captured an illicit provider of sensitive information to foreign

[134] *Griffith University v Tang* (2005) 213 ALR 724, [107] (Kirby J).

[135] Walker-Munro, *Shifting the Needle* (n 123) 4.

[136] Cabinet Office (UK), *National Security Strategy 2025: Security for the British People in a Dangerous World* (Policy Paper CP1338, 24 June 2025) 42.

intelligence agents, or subjected an honest open-source researcher to prosecution and potentially twenty years' imprisonment.[137] A properly formulated approach to research security not only subsumes foreign interference, it covers acts that are legal but are still of concern to Australia's interests.

The policy will also need to address that the time for the UFIT to act as a worthwhile contributor to Australian research security has well and truly passed. Although UFIT was instrumental in establishing the UFIT Guidelines and guiding early policy development, its utility appears to have waned. Departmental guidance from both Home Affairs and Education on countering foreign interference in higher education has continued largely independently of (or at least tangentially to) UFIT's involvement, and the Guidelines themselves have not been refreshed since 2021 despite several significant shifts in Australian geopolitics and foreign policy. Further, UFIT has been either subordinated or eroded by the establishment of numerous sub-groups such as the Trusted Information Sharing Network for higher education ('TISN'),[138] the Western Australian universities community of practice[139] and the Informal Foreign Interference Network ('INFIN'). Put another way, one might ask: 'If UFIT was working, why would universities need these additional bodies?'

An Australian research security policy will also need to address the generalised academic naivety as to Australia universities as intelligence targets. In 1988, then Director-General of Security Harvey Bennett famously quipped: 'With the simple self-confidence which living in an island state breeds, Australians are sometimes doubtful that their country might be of interest to foreign intelligence services.'[140] Nearly thirty years later, Mike Burgess gave the 2025 Hawke lecture, where he said that '[a] new iteration of great power competition is driving relentless hunger for strategic advantage and an insatiable appetite for inside information. ... Nation states are spying at unprecedented levels and with unprecedented sophistication.'[141] Burgess' comments come

[137] Brendan Walker-Munro and Sarah Kendall, 'Could Using Open-Source Information Online Get You Arrested for Foreign Interference?', *The Conversation* (online, 4 May 2023) <https://theconversation.com/could-using-open-source-information-online-get-you-arrested-for-foreign-interference-204548>. For completeness, we note that a Chinese national has recently been charged with reckless foreign interference for surveilling the Buddhist organisation Guan Yin Citta Dharma Door –– however, this has no direct link to academia and will not be further examined: Elizabeth Byrne and Jade Toomey, 'Court Documents Allege "Unexplained Wealth" of Chinese National Charged with Reckless Foreign Interference', *ABC News* (online, 11 August 2025) <https://www.abc.net.au/news/2025-08-11/chinese-national-charged-foreign-interference-unexplained-wealth/105637550>.

[138] 'Trusted Information Sharing Network (TISN) for Higher Education and Research', *Critical Infrastructure Security Centre* (Web Page) <https://www.cisc.gov.au/information-for-your-industry/higher-education-and-research/partnership-and-collaboration/trusted-information-sharing-network>.

[139] Department of Education (Cth), *Report on Implementation* (n 32) 11.

[140] Harvey Barnett, *Tale of the Scorpion* (Allen and Unwin, 1988) 35.

[141] HawkeCentre (n 14) 18:15, 23:40.

alongside six years of publicised ASIO threat assessments. Yet, Macquarie's relationship with Nanjing Normal University[142] and continued issues with foreign research collaborations[143] suggest that the message is not quite cutting through.

B *Dealing with Information Asymmetry*

In June 2025, the ARC communicated that it was strengthening its processes to protect the security of ARC funded research to meet new legislative requirements under amendments to the *Australian Research Council Act 2001* (Cth).[144] In addition to the establishment of the ARC Board (which replaced the previous governance structure), other actions by the ARC to support obligations where matters of national security, defence or international relations arise included engaging with universities for earlier research screening and to seek detailed and specific assurance and evidence that risks are managed appropriately. Although an early engagement focus is laudable, the existence of a veto power at both the level of the ARC Board and the Minister is concerning where there is no legislative requirement for transparency around the exercise of such powers.[145]

As touched on earlier, information sharing between governments, industry and academia remains a significant barrier to enhancing research security across all universities. The FOI case studies illustrate a range of threats to research security and allude to the key information that would enable universities to develop better safeguarding practices. Lack of knowledge sharing is already a well-known issue broadly relevant to national security. As Rory Medcalf recently said: 'When it comes to the security landscape, the gap between what government knows and what it says in public must become narrower, not widen.'[146] The result is that whilst

[142] Ross (n 44).

[143] James King, 'Australian university uses taxpayer funds for research with Russian nuclear scientist', *Daily Telegraph* (online, 31 December 2025) <https://www.dailytelegraph.com.au/education/higher-education/australian-university-uses-taxpayer-funds-for-research-with-russian-nuclear-scientist/news-story/ee7b44ed1c6cb72f649c6f142a710109>; James King, 'Top scientist on Australian defence project worked with Chinese military researchers', *Daily Telegraph* (online, 28 January 2026) <https://www.dailytelegraph.com.au/news/national/top-scientist-on-australian-defence-project-worked-with-chinese-military-researchers/news-story/a923da9d45edb253401aa37c176d3eeb>.

[144] Australian Research Council, 'Strengthened Processes, Funding Announcements and Extension Updates' (Network Message, 18 June 2025) <https://www.arc.gov.au/news-publications/media/network-messages/strengthened-processes-funding-announcements-and-extension-updates>.

[145] *ARC Act* (n 58) ss 47(8), 48(6) permit the Minister to refuse grant applications or approvals 'for reasons relevant to the security, defence or international relations of Australia', but there is no provision that requires the Minister explain his or her reasons for doing so.

[146] Rory Medcalf, 'Why We Need a Different Conversation about National Security' (Speech, 'Securing Our Future' National Security Conference, Australian National University, 8 April 2024).

government may hold relevant information, they are unaware in practical terms what most universities and researchers are doing. Simultaneously, universities and researchers remain largely unaware of what their fellow universities and researchers are doing, and privacy laws prevent them from informing each other. Promoting information sharing about who the threats are and what they are doing would, we argue, enable universities to proactively identify and address national security concerns at a local level, improve risk-based approaches, and foster a broader community-approach to research security.

Dealing with information asymmetry will also require Australia to confront whether it possesses the legislative capacity and Ministerial boldness to 'name names' of intelligence officials, foreign interference agents and proxies which pose threats to research security. This could be achieved either under broad-based provisions of *Autonomous Sanctions Act 2011* (Cth), or via a targeted legal reform of that Act. For example, the Joint Standing Committee on Foreign Affairs, Defence and Trade recently recommended that Australia 'include criteria for the thematic area of "threats to international peace and security"' in the *Autonomous Sanctions Regulations 2011* (Cth) to address inter alia 'pervasive national security threats to academia'.[147]

Unfortunately, the Australian government and its grant-awarding bodies have a history of being reticent to engage in naming entities that pose a research security risk, a contrast to its international counterparts. For example, the US Secretary of War must publish an annual list of foreign entities that have a demonstrated history of intellectual property theft, espionage, intelligence recruitment, or otherwise 'operate under the direction of the military forces or intelligence agency of the applicable country' or 'pose a serious risk of improper technology transfer of data, technology, or research that is not published or publicly available'.[148] The Canadian government, under its Policy on Sensitive Technology Research and Affiliations of Concern ('STRAC'), also publishes a list of *Named Research Organisations* which include any 'university, research institute or laboratory connected to military, national defence, or state security entities that could pose a risk to Canada's national security'.[149] Japan likewise publishes an 'End-User List' of entities to whom exports are forbidden without a licence,

[147] Joint Standing Committee on Foreign Affairs, Defence and Trade, Parliament of Australia, *Australia's Thematic Sanctions Framework: A Legislated Review of the Operation of the Autonomous Sanctions Amendment (Magnitsky-Style and Other Thematic Sanctions) Act 2021* (Report, March 2025) ix [1.71], 11 [1.35].

[148] *William M (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub L No 116-283, §1286, 41 Stat 1417. This is in addition to the Entity List maintained by the Bureau of Industry and Security under US Export Administration Regulations of 'persons or addresses involved in activities contrary to US national security or foreign policy interests' (15 CFR § 744, Supp No 4 (2026)).

[149] Government of Canada, *Named Research Organizations* (January 2024) 3.

because the 'concerns about the development of weapons of mass destruction have not been eliminated'.[150]

Engaging in naming foreign entities with whom Australian research collaboration is not permitted or welcomed carries obvious risks to diplomacy, geopolitics and foreign policy. Those risks might be impossible to countenance for a country for whom tertiary education is in the top five of exported commodities.[151] But that argument ignores a fundamental observation about Australia's higher education sector: naming and shaming already occurs, but not in a holistic or coordinated way. For example, the publication of the Australian Strategic Policy Institute's *China Defence Universities Tracker* in 2019 was answered in some corners of the media with condemnation for pillorying Chinese students;[152] yet it had negligible impact on Australia's foreign student numbers or education export value. Nor has ASIO's carefully crafted but consistent warnings about espionage or intellectual property theft over the past six years done anything to discourage foreign student attendance in Australia. In February 2023, Burgess said that '[f]oreign intelligence services from multiple countries are aggressively seeking secrets about our...academic and think tank research';[153] yet in December of that same year Universities Australia CEO Catriona Jackson called our education exports for 2023 'the biggest export we don't dig out of the ground'.[154]

Declaring a list of prescribed entities (whether sanctioned or otherwise) also has the benefit of confronting and dealing with academic naivety in the research security space. Taking a look at the Canadian *Named Research Organisations* list published under their STRAC policy, it is difficult to conclude that Canadian researchers would *not* be threatened by potential associations with the 'Explosion and Impact Technology Research Centre' (Iran), the 'Center for Military Technical Problems of Biological Defense' (Russia), or the 'Rocket Force Research Institute' (People's Republic of China). Similarly, the STRAC policy makes very clear that researchers should remain open to the possibility of risk no matter the nature of their collaboration:

[150] Japan Ministry of Economy, Trade and Industry, 'Review of the End User List Providing Information on Foreign Entities for which Concern Cannot be Eliminated Regarding the Development of Weapons of Mass Destruction and Missiles' (Media Release, 31 January 2025).

[151] 'Education Export Income: Financial Year', *Department of Education (Cth)* (Web Page, 3 February 2026) <https://www.education.gov.au/international-education-data-and-research/education-export-income-financial-year>.

[152] Brian Toohey, 'Reports of China Spies and Takeover Plots are Fanciful', *The Age* (online, 5 December 2019) <https://www.theage.com.au/national/reports-of-china-spies-and-takeover-plots-are-fanciful-20191204-p53gnu.html>; Myriam Robin, 'The Think Tank Behind Australia's Changing View of China', *The Australian* (online, 15 February 2020) <https://www.afr.com/policy/foreign-affairs/the-think-tank-behind-australia-s-changing-view-of-china-20200131-p53wgp>; Sam Varghese, 'ASPI Sensitive to Fact that China Study Paid for by US State Department', *ITWire* (online, 16 February 2020) <https://itwire.com/opinion-and-analysis-sp-481/open-sauce/aspi-sensitive-to-fact-that-china-study-paid-for-by-us-state-department.html>.

[153] Burgess, 'ASIO 2023 Annual Threat Assessment' (n 91).

[154] Universities Australia, 'Education Surges as Other Exports Drop' (Media Release, 5 December 2023).

> Researchers should keep in mind that institutions that are not included on the list may still pose a risk. As a best practice, researchers are encouraged to apply due diligence practices to mitigate risks that may be associated with any collaboration or partnership in a sensitive technology research area. Researchers are also encouraged to transparently disclose their affiliations, funding, and in-kind support with their sponsoring institution and with their research team, to foster trust and to ensure the security of sensitive research from unwanted transfer of knowledge and technology.[155]

In summary, attempts to address research security in Australia that fall short of some kind of 'naming and shaming' regime will 'ultimately be sub-optimal unless the government finds the courage to publicly name those who are interfering'.[156]

C *A Healthier, More Balanced View of Risk*

Beneath both a more prominent research security policy and the possibility of dealing with information asymmetry between government and academia, there is also a need for a more fulsome discussion of risk between both of those parties. In a recent report on Australia's National Intelligence Community, Chris Taylor argued that governmental innovation is essential to keep pace with larger partners and keep ahead of adversaries; yet Australia's intelligence agencies are increasingly risk averse and struggling to adopt emerging technologies.[157] Those findings echo an earlier landmark examination of innovation in the US intelligence community, which concluded that

> decisionmaking remains too focused on the risk of action but fails to assess and incorporate the risk of inaction and the opportunity cost of not acquiring and integrating new technologies into intelligence missions. This task force does not cavalierly dismiss the critical threats and risks … associated with new technology and data streams. Indeed, risk must always be central in analyzing technology adoption, but decisions cannot be made solely on those grounds. An element of [US]IC culture that leaders must prioritize transforming is this risk aversion, where risk-taking, experimentation, and creation will be rewarded and where innovators are not unduly punished when there is inevitable failure.[158]

Risk aversion has been, and remains, a significant brake on national security decision-making, whether in the university sector or elsewhere.[159] When it comes to regulating sensitive areas of research, there is space to address gaps in

[155] Government of Canada, *Named Research Organizations* (n 149) 3.

[156] James Corera and Chris Taylor, 'Countering Foreign Interference: The Government Should Name Names', *The Strategist* (online, 28 January 2025) <https://www.aspistrategist.org.au/countering-foreign-interference-the-government-should-name-names/>.

[157] Chris Taylor, *Match-Fit for the Global Contest? Innovation, Leadership, Culture and the Future of Australia's National Intelligence Community* (Special Report, 29 July 2025).

[158] Center for Strategic and International Studies, *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation* (Report, January 2021) 42.

[159] Gary P Corn, 'National Security Decision-Making in the Age of Technology: Delivering Outcomes on Time and on Target' (2021) 12(1) *Journal of National Security Law and Policy* 61.

Australia's framework through voluntary codes of conduct or accreditation schemes.[160] However, this may not meet all of Australia's strategic objectives, such as the need to have a comparable export control framework to the US, itself necessary for Australia to be part of the licence-free environment of the AUKUS community.[161] Moreover, it is unclear whether the costs associated with establishing and complying with self-regulation versus the costs of a focused Australian government process would be lower for the higher education research sector. The nature and the severity of the risks also suggest that instead of voluntary approaches, which may be inconsistent and have a slow uptake, government regulation would be more appropriate.

We suggest that a proper research security framework would use a Commonwealth research security policy (replacing the UFIT Guidelines) as a kind of 'baseline', establishing a set of requirements that apply across all universities in Australia's higher education research sector, irrespective of size, target markets, demographics and research profiles or specialties. Those 'baselines' should be the subject of auditing or certification by a governmental body such as the Tertiary Education Quality and Standards Agency (TEQSA). Once a set of commonalities that holistically address broad research security risk has been established across the sector, the role of government can shift from being regulator to being a trusted advisor, similar to the role provided by the UK'S RCAT. In that environment, universities should be encouraged to develop and self-assure their own security and risk management programs, but with guidance from government and its intelligence organs as appropriate to enable up-to-date threat intelligence sharing and best practice implementation.

Another approach drawing international attention is the establishment of security committees, composed of senior academics and risk professionals from across multiple faculties and given a mandate to review the entire research program of the university. Originating in Germany following the June 2014 report published by centralised research funding bodies *Deutsche Forschungsgemeinschaft* ('DFG') and Leopoldina,[162] these *Kommissionen für Ethik der Forschung* ('committees for ethics in security-relevant research', or 'KEF') were established at approximately 120 research institutions and campuses across Germany to advise on research with potential national security implications.[163]

There are criticisms of scrutiny committees. Some have suggested that these committees could themselves become tools of repression or suppression of

[160] See generally Smith and Walsh (n 125).

[161] Gary Dutton et al, 'Reform of Australia's Export Control Regime', *PriceWaterhouseCoopers* (Insights Article, 5 March 2025) <https://www.pwc.com.au/tax/trade/reform-of-australias-export-control-regime.html>.

[162] Deutsche Forschungsgemeinschaft and Leopoldina Nationale Akademie der Wissenchaften, *Scientific Freedom and Scientific Responsibility: Recommendations for Handling of Security-Relevant Research* (Report, June 2014).

[163] 'Find Contact Persons', *Gemeinsamer Ausschuss zum Umgang mit Sichereheitsrelevanter Forschung* (Web Page) <https://www.sicherheitsrelevante-forschung.org/contactpersons/>.

academic freedoms, by refusing to permit research in valuable areas of human endeavour because of a failure to properly meet 'risk appetites' (whether or not it is even physically possible to do so, given the nature of the research concerned).[164] But other jurisdictions have followed suit in establishing similar scrutiny committees: in the US, research security committees have been established largely in response to National Security Presidential Memorandum No 33 issued by the first Trump administration.[165] The EU is likewise considering the establishment of research security committees along the same lines as research ethics committees, in order to meet the obligations imposed by the European Council Recommendation of May 2024.[166]

Of course, such ambitious models have resourcing implications for both government (as regulator) and universities (as regulatees). Other jurisdictions offer funding vehicles to support universities in developing and implementing research security programs or initiatives, either in the form of research and development incentives or payment schemes designed to defray the costs of personnel and capital investment. For example, this could be achieved by establishing a 'national security focused technology fund' (in emulation of the UK's National Security Strategic Investment Fund)[167] or alternatively a research security-specific fund akin to Canada's Research Support Fund.[168] Whether Australia follows suit is a matter for the Treasury; given that universities have already borne the brunt of compliance costs for countering foreign interference on behalf of the government,[169] it might be appropriate (and indeed wise) for it to find a way to support the protection of Australian interests in higher education research.

V Conclusion

Australia had a strong head start when it passed its suite of national security laws in 2018, but it has since lost that first-mover advantage. The risk environment has

[164] Jessica Hehman and Catherine Salmon, 'How Institutional Review Boards Can Be (and Are) Weaponized Against Academic Freedom', *Unsafe Science* (Blog Post, 1 July 2024) <https://unsafescience.substack.com/p/how-institutional-review-boards-can>; Igor R Efimov et al, 'Politicizing Science Funding Undermines Public Trust in Science, Academic Freedom, and the Unbiased Generation of Knowledge' (2024) 9 *Frontiers in Research Metrics and Analytics* 1418065:1–13.

[165] Office of the US President, *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy* (National Security Presidential Memorandum No 33, 14 January 2021).

[166] Vasiliki Mollaki et al, 'Challenges and Recommendations for Research Security: Learning from Research Ethics and Integrity' (2026) *Research Ethics* 17470161251404962:1, 8.

[167] 'National Security Strategic Investment Fund: About NSSIF', *British Business Bank* (Web Page) <https://www.british-business-bank.co.uk/finance-options/equity-finance/national-security-strategic-investment-fund>.

[168] Public Safety Canada, *Evaluation of the Funding to Build Canada's Research Security Capacity* (Report, 4 July 2025).

[169] Department of Education (Cth), *Report on Implementation* (n 32).

changed significantly, and regimes like the Foreign Arrangements Scheme and Foreign Interference Transparency Register now appear as outdated relics. Universities have changed as well, being increasingly mobilised to counter fractured geopolitics whilst also trying to balance finances tied to foreign students. Asking universities in that environment to work more closely and more openly with government, without a reciprocal investment by government in research funding, is not likely to be successful. Yet as the FOI case studies identified in this paper demonstrate, the current approach by Australia's higher education research ecosystem is simply not working.

As we have argued, Australia needs to adopt a research security policy as a matter of priority. That policy needs to be tied closely to the NCGP, so that only research which benefits Australia's national interests receives competitive funding. That might require the NCGP to be comprehensively reviewed to make sure it still meets its objectives, especially given recent criticisms that the program is being subordinated by generative AI[170] and broader university hiring dynamics.[171] That policy also needs to learn the lessons from other countries that academic freedom is a core promise for, and crucial enabler of, research security. Such lessons should encourage government and the higher education sector to co-design these measures, rather than impose them by fiat.[172]

Both the sector and the government also need to work together to iron out issues around sharing information on the one hand, and what that information *means* on the other. For example, privacy laws currently prevent universities from informing other institutions about the result of their due diligence investigations or incidents.[173] This allows foreign agents and their proxies to attempt infiltration at multiple Australian universities (both physically and virtually) and increasing their likelihood of success and little risk of detection. Those same laws also prevent 'naming and shaming' individuals who might pose a risk to the sector; however, sharing with government agencies *is* permitted, thus situating bodies like the CFICC and NCFIC as perfect 'clearinghouses' for the sector about persons or entities posing high risk to research. The government could consider — as part of their broader *Privacy Act 1988* (Cth) reforms — including opportunities for the sector better identify and call-out threats.

Higher education researchers also need to become far more aware of the risks applying to their work, especially when they look for funding or opportunities overseas. At the same time, government can support researchers by increasing

[170] Juan Manuel Parrilla, 'ChatGPT Use Shows that the Grant-Application System is Broken' (2023) 623 *Nature* 423.

[171] Australian Council of Learned Academies, *Research Assessment in Australia: Evidence for Modernisation* (Report, 15 November 2023)

[172] Ross McLennan, 'Balancing Collaboration and Security: A High-Wire Challenge for Australia's Universities' (Speech, Australian Institute of International Affairs, 8 June 2021); Kirsten Lyons, 'Universities' Relevance Hinges on Academic Freedom', *The Conversation* (online, 3 June 2021) <https://theconversation.com/universities-relevance-hinges-on-academic-freedom-160346>.

[173] See, eg, Australian Privacy Principles 6.1(b), 6.2: *Privacy Act 1988* (Cth) sch 1 pt 6.

research funding and making it easier to apply for. The case studies in this paper demonstrate that researchers become especially vulnerable when they partner internationally but without regard for due diligence, a finding supported by the literature.[174]

Government intervention may not always be welcome, but it is also clear that the existing frameworks to support research security in a time of heightened geopolitical tensions do not always meet national interest objectives. To address contemporary threats to research security and the ability to respond to new and emerging threats (without unnecessary restrictions) a clear, robust, purposive and fit-for-purpose regulatory framework is required. Preferably, that framework should be adaptable, scalable and interoperable with the international countries with whom we align our values of transparency, openness, innovation and collaboration. If Australia intends to retain its position as a top-flight research environment, then the university sector needs to demonstrate that its collective protective security approach is to a standard that at least matches its US or European counterparts.

[174] Tania Babina et al, 'Cutting the Innovation Engine: How Federal Funding Shocks Affect University Patenting, Entrepreneurship, and Publications' (2023) 138(2) *Quarterly Journal of Economics* 895.