Securing Australia's Research: Strategies and Priorities

Sooryavansh Seewoosungkur

Norman Paterson School of International Affairs (NPSIA), Carleton University, Ottawa, Canada

sooryavanshseewoosun@cmail.carleton.ca

Sooryavansh, also known as Sasha, is a recent graduate of the Norman Paterson School of International Affairs (NPSIA). Through active engagement in international initiatives and experience in policy analysis across various professional endeavors, he has developed practical expertise in providing policy solutions in areas such as bilateral trade, research funding, cybersecurity, science and innovation, and sustainable development. Currently, he serves in the Government of Canada, where he supports international research collaborations and advances research policy priorities. Outside of these initiatives, he leads a team of researchers at a non-profit organization dedicated to advancing sustainable development policies in Canada, training them in qualitative research methods. In his leadership role, he collaborates closely with subject matter experts to develop actionable policy recommendations tailored to the needs of relevant stakeholders. His broad research interests include the weaknesses within Australia's research ecosystem due to foreign interference and insider threats targeting sensitive research, the impact of digital transformation on policy development, the role of AI in enhancing cybersecurity measures, and strategies for fostering international cooperation in science and technology.

Acknowledgements

Dr. Victor Munro

Canadian Insider Risk Management Centre of Excellence

Securing Australia's Research: Strategies and Priorities

Abstract: *With increasing global scientific cooperation, ensuring the integrity and security of research is vital for safeguarding national and economic interests. This study addresses the need for a robust Research Security (RS) framework in Australia, highlighting its current weaknesses compared to more established systems in Canada and the United States (US). The research begins by tracing the historical development of RS, from its origins during the Cold War to the contemporary challenges it addresses today, including foreign interference, and insider threats, which are exacerbated by Australia's fragmented and reactive RS approach. Using a criteria-based and case assessment method, the study (1) compares the RS approaches of Canada, the US, and Australia to derive policy conclusions for Canberra, and (2) evaluates incidents of research breaches in the three countries to identify Australia's vulnerabilities. Based on the findings, recommendations for developing a cohesive RS strategy in Australia are provided, including establishing a central RS authority, enhancing cybersecurity protocols in research institutions, conducting risk assessments for international research collaborations, and implementing comprehensive insider threat mitigation programs. These strategies aim to protect Australia's research assets and align its RS efforts with global best practices.*

Keywords: Research Security, National Security, Foreign Interference, Cybersecurity, Insider Threats, Research Funding, Espionage.

Introduction

In the rapidly evolving global landscape, marked by advancements in science and technology, the imperative to secure research has become a major concern for national security. The exposure and misuse of sensitive information, research findings, and technological innovations pose significant threats to a nation's economic health, defense capabilities, public safety, and international standing. This reality is reflected in academia and the broader innovation sector in Western nations, where the significance of Research Security (RS) is increasingly acknowledged. RS is centered on the development and implementation of policies and programs designed to protect sensitive research from being compromised, stolen, or released without authorization.[1] This concern is further amplified in areas of research with dual-use potential—that is, research that has the potential to be used for both beneficial and harmful purposes (civilian or military).[2] China, Russia, Iran, North Korea, and Saudi Arabia have been identified as active participants in efforts to exploit Western research for their geopolitical and military gains.[3]

Within this context, Australia faces several challenges, including foreign threats, internal weaknesses, and espionage activities. In contrast to its Five Eyes (FVEY) allies, Australia does not possess an RS policy to protect its research from these widespread threats. RS and knowledge security – important concepts in the international research community –

[1] "Research Security," The National Counterintelligence and Security Center, 2024, https://www.dni.gov/index.php/safeguarding-science/research-security?highlight=WyJzIiwiJ3MiXQ==.
[2] Walker-Munro, David Mount, and Ruby loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," TC Beirne School of Law Publications, n.d., 20.
[3] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 3.

are not recognized or explicitly defined within any policy framework.[4] Conversely, Canada and the United States (US) have implemented concerted efforts to defend their research.

Canberra's research sector is hindered by a fragmented approach and a lack of cohesive action, notably in its failure to act on the recommendations of the 2022 Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry, which sought to address national security risks affecting the Australian higher education (HE) and research sector. Moreover, Australia also faces internal challenges, such as insider threats—members within a research organization who could jeopardize security, either deliberately or accidentally.[5] The absence of an overarching RS policy and strategies to manage insider threats further exacerbates Australia's vulnerabilities.

The AUKUS agreement is a partnership among Australia, the United Kingdom (UK), and the US, which entails the transfer of sensitive military technology and collaborative research. According to the Australian Signals Directorate (ASD), Canberra is currently the most susceptible to exploitation, attributed to its inadequate cybersecurity and RS measures.[6]

Given the identified policy issues in Australia and the glaring weaknesses within the research ecosystem, this study will conduct a comparative analysis of RS practices in Australia, the US, and Canada to develop a comprehensive RS strategy for Australia. Through a criteria-based approach and case assessment, along with discussions on policy contrasts and an evaluation of RS programs and policies, the research will establish specific criteria to examine the RS frameworks of the involved countries. The findings will inform a discussion on policy recommendations for Australia, culminating in a proposed policy roadmap and RS strategy through a comparison of international best practices.

Brief History of RS

As Wilner et al. argue, post-1945, nations shifted their attention to safeguarding military technological advancements from foreign espionage, with a particular focus on nuclear and atomic technologies due to the presence of Soviet-aligned ideologists in the West, the expansion of the Soviet Union's military capacity, and the advent of 'Cold War' great power rivalry/competition.[7] In a bid to maintain its military and technological prowess, the US ensured that foreign researchers were closely monitored or outright restricted from entering the country through visa regulations.[8] This approach persisted until the disintegration of the Soviet Bloc.

The end of the Cold War introduced various non-military considerations into RS, such as economic factors, intellectual property (IP) theft, profit-making ventures, and international business competition.[9] These elements were driven by Research and Development (R&D) activities undertaken by private sector firms worldwide. Wilner et al. contend that the focus of state security efforts started to shift towards minimizing the economic impact of industrial

---

[4] Brendan Walker-Munro, "Australia Risks Falling Behind Allies on Research Security. Will It Take a Spy Scandal in Our Universities to Catch Up?," The Conversation, n.d., https://theconversation.com/australia-risks-falling-behind-allies-on-research-security-will-it-take-a-spy-scandal-in-our-universities-to-catch-up-221602.
[5] Happ, "Insider Threat Programs at Universities: A Necessary Reality," University of Texas, 2017, 46, https://www.utph.org/index/docs/Insider-Threat-Programs-at-Universities.pdf?language_id=1.
[6] Daniel Croft, "Australia the 'Weakest Link' in AUKUS on Cyber Security," Defence Connect, March 23, 2023, https://www.defenceconnect.com.au/intel-cyber/11670-australia-the-weakest-link-in-aukus-on-cyber-security.
[7] Alex Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," International Journal Canada S Journal of Global Policy Analysis 77, no. 1 (March 1, 2022): 28, https://doi.org/10.1177/00207020221118504.
[8] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 28.
[9] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 29.

espionage.[10] This shift broadened the threat landscape, moving beyond the US-Russia dyad to include China, India, and Germany – all seeking to enhance their major industries and develop economic stability.[11]

In the 2010s, the debate around safeguarding research while promoting open science gained prominence.[12] Presently, however, there seems to be a Cold War-like reversal in the RS landscape as China aggressively advances its military capabilities and economic power, positioning itself as a formidable challenger to the West.[13] Through strategic investments in emerging technologies such as autonomous systems, quantum computing, and artificial intelligence (AI), China aims to reshape the military balance in the Indo-Pacific region and beyond.[14] The US Department of Defense (DoD) highlights China's efforts to leverage these technologies to pioneer "intelligentized" warfare, a concept that integrates AI with military operations to create more effective and efficient combat strategies.[15] To accelerate advancements in these areas, China has been at the forefront of efforts to illicitly acquire foreign research to bolster its capabilities.[16]

Threat Landscape

Foreign Interference

Foreign interference in the context of research refers to actions by foreign entities that are coercive, clandestine, deceptive, or corrupting, aiming to improperly influence or access research activities and decisions to harm a nation's interests.[17] This can manifest as cyber attacks or through leveraging collaborations to illicitly obtain IP or sensitive data. Research institutions and grant administrators must thus remain updated on recent developments in research funding practices and international collaborations to mitigate risks.[18] Western research institutions currently face significant compliance challenges due to foreign interference, as noted in the "Brief History of RS" section, an issue that has gained prominence in academia following federal warnings about national government schemes to exploit research in Western nations. Since Xi Jinping assumed leadership in 2012, China has aimed to become a global leader economically and militarily, transitioning from a manufacturing-based economy to one focused on innovation.[19] This strategy includes

---

[10] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 29.
[11] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 29.
[12] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 29.
[13] CFR Editors, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," Council on Foreign Relations, November 4, 2021, 1, https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape.
[14] CFR Editors, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," 1.
[15] CFR Editors, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," 1.
[16] Gordon Long and The MITRE Corporation, "Fundamental Research Security," December 6, 2019, 9, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.
[17] Public Safety Canada, "Protecting Your Research and Intellectual Property," April 9, 2024, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/prp-en.aspx.
[18] Tammy F. Chu, "The Complex Challenge of Foreign Interference in Research Administration and Compliance.," Research Management Review 24, no. 1 (January 1, 2020): 2, https://files.eric.ed.gov/fulltext/EJ1253140.pdf.
[19] Chu, "The Complex Challenge of Foreign Interference in Research Administration and Compliance.," 3.

targeting and exploiting Western universities/research institutions that are crucial for scientific and technological progress.[20]

It should be noted that not all efforts by countries with differing political alignments or foreign policies to extend their research collaborations are seen as malicious. 'Legitimacy-bearing' activities include government lobbying, paid media opportunities, organizing cultural and educational exchanges, and visitor programs.[21] Nonetheless, Western intelligence and security agencies are alarmed by what they perceive as China's increased efforts to influence and access Western-led research through methods that fall outside these norms.[22] Examples include "enlisting students and visiting scholars to divert IP from confidential grant applications, implanting spies under the guise of collaboration for research, incentivizing scientists to operate 'shadow laboratories' in China, and using talent recruitment programs to compel researchers to misappropriate IP for personal benefits."[23]

Insider Threats

Carnegie Mellon defines an insider threat as the "potential for individuals with authorized access to an organization's critical assets to use their access, maliciously or unintentionally, in ways that could negatively impact the organization, while insider risk refers to the impact and likelihood of such threats becoming reality."[24] Methods used by insider threats often include unauthorized data transfer, IP theft, misuse of sensitive research findings, sabotage of research processes, and manipulation of academic or administrative systems to alter data or outcomes. These threats can manifest through actions such as copying research data onto unauthorized devices, collaborating with external entities to share proprietary information, or deliberately compromising research integrity for personal gain. Such challenges are pronounced in universities due to the autonomy of academic staff and a culture that values open access.[25] It is therefore crucial for these institutions to develop safeguards against such threats, despite the highly evident conflict with the principle of free academic exchange. Current analysis indicates that about 70% of these threats are intentional, highlighting the importance of universities and research institutions implementing strong insider threat programs to safeguard their integrity and contributions to innovation.[26] Failing to address this can result in the loss of valuable data, long-lasting harm to a university's reputation and trust, and, more severely, a threat to national security. Data privacy expert Jason du Preez has pointed out the extensive economic losses and trust erosion these threats can cause, affecting not only the academic and government communities but civilians in general.[27] Research-intensive universities part of the U15 in Canada, the Association of American Universities (AAU), and the Group of 8 in Australia are particularly vulnerable to nefarious insiders. In his analysis, Happ discusses many examples, including the case of Thomas Jefferson University in the US, where employees transferred cancer research

[20] Chu, "The Complex Challenge of Foreign Interference in Research Administration and Compliance.," 3.
[21] Chu, "The Complex Challenge of Foreign Interference in Research Administration and Compliance.," 3.
[22] Chu, "The Complex Challenge of Foreign Interference in Research Administration and Compliance.," 4.
[23] "China's Influence & American Interests: Promoting Constructive Vigilance," Hoover Institution, n.d., https://www.hoover.org/research/chinas-influence-american-interests-promoting-constructive-vigilance.
[24] "CERT Definition of 'Insider Threat' - Updated," SEI Blog, March 7, 2017, https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/.
[25] Happ, "Insider Threat Programs at Universities: A Necessary Reality," 46.
[26] Happ, "Insider Threat Programs at Universities: A Necessary Reality," 47.
[27] Happ, "Insider Threat Programs at Universities: A Necessary Reality," 47.

findings to the University of Manchester.[28] Further examples related to research are discussed in the following sections, notably in the case assessment.

Intersections (Foreign-Influenced Insiders)

Foreign states often attempt to recruit insiders within organizations to gain access to sensitive information or IP.[29] Wilner et al. highlight that this issue is particularly prevalent in military-oriented research but extends beyond it due to the increase in sensitive research areas and methodologies.[30] Foreign funding programs and lucrative collaborative agreements serve as tools to influence domestic researchers, thereby amplifying insider risks within research institutes benefiting from foreign financial support. In such scenarios, financial mechanisms serve as strong leverage. Further, in Western nations, notably more pronounced in Australia, research institutions and universities host a significant number of international student researchers who are susceptible to being profoundly influenced by appeals to patriotism or threats to personal or family safety, driving them to pose insider threats by gathering information for the benefit of their home countries.[31] The methods for collecting information can range from direct theft to subtler strategies that exploit the collaborative spirit of academia. The Australian Department of Home Affairs has flagged the recruitment of insiders by foreign intelligence services as a significant threat, particularly to research institutions in light of AUKUS.[32] To this note, Confucius Institutes, which were established by China to foster cultural and educational exchanges, have attracted global scrutiny.[33] Despite their intended purpose, these institutes have faced criticism for potentially serving as conduits for Chinese governmental influence, sparking debates over academic freedom and IP theft.[34] The response of such institutes has been to adapt rather than to cease efforts, engaging in new forms of collaboration, such as research partnerships with Western academic institutions.[35] Their integration into various campuses in Australia in the form of "Centres of Excellence" and active participation in research teams has increased concerns about long-term insider threats.[36]

Analysis: The Contrasting Approaches of Canada, the US and Australia

This section details the different contemporary RS strategies, allowing for a contextualized comparison useful for drawing insightful policy lessons for Australia.

Canada

[28] Happ, "Insider Threat Programs at Universities: A Necessary Reality," 47.
[29] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 32.
[30] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 33.
[31] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 33.
[32] "Department of Home Affairs Website," Department of Home Affairs Website, n.d., https://www.homeaffairs.gov.au/.
[33] Tory Shepherd, "University Students and Staff Face Increasing Threats, Foreign Interference Inquiry Finds," The Guardian, March 25, 2022, https://www.theguardian.com/australia-news/2022/mar/25/university-students-and-staff-face-increasing-threats-foreign-interference-inquiry-finds.
[34] Lee Edwards, "Confucius Institutes: China's Trojan Horse | the Heritage Foundation," The Heritage Foundation, n.d., https://www.heritage.org/homeland-security/commentary/confucius-institutes-chinas-trojan-horse.
[35] Shepherd, "University Students and Staff Face Increasing Threats, Foreign Interference Inquiry Finds."
[36] Shepherd, "University Students and Staff Face Increasing Threats, Foreign Interference Inquiry Finds."

Canada's recent advancements in research—through a combination of advanced technologies, a skilled workforce, and an open academic culture—have alerted federal authorities and security agencies to potential vulnerabilities to international espionage and insider threats.[37] The 2018 arrest of Huawei executive Meng Wanzhou by Canada, leading to China's detention of Canadians Michael Kovrig and Michael Spavor, heightened Canada's intelligence community's threat awareness, notably revolving around economic and security risks from China, with further retaliatory actions anticipated.[38] These concerns extended to research due to the large presence of foreign academics in Canada, namely from China, leading to the creation of a Universities Working Group. Composed of the U15 Group of Canadian Research Universities, Public Safety Canada, Global Affairs Canada, Innovation, Science and Economic Development Canada (ISED), and other federal bodies, including research funding agencies—namely, the Social Sciences and Humanities Research Council of Canada (SSHRC), the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canadian Institutes of Health Research (CIHR), and the Canada Foundation for Innovation (CFI)—the group sought to develop guidelines that balance research openness with protection against espionage and foreign threats.[39]

During COVID-19, Canada's research vulnerabilities were further highlighted. The increased targeting of health research, with Canada being a leader in health and biotechnology, prompted the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) to echo the heightened risks of IP theft and data breaches, especially from cyber attacks.[40] In 2021, ISED launched the National Security Guidelines for Research Partnerships (NSGRP) as a response to these ongoing security concerns. The policy assists the aforementioned research funders, institutions, and researchers in evaluating national security risks throughout the grant application and research development process, with specific attention to partnerships with the private sector and collaborations in sensitive research areas such as biotechnology and quantum computing.[41]Any grant proposal that includes a research partner (such as private sector bodies, industry organizations, producer groups, or foreign entities) is required to submit a completed Risk Assessment Form when applying for funding that mandates the application of the NSGRP, especially for research involving sensitive areas.[42] This can include research partner organizations from the public and/or not-for-profit sectors. The risk assessment form requires information on the research and the partners involved.[43] Applicants are also expected to develop and execute a risk mitigation plan to address the identified risks within the grant

---

[37] Innovation, Science and Economic Development Canada, "Research Security Policy Statement – Spring 2021," Canada.Ca, March 24, 2021, https://www.canada.ca/en/innovation-science-economic-development/news/2021/03/research-security-policy-statement--spring-2021.html.

[38] Brian Owens, "A New Era of Research Security — University Affairs," University Affairs, June 14, 2023, https://universityaffairs.ca/features/feature-article/a-new-era-of-research-security/.

[39] Owens, "A New Era of Research Security — University Affairs."

[40] Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch and Communications and Marketing Branch, "Policy Statements," January 16, 2024, https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/policy-statements.

[41] Owens, "A New Era of Research Security — University Affairs."

[42] Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch and Communications and Marketing Branch, "National Security Guidelines for Research Partnerships," October 6, 2022, 9, https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships.

[43] Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch and Communications and Marketing Branch, "National Security Guidelines for Research Partnerships," October 6, 2022, 9.

duration.[44] The NSGRP was tested when the NSERC Alliance Grants applications were subjected to rigorous security checks, resulting in the rejection of several scrutinized proposals — this translated to approximately 4% of over a thousand submissions.[45]

Against this backdrop, in January 2024, the Canadian government introduced the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC) to further protect Canadian research. This new policy mandates that grant proposals submitted to SSHRC, NSERC, CIHR, and the CFI must confirm that no team member/researcher or institution involved has ties to, or receives support from, foreign entities linked to military, national defense, or security sectors that threaten Canada's national security.[46] The STRAC policy consists of two lists: Sensitive Technology Research Areas and Named Research Organizations. The former list emphasizes sensitive fields like AI, aerospace, medical technology, quantum science, and robotics whereas the latter details 105 Russian, Chinese, and Iranian organizations and universities that pose a high risk to Canada's national security.[47] As a key rule, researchers associated with these named organizations will be subject to funding restrictions in these sensitive fields.[48] In this context, researchers are defined as "applicants, co-applicants, collaborators, and highly qualified personnel, including undergraduate and graduate students, post-doctoral fellows, and research staff seeking funding from federal granting councils." [49]

If a researcher provides false information in the attestation for STRAC and NSGRP, it will lead to an investigation under the Tri-Agency Framework: Responsible Conduct of Research.[50] This can result in sanctions, including termination of the grant and barring from future funding opportunities, among other major consequences.[51]

US

Washington has intensified its approach to addressing foreign interference and insider threats within the research ecosystem. Launched in January 2021 under the Trump Administration, National Security Presidential Memorandum 33 (NSPM-33) introduced a clear and specific policy direction.[52] It mandated rigorous efforts to secure American research initiatives, assigning the Office of Science and Technology Policy (OSTP) the role of spearheading the creation of RS policy frameworks. Supported by OSTP, NSPM-33 enhances

---

[44] Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch and Communications and Marketing Branch, "National Security Guidelines for Research Partnerships," October 6, 2022, 8.

[45] Joe Friesen, "Two-thirds of Research-grant Requests Sent to Canadian Security Agencies Rejected," The Globe and Mail, January 26, 2023, https://www.theglobeandmail.com/canada/article-nserc-research-grants-sensitive/.

[46] "Policy on Sensitive Technology Research and Affiliations of Concern," May 9, 2024, 4, https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern.

[47] "Policy on Sensitive Technology Research and Affiliations of Concern," 4.

[48] Chloe Rivest, "Canada's Research Revolution: Analyzing the STRAC Policy and Its Implications — McGill Policy Association," McGill Policy Association, March 8, 2024, https://mcgillpolicyassociation.com/latest-articles/2024/3/8/canadas-research-revolution-analyzing-the-strac-policy-and-its-implications.

[49] Rivest, "Canada's Research Revolution: Analyzing the STRAC Policy and Its Implications — McGill Policy Association."

[50] "Policy on Sensitive Technology Research and Affiliations of Concern," 8.

[51] "Policy on Sensitive Technology Research and Affiliations of Concern," 8.

[52] CSET, "A New Institutional Approach to Research Security in the United States | Center for Security and Emerging Technology," Center for Security and Emerging Technology, June 9, 2023, 4, https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states.

collaboration and openness among federal entities, fosters increased sharing of information, and heightens the awareness of potentially vulnerable institutions and researchers. The Biden Administration has robustly endorsed NSPM-33, with a focus on four main areas: "requirements for disclosure; involvement in foreign talent recruitment programs; RS educational and programmatic obligations; and risk evaluation."[53]

In line with NSPM-33, disclosure practices have become a focal point in the allocation of research funds, requiring full transparency from funding candidates about all resources available for their research, including domestic and international, along with various forms of monetary support.[54] This approach has significantly influenced how grants are awarded by the National Science Foundation (NSF) and other granting agencies, which now require the inclusion of two mandatory forms in all funding applications: the Biographical Sketch Common Form and the Current and Pending (Other) Support Common Form.[55] The OTSP has maintained continuous oversight in the development of these forms. Applicants are also required to disclose their involvement in any foreign talent recruitment programs.[56] Beyond this, the NSF has continued to invest considerable resources into collaborating with the research community to provide researchers with information and tools to safeguard their projects and promote a culture of transparency and practices that uphold research integrity.[57] Other granting agencies such as the National Institutes of Health (NIH) have pursued similar programs.

It should also be noted that NSPM-33 introduces specific requirements for RS education and training. Section 4 (f) mandates that agencies offer training for federal employees involved in R&D or in distributing R&D funds.[58] It incorporates a variety of topics, including the threats to the US R&D framework and the signs and behaviors that could signify that an individual poses an insider threat to the research institution where they are employed, such as unusual requests for access to sensitive information, unexplained affluence or financial troubles, extensive use of unauthorized devices or networks, attempts to bypass security protocols, reluctance to report travel or foreign contacts, and abnormal work hours or patterns.[59] In addition, institutions receiving over $50 million in federal science and engineering grants annually must certify that they have established an RS program.[60]

Australia

Major concerns among allies, the Australian national security community, and academia have intensified over the potential misappropriation of Australian-funded research by China or its use in ways that conflict with Australian academic values. This issue is particularly pressing given the notable involvement of Australian academics in Chinese talent programs.[61] Australia's geographical proximity and economic reliance on China has facilitated significant collaborations between Australian institutions and those linked to the

---

[53] Melissa Flagg and Zachary Arnold, "A New Institutional Approach to Research Security in the United States: Defending a Diverse R&Amp;D Ecosystem," January 1, 2021, 1, https://doi.org/10.51593/20200051.
[54] Flagg and Arnold, "A New Institutional Approach to Research Security in the United States: Defending a Diverse R&Amp;D Ecosystem," 2.
[55] "NSPM-33-Implementation-Guidance" (National Science and Technology Council, 2021), 3, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.
[56] "NSPM-33-Implementation-Guidance," 3.
[57] "Research Security," NSF - National Science Foundation, n.d., https://new.nsf.gov/research-security.
[58] Emily G. Blevins and Marcy E. Gallo, "Research Security Policies: An Overview" (Congressional Research Service, 2022), 2, https://crsreports.congress.gov/product/pdf/IF/IF12589.
[59] Blevins and Gallo, "Research Security Policies: An Overview," 2.
[60] Blevins and Gallo, "Research Security Policies: An Overview," 2.
[61] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 39.

People's Liberation Army (PLA).[62] Unlike many of its allies, Australia has not implemented robust programs to protect sensitive research, relying instead on a few blunt regulatory measures without a clear public policy, leaving the research sector vulnerable to national security threats.

While Canberra does not explicitly recognize or define RS through a formal public policy—a major deficiency—it has made some attempts to address contemporary threats to research, albeit limited. In 2019, the University Foreign Interference Taskforce (UFIT) was established as a partnership between the Australian government and universities to address and mitigate the risks of foreign interference within the Australian HE sector.[63] Under UFIT, various Guidelines to Counter Foreign Interference were last included in 2021, offering important considerations for universities to review their threat landscape and ensure that foreign interference is addressed. The guidelines have four key pillars: 1) governance and risk frameworks, 2) communication, education, and knowledge sharing, 3) due diligence, risk assessments, and management, and 4) cybersecurity.[64] However, they have been criticized for not being specific or regularly updated to address the rapidly evolving landscape of threats and for predominantly delegating the responsibility for monitoring national security risks to individual universities.[65] In comparison to its international counterparts, they also fail to include important areas of vulnerability, including research partnerships with foreign actors and deliberate acts of espionage targeting staff.[66]Additionally, the effectiveness of the guidelines is undermined by their non-mandatory adoption across universities.[67]

The Australian Research Council (ARC), as the principal funding body for university research, administers most of the government's investment in this area through the National Competitive Grants Program (NCGP).[68] It has recently developed a definition and approach to RS and risk mitigation. This includes a review of funding applications with considerations for current or recent foreign financial support, education or research-related activities, involvement in a foreign talent program, obligations to a foreign university, associations with a foreign government, military, policing, or intelligence organization, and associations with entities under Australian sanctions.[69] Other key research organizations and funders, such as the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and the National Health and Medical Research Council (NHMRC), have not implemented comparable initiatives. However, upon reviewing ARC's framework, it is also unclear how those reviews are conducted and how researchers are mandated to attest to their affiliations or involvement with entities that may pose national security risks. Additionally, similar to UFIT, ARC places a large amount of responsibility for assessing risks on researchers and universities without providing a centralized strategy for protection against such risks. A more concerning issue is that a substantial portion of Australian university research, up to almost 70 percent, is self-funded, primarily through international student enrollments and

---

[62] Wilner et al., "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions," 39.
[63] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 4.
[64] "Guidelines to Counter Foreign Interference in the Australian University Sector," Department of Education, 2019, https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector.
[65]Brendan Walker-Munro, "Submission to the Department of Education Interim Report on the Universities Accord," 2023, 5, https://www.education.gov.au/system/files/2023-08/AUA_inter_tranche3_040%20Brendan%20Walker-Munro.pdf.
[66]Walker-Munro, "Submission to the Department of Education Interim Report on the Universities Accord," 5.
[67] Walker-Munro, Mount, and Loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 4.
[68] "Australia Research Council," n.d., https://www.arc.gov.au/find-information.
[69] "Australia Research Council – Research Security,"n.d., https://www.arc.gov.au/funding-research/research-security.

international agreements, with the ARC or other funders catering to the remaining 30-40 percent; a starkly low number compared to Canada's funding structures, where federal granting agencies provide the primary source of funds.[70] This instability not only affects the financial health of institutions but also increases Canberra's susceptibility to foreign influence, as universities may become reliant on foreign partnerships.[71]

The most recent attempt to rectify the aforementioned gaps—the 2022 PJCIS Inquiry—highlighted significant foreign interference and coercive practices in Australia's research and HE sector. Yet, most of its proposed recommendations have not been enforced. For example, the Australian Security Intelligence Organisation (ASIO) declined a proposal from the PJCIS that involved sharing details of its activities and work related to protecting HE institutions.[72] Following this, ASIO published a pamphlet titled "Collaborate with Care: Protect Your Research," aimed at assisting research institutions that often struggle to fulfill their security obligations.[73] Relying solely on this measure is highly inadequate. Other key recommendations that remain unimplemented include: "an examination of the contract between Monash University and the Commercial Aircraft Corporation of China (COMAC), a state-owned enterprise connected to the PLA; UFIT assisting universities in introducing, maintaining, and developing relevant training on national security issues for staff and students by employing an accountable authority responsible for managing foreign interference risks at their institution; and the Department of Education, Skills and Employment undertaking a risk-based review of ARC grants from the last ten years to assess the risks linked to involvement in talent acquisition programs like the Thousand Talents of the CCP." [74]A number of the over three thousand research agreements between China and Australia are deemed to constitute serious threats to national security further evidencing the need to reconsider the PJCIS recommendations.[75]

Furthermore, the Australian Strategic Policy Institute (ASPI) has identified Shanghai Jiao Tong University (SJTU) and Tianjin University (TJU) as presenting a 'high-risk' due to their substantial ties with China's civil-military fusion initiatives and direct connections to the PLA.[76] This includes links to PLA's Unit 61398, known for cyber espionage activities.[77] Both universities have previously partnered with Australian institutions such as the University of Adelaide.[78] The risk associated with TJU is further highlighted by the arrest of

---

[70] Walker-Munro, "Why Isn't Australia Securing Its Critical Research?," EduResearch Matters, January 17, 2024, https://blog.aare.edu.au/why-isnt-australia-securing-its-critical-research/.

[71] Sherryn Groch Daniella White, "Australia Underspends on This Key Area. It May Put National Security at Risk," The Sydney Morning Herald, November 20, 2023, https://www.smh.com.au/education/australia-underspends-on-this-key-area-it-may-put-national-security-at-risk-20231111-p5ej93.html.

[72] Tom Ravlic, "ASIO Opposes Publication of Its University Monitoring Activities," The Mandarin, February 16, 2023, https://www.themandarin.com.au/212476-asio-opposes-publication-of-its-university-monitoring-activities/.

[73] Walker-Munro, "Why Isn't Australia Securing Its Critical Research?"

[74] "PJCIS List of Recommendations," Parliament of Australia, 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report/section?id=committees%2Freportjnt%2F024611%2F75668.

[75] Walker-Munro, "Australia Risks Falling Behind Allies on Research Security. Will It Take a Spy Scandal in Our Universities to Catch Up?"

[76] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 15.

[77] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 16.

[78] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 15.

three TJU-affiliated professors in the US for allegedly stealing semiconductor and opto-electronics information.[79]

Another major issue recently highlighted by Australian universities is foreign government interference on campus, with concerns about intimidation by pro-China groups and the Chinese government against those critical of the Chinese Communist Party (CCP).[80] A 2021 Human Rights Watch report indicated that Chinese government surveillance and harassment from pro-China groups targeted students from Hong Kong and China in Australian universities, claims which the Chinese Embassy in Canberra denied.[81] In some instances, it has been reported that Chinese authorities visited students' families in China to discuss the activities of the students on Australian campuses, especially if they had expressed criticism of the Chinese government.[82] Other countries, including Iran, have also been accused of "transnational" intimidation on Australian campuses, though these allegations have not yet elicited any public responses.[83] These incidents have broader implications on research, as they may deter academic freedom, lead to coerced or influenced students compromising their research, either by altering findings to avoid political repercussions or by sharing sensitive information with foreign entities, and create an atmosphere of fear and self-censorship among researchers.

Policy and Programs Evaluation: Criteria and Case Assessment

This section evaluates the RS approaches of Canada, the US, and Australia, based on a well-defined set of criteria, which includes governance, transparency, risk management, training, collaboration, funding practices, insider threat mitigation, and defense against foreign interference (See Figures 1-3 Below). These criteria will serve as the foundation for assessing the RS policies and applying a scoring system (See Table 1).

[79] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 15.
[80] John Power, "Chinese Students in Australian Universities Face Surveillance, Intimidation by Beijing for Views: Rights Group," South China Morning Post, July 2, 2021, https://www.scmp.com/week-asia/politics/article/3139289/chinese-students-australia-face-surveillance-intimidation-views.
[81] Phil Mercer, "Australian University Warns of Foreign Interference on Campus," Voice of America, August 16, 2023, https://www.voanews.com/a/australian-university-warns-of-foreign-interference-on-campus-/7227177.html.
[82] Power, "Chinese Students in Australian Universities Face Surveillance, Intimidation by Beijing for Views: Rights Group."
[83] Mercer, "Australian University Warns of Foreign Interference on Campus."

Criteria	Australia
Governance: Evaluates the existence of centralized, organized policies and frameworks governing RS, including the extent to which these policies are enforced and monitored.	The absence of a well-defined public policy on RS has resulted in uneven policy stances across the sector. While the UFIT brings together leaders from the university sector and Australian government bodies to foster a secure and resilient setting against external threats in universities, the PJCIS has pinpointed shortcomings in its organization and coordination. Additionally, it highlighted the lack of current strategies, the absence of effective implementation procedures, and insufficient monitoring of universities' compliance with these guidelines.
Risk Management & Transparency: Evaluates the strategies and mechanisms for identifying, assessing, and addressing risks associated with RS, such as insider threats and foreign interference, while also reviewing the obligations of researchers and institutions to report sources of research funding, affiliations, and any foreign involvement	A dispersed model has been adopted where each university is in charge of overseeing national security risks, leading to inconsistency in effectiveness. Yet, when evaluating research proposals, the ARC assesses potential threats, particularly for projects related to technologies identified in the Blueprint for Critical Technologies — it outlines the measures being implemented to advance and safeguard vital technology in the pursuit of the nation's best interests. Such reviews also cover a variety of other risk indicators mentioned in the previous section.
Training & Awareness: Measures the efforts to educate and inform researchers, administrative staff, and relevant stakeholders about RS risks, best practices, and compliance requirements.	Efforts such as the "Collaborate with Care" booklet aim to uplift security awareness, but overall effectiveness and reach remain limited.
Funding Practices: Considers the funding mechanisms for research, the stability of these funds, and how funding policies influence RS and the potential for foreign influence.	ARC being the main research funder poses several challenges for Australia's R&D landscape. Critical issues include underinvestment in R&D compared to allies, a decline in real-term funding for ARC and the NHMRC, and a heavy reliance on universities for some of the costs of research. This scenario places immense pressure on university budgets, leading to a situation where universities must cover a significant portion of their R&D spending from their own funds. The need for alternative revenue streams can drive universities to seek out foreign investments and partnerships that could prove to be harmful.
Insider Risk & Mitigation: Examines the strategies and measures in place to detect, prevent, and respond to threats posed by insiders who may compromise research integrity or security.	The strategy to address insider threats within research is not comprehensive or sector-wide, instead relying on measures at the university level that might vary in effectiveness. Australia's government has put into place the Protective Security Policy Framework (PSPF), which incorporates four tiers of vetting processes as a key component of its strategy to mitigate insider threats. This framework aims to create uniform and improved vetting procedures throughout the critical infrastructure sector, particularly for staff members, including those involved in the supply chain. The Australian government has also released "Countering the Insider Threat: A guide for Australian Government." However, the application of these strategies within the research domain is insufficient. The absence of explicit guidelines for mitigating insider threats in research environments points to a significant oversight. This gap is alarming and suggests an area where Australia's national security and research integrity policies could be strengthened. UFIT does not include many references to insider threats within its guidelines.
Foreign Interference: Assesses the robustness of policies and actions taken to prevent and counteract attempts by foreign entities to influence, interfere with, or steal intellectual property from research institutions.	Existing measures include the Guidelines to Counter Foreign Interference under UFIT. This initiative has developed comprehensive guidelines aimed at identifying and mitigating risks associated with foreign interference in academia. However, the guidelines themselves are inadequate in several aspects and do not address national security risks effectively, as discussed in the previous section and further ahead. The primary responsibility to address foreign interference is delegated to universities.

Figure 1: Criteria-based Assessment – Australia

Criteria	US
Governance: Evaluates the existence of centralized, organized policies and frameworks governing RS, including the extent to which these policies are enforced and monitored.	The implementation of NSPM-33 facilitates centralized governance by prioritizing collaboration and information exchange between federal agencies and institutions. The US has implemented inter-agency collaboration for RS through the OSTP and the Subcommittee on RS of the National Science and Technology Council (NSTC). This subcommittee is responsible for leading the Administration's efforts and supervising RS practices in funding agencies and institutions. This entails the formulation of norms and guidelines pertaining to the transparency and management of conflicts of interest. In 2024, the OSTP set forth guidelines to assist federal granting agencies in evaluating potential research proposals through common disclosure forms, aiming to identify conflicts of interest and potential threats, alongside guidelines for engagement with foreign talent recruitment programs to mitigate national security risks.
Risk Management & Transparency: Evaluates the strategies and mechanisms for identifying, assessing, and addressing risks associated with RS, such as insider threats and foreign interference, while also reviewing the obligations of researchers and institutions to report sources of research funding, affiliations, and any foreign involvement	Focuses on the assessment and handling of risks, especially as outlined by NSPM-33, which prohibits participation in high risk foreign talent initiatives and outlines steps for risk reduction. To adhere to NSPM-33, institutions are implementing various strategies to ensure they meet these guidelines. This includes revising policies to make disclosure expectations clear, creating online platforms for disclosure management, and introducing new protocols for reporting foreign ties. Such disclosures are crucial for identifying and addressing risks linked to foreign agreements and relationships. For instance, Emory University has established a system to manage disclosures of foreign affiliations via its Research Compliance and Regulatory Affairs office. There is a push for complete transparency regarding both financial and non-financial support, encompassing foreign connections and involvement in foreign talent recruitment efforts. The NSF, among other grantors, is transitioning to uniform formats for revealing potential conflicts of interest and commitments. This initiative is part of a larger movement spearheaded by the OSTP to unify disclosure norms across all federal agencies that fund scientific research.
Training & Awareness: Measures the efforts to educate and inform researchers, administrative staff, and relevant stakeholders about RS risks, best practices, and compliance requirements.	NSPM-33 has clear directives for RS training for federal personnel and strict requirements for research institutions to establish RS programs.
Funding Practices: Considers the funding mechanisms for research, the stability of these funds, and how funding policies influence RS and the potential for foreign influence.	NSPM-33 reinforces the need for research organizations receiving substantial federal R&D funding to maintain appropriate RS programs, aligning financial support with security standards. US federal funding agencies have followed through by developing stringent funding policies that account for potential threats to research.
Insider Risk & Mitigation: Examines the strategies and measures in place to detect, prevent, and respond to threats posed by insiders who may compromise research integrity or security.	The National Institute of Health (NIH), NSF and NSPM-33 enforce transparency in disclosing all sources of support and conflicts of interest directly targeting the identification of potential insider threats by making visible the external influences and commitments of researchers. Ongoing monitoring strategies, such as the development of 'flags' for audits and post-travel questionnaires enforced by the NIH and NSF, are practical methods for detecting behavior or circumstances indicative of insider threats. NSPM-33 also has specific clauses related to insider threats (further discussed in the analysis section below).
Foreign Interference: Assesses the robustness of policies and actions taken to prevent and counteract attempts by foreign entities to influence, interfere with, or steal intellectual property from research institutions.	The US has taken aggressive steps to prevent foreign interference in research, particularly from China, through strict policies and clauses in NSPM-33 The NSTC, as mandated by NSPM-33, leads nationwide initiatives to oversee the challenges of foreign interference vis-a-vis research.

Figure 2: Criteria-based Assessment - US

Criteria	Canada
Governance: Evaluates the existence of centralized, organized policies and frameworks governing RS, including the extent to which these policies are enforced and monitored.	Ottawa has established specific policies on RS and created a specialized team, known as the University Working Group, to focus on developing and implementing these policies. This group brings together leading research funding organizations, national security agencies, and representatives from Canadian universities. Between the start of 2020 and January 2024, the Canadian government initiated an awareness campaign about threats, introduced the NSGRP, started a pilot with the NSERC, allocated funds in the 2022 budget for RS-related roles, and formulated the STRAC policy. Canada also launched the RS Centre, supported by a dedicated RS fund, to bolster the nation's ability to protect research activities, utilizing a network of regional advisors and a main hub in Ottawa.
Risk Management & Transparency: Evaluates the strategies and mechanisms for identifying, assessing, and addressing risks associated with RS, such as insider threats and foreign interference, while also reviewing the obligations of researchers and institutions to report sources of research funding, affiliations, and any foreign involvement	NSGRP involves the utilization of attestation forms for assessing risks and strategies for their mitigation. It is compulsory to report any financial or material support received from abroad, connections with foreign entities, and involvement in talent initiatives sponsored by foreign governments when applying for research grants.
Training & Awareness: Measures the efforts to educate and inform researchers, administrative staff, and relevant stakeholders about RS risks, best practices, and compliance requirements.	The national establishment of guidelines aims to increase awareness among researchers and institutions. Canada has developed three publicly available courses on RS, among other training initiatives, and universities have established specialized offices dedicated to RS, accompanied by RS directors. They ensure that researchers are adhering to federal policies on RS.
Funding Practices: Considers the funding mechanisms for research, the stability of these funds, and how funding policies influence RS and the potential for foreign influence.	Strong federal funding and investment, along with specific policies developed by the Tri-Councils and the CFI, aim to protect sensitive research areas and prevent funding from being allocated to research that may pose a national security threat to Canada.
Insider Risk & Mitigation: Examines the strategies and measures in place to detect, prevent, and respond to threats posed by insiders who may compromise research integrity or security.	The detailed disclosure mandates and dual-phase verification procedure for grant submissions outlined by STRAC act as preventative actions to reduce insider threats. This is done by identifying and efficiently managing researchers or institutions that may have potential conflicts of interest and pose a threat to national security. The threat briefing and research safeguarding checklist/toolkit provided by CSIS specifically address the risks posed by insiders. This briefing highlights the potential risks posed by individuals within a research team or institution who have access to confidential or proprietary information. These individuals may act independently or be influenced, assisted, or coerced by external entities to acquire or misuse research data.
Foreign Interference: Assesses the robustness of policies and actions taken to prevent and counteract attempts by foreign entities to influence, interfere with, or steal intellectual property from research institutions.	Guidelines and policies reflect a strong stance against foreign interference, with specific actions against institutions and actors linked to adversarial state actors. Canada's approach includes listing over 100 institutions associated with foreign military or state security entities considered high risk, directly addressing concerns of foreign interference in sensitive research areas.

Figure 3: Criteria-based Assessment – Canada

The scoring system employs a scale from 1 to 5, where:

- 1: Indicates a very poor approach—minimal or ineffective policies in place, lacking structure and coherence.
- 2: Denotes a poor approach, reflecting some efforts toward addressing the criterion, but with significant gaps or inefficiencies that hinder overall capacity to fulfill the requirements of the criterion.
- 3: Represents a moderate approach: a somewhat effective strategic approach with considerable room for improvement, often marked by inconsistent implementation or partial coverage.

- 4: The approach is backed by strong policies and practices with some shortcomings. These policies are generally effective but may have areas that require fine-tuning or better enforcement, or their effectiveness might not be fully determined due to the relative recency of the policies and programs.
- 5: A comprehensive strategy that addresses the criterion efficiently, with policies and programs covering a wide variety of factors contributing to the goal of securing research.
    - Note that a score of 5 does not imply perfection; it demonstrates the current efforts and policy robustness in the nation's capacity to address the criteria.

Criteria	**Canada**	**US**	**Australia**
Governance	4	5	2
Risk Management & Transparency	4	4	3
Training & Awareness	4	5	2
Funding Practices	5	4	2
Insider Threat & Mitigation	3	4	2
Foreign Interference	4	4	3
Total	**24/30**	**26/30**	**14/30**

Table 1: Scoring System

Following the initial assessment above, the investigation continues with a detailed case evaluation spanning from 2012 to 2024. This period has seen a notable increase in efforts to safeguard research through various policies, both governmental and institutional, although not always formally linked to RS policy frameworks developed by governments, as some of these frameworks are relatively new. Simultaneously, there has been a rise in attempts by malicious actors to exploit Western research. The focus of the cases is on instances of breaches or malicious operations aimed at compromising research at various research institutions, defined for the purposes of this study as "a university, college, laboratory, government agency, corporation, not-for-profit organization, or other entity within the public or private sphere with the stated mission or mandate of supporting research." [84] Each case is categorized based on the type of threat it represents—be it foreign interference, insider risk, or a combination of both. The investigation examines these incidents through a selection of 23 cases from Canada, the US, and Australia. Overall, the case assessment aims to uncover vulnerabilities within these research institutions to draw conclusions relevant to RS policy and evaluate the effectiveness and resilience of each country's or institution's measures. Annex A presents the case assessment framework used for evaluating the cases, while Annex B provides the set of cases (dataset).

[84] "Research Institution Definition: 147 Samples | Law Insider," Law Insider, n.d., https://www.lawinsider.com/dictionary/research-institution.

This method encountered several limitations. Firstly, there was no comprehensive database for such incidents; the cases were compiled from various media websites. Secondly, there was a noticeable scarcity of Canadian cases in the media compared to those from the US and Australia. This disparity potentially reflects a lack of transparency in post-incident resolutions in Canada, which hindered the study's initial aim of achieving an equitable case distribution among the three countries. The relatively low number of cases impeded the investigation overall; obtaining 50 or more cases would have improved the derivation of conclusions and policy insights. In addition to reduced post-incident resolution, another reason for the low number of cases is that several breaches could be classified or undisclosed by intelligence agencies or research institutions. Thirdly, while most incidents involved research breaches, some cases focused more critically on acquiring individuals' personal data, even though research was targeted by the perpetrators. Lastly, several cases had limited information available, making it challenging to fully address all the sections in Annex A.

	A	B	C	D	E	F
1	**Country**	**Incident Overview**	**Nature of the Threat**	**Impact Assessment**	**Response and Mitigation**	**Evaluation**
2	Australia	A Chinese national, acting as a spy under the guise of a visiting professor, attempted to infiltrate a prestigious Australian research institution to collect sensitive information. The spy was provided with funding and a list of intelligence requirements from their government. The individual involved was a Chinese national recruited by Chinese intelligence. The targeted entity was an Australian research institution, which was not named .	The incident is categorized as foreign interference, as a spy was strategically placed inside an educational establishment to carry out espionage activities. The strategy included enlisting an academic who thereafter used their role to allocate studies that were in line with the intelligence objectives of a foreign nation. Although the specific field of research was not disclosed, it involved an area valuable enough to attract international espionage efforts.	The swift action by the Australian Security Intelligence Organization (ASIO) thwarted the attempt before any known damage could be inflicted on the integrity of the research institution's work or intellectual property .	ASIO intervened promptly, removing the academic from Australia and preventing the espionage plan from succeeding.	Preceding the incident, it is evident that there were protocols designed to detect and address potential espionage risks inside the scientific establishments of Australia. The incident's public exposure and the actions of the ASIO demonstrate a response to the changing landscape of research espionage, namely from players such as China. However, the research institution in question should have had the framework to detect this threat.
3	Australia	A sophisticated spear-phishing attack, allegedly funded by the Iranian government, targeted multiple Australian universities, stealing a vast amount of academic data. The perpetrators were associated with the Iran-based Mabna Institute. The targets included 26 Australian universities, with the Group of Eight as prominent victims (Australia's research-oriented universities similar to the U15 – the University of Melbourne, the Australian National University, the University of Sydney, the University of Queensland, the University of Western Australia, the University of Adelaide, Monash University and UNSW Sydney).	This incident is classified as foreign cyber espionage; the campaign involved spear-phishing to trick academics into providing login credentials, which were then used to access and exfiltrate academic resources materials.	The immediate impact was the unauthorized access and theft of over 31 terabytes of data, potentially undermining the research integrity and intellectual property of the targeted institutions; the state-sponsored nature of the attack and the scale of the theft highlight the vulnerability of academic institutions to cyber espionage and the potential implications for national security.	The US Department of Justice, given that American institutions were targeted as well, charged nine Iranians in connection with the theft, suggesting a law enforcement and diplomatic response to the incident. While specific mitigation measures taken by the Australian universities and the government are not detailed, the scale of the incident likely prompted a reassessment of cybersecurity protocols and defenses against such phishing campaigns.	The success of the spear-phishing campaign suggests that existing measures were not fully effective in preventing such sophisticated social engineering attacks.The response led to legal action against the perpetrators, indicating international collaboration in addressing the threat.

Figure 4: Case Assessment Extract

Discussion & Policy Implications for Australia

Criteria-Based Assessment

Canada and the US, both achieving high overall scores, have a well-established approach to RS. For Canada, the total score of 24 translates to 80% robustness in RS measures and in addressing the criteria. The US, with a score of 26, reaches 87%. Australia's total score of 14 indicates a 47% level towards addressing the various criteria, a substantial gap compared to its North American counterparts. The high scores for the North American nations indicate that these countries have RS policies that are actively enforced, continuously updated, and deeply integrated into their research frameworks. However, it is important to note that, especially in Canada, the STRAC and NSGRP policies are relatively new and have not been fully tested. The Canadian approach, with its substantial funding and support structures, shows great promise but requires time to demonstrate its full impact. For example, the long-term outcomes of NSGRP's application to funds like the Tri-Agency's Canada Biomedical Research Fund [85] and STRAC's implementation in other Canadian funding programs, such as SSHRC's Partnership Engage Grants and the CFI's annual Innovation

[85] "Research Security - Tri-agency Guidance on the National Security Guidelines for Research Partnerships (NSGRP)," Government of Canada, 2024, https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp#a3.

Fund are yet to be seen.[86] In addition, the existing counter-culture within some research institutions, where RS is not always viewed as necessary and is seen as both an administrative burden and counterproductive to innovation, could influence the full adoption of these policies and potentially increase insider risk from individuals seeking to uproot these rigid structures. RS policies are also criticized by some in the Canadian and American research communities for hindering international collaboration, potentially leading to racial profiling and discrimination and diverting resources from core research activities.

Despite both American and Canadian frameworks being robust and well-designed, with scores equivalent to or exceeding the 80 percent threshold, the US's NSPM-33 currently stands out as the more comprehensive and mature system for RS. An earlier start to RS policy discussions and implementation has allowed the US to address initial challenges and improve its framework based on practical experiences. NSPM-33 is also more standardized, combining various requirements for training and awareness and regulations for funding agencies, whereas in Canada, the coordination between various bodies and the standardization of enforcement can be further improved.

With respect to Australia, the disparity in score highlights the differences in RS strategies and underscores the clear need for policy development in the country. The gap also implies that Canberra lacks the centralization and specificity seen in Canadian and US approaches. In maintaining a linear scale where each score signifies a 20% increment towards achieving the highest score of the criterion, the relative standings of each country's RS policies according to each criterion highlight Australia's various shortcomings and provide several policy contrasts between the three nations. For example:

- Governance (US: 100%, Canada: 80% and Australia: 40%): The 60% gap in governance for Australia implies a need for a more centralized approach. Policy considerations could involve establishing a central authority for RS that would take the lead in integrating the current scattered efforts of Australian government agencies and research institutions to secure research.
- Insider Threats (US: 80%, Canada: 60% and Australia: 60%): The US and Canada have higher scores compared to Australia within the context of RS. While various government departments in Canada and Australia have developed insider threat programs, there have not been explicit efforts to apply them specifically to the research ecosystem and adapt them to various scenarios that might cause insider threats, which is crucial to fully address the threat landscape. By contrast, the US has applied insider risk mitigation considerations to its RS policies across the board.
    - The US has made clear efforts to address insider threats in its research sector, as specified in NSPM-33, particularly through the creation and operational demands of RS initiatives. Section 4 (g) of NSPM-33 obligates funding bodies to verify that research organizations receiving over $50 million in annual federal science and engineering support affirm the development and functioning of extensive RS programs.[87] Such programs cover a range of security measures, including cybersecurity, security for international travel, awareness and importantly the detection of insider threats, and export control training where necessary.[88] Although NSPM-33 initially distinguishes "insider

[86] "Research Security - Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)," Government of Canada, 2024, https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp#a3.

[87] Blevins and Gallo, "Research Security Policies: An Overview," 2.

[88] Blevins and Gallo, "Research Security Policies: An Overview," 2.

threat awareness and identification"as separate elements of RS efforts, the Implementation Guidance merges these components under a unified category known as RS training.[89]

- In the Canadian context, Public Safety Canada highlights the importance of strengthening Canada's defense against insider risks, and has created the "The Insider Risk Assessment Tool" (IRAT), enabling organizations to assess internal security measures in relation to insider risk and provide individualized reports that include evaluation results, resilience enhancement suggestions, and ratings.[90] Public Safety has also developed a guide titled "Enhancing Canada's Critical Infrastructure Resilience to Insider Risk," which includes eight security actions aimed at strengthening organizational resilience.[91] The guide emphasizes the importance of identifying critical assets, implementing thorough employee screening processes, and establishing robust third-party security agreements.[92] These strategies and measures outlined for mitigating insider threats in Canada, while primarily focused on protecting critical infrastructure, are applicable to research. However, these guidelines have not yet been formally applied to RS, representing an important next step to further integrate insider risk considerations within Canada's RS framework. CSIS has reinforced the presence of insider threats in the research ecosystem through its initial threat briefings and case study scenarios on the research sector; however, this is insufficient.[93] The NSGRP and STRAC both fail to explicitly mention the threats presented by insiders despite the fact that both policies aim to prevent long-term harmful research partnerships and thereby mitigate insider threats. This should be explicitly articulated within the policies.
- The Countering the Insider Threat: A Guide for Australian Government, the Protective Security Policy Framework (PSPF), and the Security of Critical Infrastructure Act are central to Australia's strategy for mitigating insider threats, emphasizing the importance of risk management programs embedded with rigorous vetting, continuous behavioral monitoring, extensive training and awareness programs, robust incident response plans, and understanding psychological and social factors contributing to insider risks.[94] Yet, similar to Canada, there is a significant gap in their application within research. Australian research institutions are particularly vulnerable to insider cyber threats as they continue to lag behind in basic cybersecurity measures, as further evidenced in the case assessment.

---

[89] Blevins and Gallo, "Research Security Policies: An Overview," 2.

[90] Public Safety Canada, "The Insider Risk Assessment Tool," October 24, 2022, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/irat-oari-en.aspx.

[91] Public Safety Canada, "Enhancing Canada's Critical Infrastructure Resilience to Insider Risk," July 28, 2022, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx.

[92] Public Safety Canada, "Enhancing Canada's Critical Infrastructure Resilience to Insider Risk."

[93] Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch and Communications and Marketing Branch, "CSIS and Research Security," March 31, 2023, https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/csis-and-research-security.

[94] "Countering the Insider Threat: A guide for Australian Government," Australian Government, n.d., https://www.ag.gov.au/integrity/publications/countering-insider-threat-guide-australian-government.

The high-value nature of Australian research output, especially considering the AUKUS agreement, renders it essential to rigorously extend insider threat mitigation strategies to the research ecosystem to protect against both malicious and unintentional insider actions.

- Foreign Interference (US: 80%, Canada: 80% and Australia: 60%): The US and Canada lead with a high score, indicating a robust, well-enforced policy against foreign interference.
    - Compared to its other scores, Australia has shown relative improvement in mitigating foreign interference through UFIT and its moderate attempts to implement RS practices in research funding. However, as noted previously, the Guidelines to Counter Foreign Interference in the Australian University Sector released by UFIT are not mandatory for universities, and their adoption is not always a precondition to receiving funding for sensitive research. The Group of Eight, in tandem with government agencies in Australia, needs to increase their international engagement with allies to observe and integrate best practices.

Case Assessment (Annex B)

In the evaluations conducted across all three countries, cyberattacks emerged as the primary method used by adversaries to compromise sensitive research and data, accounting for approximately 60% of the incidents, with Australia experiencing the highest frequency at around 70%. This reinforces the fact that there are significant digital vulnerabilities within research institutions and universities. Notable examples include the ransomware attack on the University of Sherbrooke and the sophisticated breach of Canada's National Research Council (NRC). In Australia, the spear-phishing attack targeting 26 universities, including the Group of Eight, and the cyberattack on the Australian National University (ANU) highlight the pervasive nature and sophistication of these threats.

Foreign espionage and insider threats were recurring themes, accounting for several of the cases. Many incidents involved the strategic exfiltration of sensitive research to benefit foreign governments, alongside cases where individuals turned into insider threats, either being slowly lured or forced into espionage activities. For instance, Dr. Charles Lieber's concealed collaboration with China's Thousand Talents Plan in the US [95] and Dr. Xiangguo Qiu's unauthorized transfer of sensitive research to China in Canada highlights the significant risks posed by insider threats and foreign espionage.[96] Another key example in Australia is the thwarted espionage attempt by a Chinese national posing as an academic, aimed at acquiring sensitive information from a top research institution.[97] This incident revealed the need for more robust vetting processes and ongoing monitoring to identify and mitigate such threats effectively. The cases of Charles Lieber and Xiangguo Qiu, along with the dismissal

[95] "Former Harvard University Professor Sentenced for Lying About His Affiliation With Wuhan University of Technology; China's Thousand Talents Program; and Filing False Tax Returns," April 26, 2023, https://www.justice.gov/usao-ma/pr/former-harvard-university-professor-sentenced-lying-about-his-affiliation-wuhan.

[96] Rebecca Trager, "Two Canadian Scientists Were Fired in 2021 for Passing Information to China," Chemistry World, June 10, 2024, https://www.chemistryworld.com/news/two-canadian-scientists-were-fired-in-2021-for-passing-information-to-china/4019098.article.

[97] Daniel Hurst and Dan Sabbagh, "Visiting Professor Used PhD Students to Gather Intelligence for China, Asio Boss Alleges," The Guardian, October 18, 2023, https://www.theguardian.com/australia-news/2023/oct/18/visiting-professor-used-phd-students-to-gather-intelligence-for-china-asio-boss-alleges.

of Emory University researchers, also point to vulnerabilities in inadequate disclosure requirements for foreign funding avenues and insufficient monitoring of financial ties.[98] Undisclosed sources of foreign funding resulting in a research breach accounted for approximately 15% of the cases.

As evidenced by the findings, the response mechanisms in Australian institutions have often been reactive rather than proactive. While the ASIO successfully intercepted China's espionage attempt, the initial breach indicated pre-existing vulnerabilities that were not adequately addressed.[99] Similarly, the response to the cyberattack on ANU involved significant post-incident forensic efforts but highlighted the inadequacy of preventive measures.[100] This pattern indicates that although Australia has the capability to respond effectively to incidents, there is a critical need for stronger preventive measures and more proactive strategies. The cases also demonstrated that the US, through the Department of Justice (DoJ), employs punitive measures and legal actions, such as prosecuting individuals who compromise research, intending to deter such activities in the short and long run. As noted previously, the fewer cases in Canada underline the lack of post-incident transparency and point to limitations in research and accessibility of information, creating challenges in balancing and comparing cases between the three countries.

Recommended RS Approach for Australia

Australia has recently been dubbed the "weakest link" within the AUKUS agreement by both its allies and international media, highlighting its vulnerabilities compared to its counterparts.[101] Given this, there is a pressing need to revisit the legal and regulatory frameworks concerning sensitive research. Conducting such a review independently is impractical—federal agencies and universities need to work together to develop an RS policy that aligns with current realities. The Universities Accord, tasked with developing a progressive strategy for the nation's universities and tertiary education, recently delivered its final recommendations to Education Minister Jason Clare. This document could have served as an opportune moment to articulate the importance of a nationwide strategy focusing on the protection of research and knowledge or to reference the 2022. However, it failed to mention RS. Below are key policy recommendations and a centralized roadmap approach to RS.

General

- Crafting a clear and centralized policy on securing research and knowledge is a significant responsibility for the Australian government, notably the Department of Education, the Department of Home Affairs, and the Department of Industry, Science, and Resources (DISR). Canberra must not wait for the next breach that could pose major national security and economic risks and also harm its key allies. Immediate action is needed to address the key issues identified. The next section (Roadmap) delves deeper into the potential role of DISR in an RS centralization effort and in

[98] "Former Harvard University Professor Sentenced for Lying About His Affiliation With Wuhan University of Technology; China's Thousand Talents Program; and Filing False Tax Returns."
[99] Hurst and Sabbagh, "Visiting Professor Used PhD Students to Gather Intelligence for China, Asio Boss Alleges."
[100] Stephanie Borys, "The ANU Hack Came Down to a Single Email — Here's What We Know," ABC News, October 2, 2019, https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540.
[101] Croft, "Australia the 'Weakest Link' in AUKUS on Cyber Security."

coordinating the roles of government, intelligence agencies, and universities in managing and addressing various national security risks in the research ecosystem.

UFIT & Foreign Interference

- To enhance focus on scrutinizing research collaborations, the Australian Government should revise and update the UFIT guidelines, looking to the Canadian NSGRP for a model.
    - The UFIT guidelines advise universities to view foreign interference risks as a primary concern. However, they emphasize that instead of broadly searching for the risks, efforts should be concentrated on conducting due diligence specifically on activities and partners already identified as vulnerable or "at risk of foreign interference."[102] In essence, they prioritize investigating known risks rather than conducting due diligence to identify agreements that require a national security risk assessment.[103]Supported by Australia's national intelligence community and through UFIT revisions, universities should be equipped with advanced tools for assessing risks associated with proposed agreements.[104] Emphasis should be placed on how universities will handle foreign interference and espionage risks in the future, including the practical implementation and enforcement of UFIT guidelines.[105] Currently, there are insufficient oversight mechanisms to ensure these guidelines are being fully implemented in all universities.
    - NHMRC, ARC, and CSIRO, the key Australian research funders, should amend their policies to require proof of compliance with UFIT guidelines for all grant funding processes. Consequences for non-compliance should be clearly stated, especially in ARC's Research Integrity Policy, which currently does not sufficiently address foreign interference or espionage as threats to research integrity. The ARC has initiated the process of verifying risks in sensitive research prior to funding through their recently released RS measures. However, other major funders, such as NHMRC and CSIRO, must also adopt similar practices. The approach should reflect the model in Canada, where the Tri-Agency, CFI, and other funders like Genome Canada and MITACS have all integrated national security considerations into their funding practices, along with detailed internal RS plans.
    - While the ARC has implemented risk assessments within its NCGP, it must also explicitly clarify how these assessments are applied to their other funding programs.
    - Universities that rely on self-funding for their research must enforce risk assessment procedures, especially when collaborating with international partners. However, during the negotiations of the financial arrangement and thereafter, universities often lack the requisite expertise or resources to do

[102] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 28.
[103] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 28.
[104] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 28.
[105] Walker-Munro, Mount, and loannou, "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education," 28.

thorough due diligence on their international counterparts.[106] Due to classification restrictions, both the Department of Home Affairs and ASIO, which possess more capabilities for undertaking such assessments, are not always able to provide the required information. Therefore, it is critical for the intelligence community and academic institutions to develop improved communication mechanisms, but more importantly, for Australian researchers to receive sufficient domestic financing from granting agencies, rather than from their universities, to avoid interference from foreign entities.[107] The policy directions for the Australian government should include increasing funding for the NHMRC, ARC, and CSIRO and establishing stringent financial criteria for universities.[108] The former approach would best balance academic freedom and national security.
    - To further enforce these measures, the 2022 PJCIS recommendations need to be revisited and implemented, with further discussion on leadership from one department outlined in the Roadmap section.
- UFIT should also tackle the issues of on-campus intimidation and related national security risks related to research.
- A significant part of all the above-mentioned efforts should involve UFIT supporting universities in implementing, maintaining, and enhancing relevant training and programs on national security for both faculty and students.

Cybersecurity

- ASIO, Home Affairs, and the Australian Cyber Security Centre should work closely with the education and research sectors to provide frequent updates on the risks of espionage and foreign interference, especially from a cybersecurity perspective.[109] Universities need to be informed about the constantly evolving tactics, techniques and procedures (TTPs) used by threat actors.
    - To ensure their RS programs are robust, universities should integrate cyber defenses by implementing advanced encryption protocols to protect sensitive research data from unauthorized access, employing robust intrusion detection systems to monitor and respond to suspicious activities targeting research networks, and conducting regular cybersecurity training focused on research staff and students. This training is crucial to ensure awareness and preparedness against potential cyber threats, especially given the increased cyber-attacks targeting Australian academic institutions, as demonstrated by the dataset findings.[110]

Insider Threat Mitigation

- Within the research domain, Australian governmental guidelines for insider threats, including the PSPF and the Countering the Insider Threat: A guide for Australian

[106] Walker-Munro, "Submission to the Department of Education Interim Report on the Universities Accord," 22.
[107] Walker-Munro, "Submission to the Department of Education Interim Report on the Universities Accord," 22.
[108] Walker-Munro, "Submission to the Department of Education Interim Report on the Universities Accord," 22.
[109] "PJCIS List of Recommendations."
[110] "PJCIS List of Recommendations."

Government, should be strictly enforced. While UFIT currently mentions in section 3.2.1[111] that universities should conduct due diligence on partners and personnel, there needs to be a more explicit reference to the threats posed by insiders, detailing how foreign coercion affects researchers on Australian campuses and outlining appropriate mitigation strategies.

- Additionally, Australian universities hosting a Confucius Institute must publicly share details of such partnerships and ensure they retain control over staff appointments and curriculum content, while enforcing strong protections for academic freedom and free speech in all agreements. Research partnerships with Confucius Institutes may pose long-term insider risks on Australian campuses.

Roadmap

Figure 5: Australian National RS Framework Development

Lead Agency

For the recommendations to be accounted for and implemented, Australia needs a specific agency to lead the charge. DISR is ideally positioned to lead Australia's initiative to enhance RS for several reasons. DISR's overarching mission encompasses the promotion of Australia's prosperity through research, innovation, science, and commercialization of new technologies, which places it at the heart of industry, academia, and government, thereby allowing DISR to effectively coordinate among various stakeholders involved in R&D. Moreover, DISR's existing relationships with key research funding and regulatory bodies, such as ARC and CSIRO, provide it with the necessary leverage to implement comprehensive security measures across the research landscape. Australia's Department of Education has repeatedly been pressed to implement or consider the implementation of an overarching RS policy, but to no avail. The content of the Universities Accord is a testament to this, as previously mentioned. Therefore, policy discussions must consider alternative departments, such as DISR, to lead the implementation of an RS policy in collaboration with the Department of Education, along with other key stakeholders. Based on the policy comparison

[111] "Guidelines to Counter Foreign Interference in the Australian University Sector."

with the US and Canada, above is a roadmap and below is a brief walkthrough for the development of the "Australian National Research Security Framework." Key highlights include:

- DISR creating an RS coordination unit dedicated to overseeing the initiative's implementation.
- Through the unit, DISR would establish an RS Working Group (RSWG) comprising representatives from key government agencies, academia, industry, and security organizations.
- Through both of these mechanisms, DISR would initiate a comprehensive stakeholder engagement process to develop a robust RS policy framework.

Key Steps

1: Framework Enforcement

- Subsequent to ministerial authorization, launch the Research Security Initiative (RSI) to develop the Australian National Research Security Framework.
    - DISR would announce the initiative's goals, emphasizing the enhancement of national RS in collaboration with key stakeholders.
    - Develop a comprehensive communication plan to introduce the RSI to the public, stakeholders, and international partners.
- Inception of the Research Security Coordination Unit (RSCU)
    - Set up the RSCU within DISR to oversee the implementation of the RSI.
    - Define the RSCU's structure, roles, and responsibilities. Consider the resources needed and key stakeholders that will be part of the RSWG.
    - Recruit a multidisciplinary team to form a RSWG under RSCU with the appropriate expertise.
    - Identify and begin engaging with all relevant stakeholders to ensure their input informs the initiative from the get-go.

2: Policy Development and Framework Construction

- Benchmarking and Policy Drafting
    - The working group within RSCU would draft a comprehensive national RS framework, incorporating international best practices and stakeholder input.
    - RSCU would be responsible for reinvigorating UFIT and integrating it as part of a broader framework. Under this framework, the existing UFIT guidelines would be revised and updated to align with and be integrated into the comprehensive national RS framework. This would include the recommendations made by PJCIS, among many other considerations, such as mitigation strategies to address insider threats in alignment with "Countering the Insider Threat: A Guide for Australian Government."
    - The Australian National Research Security Framework could model NSPM-33, for example, requiring all federal research funding agencies to strengthen and standardize disclosure requirements for federally funded awards and enforce the establishment of RS programs at major research institutions and universities receiving federal funds or conducting intensive research.
    - This would entail a reevaluation of the research funding structure in Australia by amending policies of key research funders (NHMRC, ARC, and CSIRO) to require researchers to comply with updated UFIT guidelines as a condition for receiving research grants in sensitive areas, notably those highlighted in "Australia's List of Critical Technologies in the National Interest." As noted previously, the ARC has begun adopting risk assessment procedures

throughout the lifecycle of grants, which is a step in the right direction, although other funders have not implemented such measures. To achieve more tangible progress, funding structures must also be rebalanced to ease the pressure on universities. Increased funding for NHMRC, ARC, and CSIRO would help reduce universities' reliance on research partnerships that could pose major national security risks.
    - As per the new framework, Australian universities, notably within the Group of Eight, will have to adopt comprehensive RS measures, including policies, procedures, and controls that ensure the integrity and security of their research programs.

3: Implementation and Capacity Building

- Pilot Projects and Training Programs
    - Identify and launch pilot projects in a diverse range of granting agencies and research institutions to evaluate the practicality and effectiveness of the policy framework.
    - Develop and deliver targeted training programs for researchers, grant administrators, and policymakers on best practices in RS.

4: Policy Finalization and Approval

- Integration of Feedback and Final Refinements
    - RSCU integrates all feedback and finalizes the policy titled "The Australian National Research Security Framework."
    - The finalized policy will then be submitted to the appropriate governmental bodies for approval. This will involve the DISR and the Department of Education, culminating in sign-off by the designated minister or authority. A detailed implementation roadmap should also be released, outlining timelines for adopting the policy.

Conclusion

The importance for Australia to develop an RS framework is clear from the findings and analysis presented. The global shift towards recognizing the importance of protecting sensitive research from external threats places Australia at a critical juncture, where it can either follow its FVEY counterparts or continue to stray aside. The US and Canada have, in accordance with the threat level, developed responses in collaboration with universities.

To address these challenges, the paper proposes a strategy for Australia, emphasizing the role of the DISR in leading the effort. Australia can establish a strong RS framework by promoting cooperation among government, intelligence services, and the academic sector. The proposed methods include creating an overarching RS policy, revising guidelines to effectively address foreign interference, augmenting cybersecurity measures in universities, and implementing comprehensive techniques to mitigate insider risks, among many others. This can only be achieved if an established centralized body takes the lead in weaving strategies together, deviating from the current fragmented state of RS in Australia. Through the adoption of strategies grounded in an understanding of the current RS environment and informed by successful practices, Australia can strengthen its position and ensure the security of its research contributions internationally.

Annex A: Case Assessment Framework

Incident Overview

- Description: A concise summary of the incident, including the nature of the breach (cyberattack, physical theft, espionage) and location/date (if relevant).
- Entities Involved: Identification of the parties involved, including the perpetrator(s) and the targeted institution or country.

Nature of the Threat

- Type of Threat: Classification of the threat as foreign interference, insider threat, or a combination of both.
- Methodology: The tactics, techniques, and procedures (TTPs) employed by the perpetrators.
- Targeted Research Area: The specific field of research or type of data targeted, if applicable and available.

Impact Assessment

- Immediate Impact: The direct consequences of the incident on the targeted institution's research integrity, financial status, and personnel.
- Broader Implications: The wider repercussions on national security, international relations, or the global research community.

Response and Mitigation

- Initial Response: The immediate actions taken by the targeted institution or government in response to the incident.
- Mitigation Measures: The short-term and long-term measures implemented to prevent future occurrences, including changes to policies, practices, or infrastructure.

Evaluation

- Pre-incident Framework: An analysis of the measures in place prior to the incident and their potential vulnerabilities.
- Effectiveness of Response: An evaluation of how effectively the measures addressed the incident and mitigated its impact.
- Adaptability: The ability of an RS framework to adapt to emerging threats and incorporate lessons learned from the incident.

Annex B: Dataset

Country	Incident Overview	Nature of the Threat	Impact Assessment	Response and Mitigation	Evaluation
Australia	A Chinese national, acting as a spy under the guise of a visiting professor, attempted to infiltrate a prestigious Australian research institution to collect sensitive information. The spy was provided with funding and a list of intelligence requirements from their government. The individual involved was a Chinese national recruited by Chinese intelligence. The targeted entity was an Australian research institution, which was not named .	The incident is categorized as foreign interference, as a spy was strategically placed inside an educational establishment to carry out espionage activities. The strategy included enlisting an academic who thereafter used their role to allocate studies that were in line with the intelligence objectives of a foreign nation. Although the specific field of research was not disclosed, it involved an area valuable enough to attract international espionage efforts.	The swift action by the Australian Security Intelligence Organization (ASIO) thwarted the attempt before any known damage could be inflicted on the integrity of the research institution's work or intellectual property .	ASIO intervened promptly, removing the academic from Australia and preventing the espionage plan from succeeding.	Preceding the incident, it is evident that there were protocols designed to detect and address potential espionage risks inside the scientific establishments of Australia. The incident's public exposure and the actions of the ASIO demonstrate a response to the changing landscape of research espionage, namely from players such as China. However, the research institution in question should have had the framework to detect this threat.
Australia	A sophisticated spear-phishing attack, allegedly funded by the Iranian government, targeted multiple Australian universities, stealing a vast amount of academic data. The perpetrators were associated with the Iran-based Mabna Institute. The targets included 26 Australian universities, with the Group of Eight as prominent victims (Australia's research-oriented universities similar to the U15 – the University of Melbourne, the Australian National University, the University of Sydney, the University of Queensland, the University of Western Australia, the University of Adelaide, Monash University and UNSW Sydney).	This incident is classified as foreign cyber espionage; the campaign involved spear-phishing to trick academics into providing login credentials, which were then used to access and exfiltrate academic resources materials.	The immediate impact was the unauthorized access and theft of over 31 terabytes of data, potentially undermining the research integrity and intellectual property of the targeted institutions; the state-sponsored nature of the attack and the scale of the theft highlight the vulnerability of academic institutions to cyber espionage and the potential implications for national security.	The US Department of Justice, given that American institutions were targeted as well, charged nine Iranians in connection with the theft, suggesting a law enforcement and diplomatic response to the incident. While specific mitigation measures taken by the Australian universities and the government are not detailed, the scale of the incident likely prompted a reassessment of cybersecurity protocols and defenses against such phishing campaigns.	The success of the spear-phishing campaign suggests that existing measures were not fully effective in preventing such sophisticated social engineering attacks.The response led to legal action against the perpetrators, indicating international collaboration in addressing the threat.
Australia	Australian National University (ANU) suffered a sophisticated cyberattack targeting personal data and potentially research data. Detected in April 2019, the attack occurred between November 2018 and May 2019 in Canberra, Australia.	This was indicative foreign interference: the attack employed credential theft, infrastructure compromise, and advanced malware, demonstrating high capability and persistence. Personal data from the ANU's systems, with potential interest in research data.	Unauthorized access to personal data and sensitive material, with the extent of data theft initially feared to be 19 years of records but later reassessed. Implications were severe for individuals whose data was compromised.	Upon the detection of the compromise, the cyber team at ANU, in collaboration with Northrop Grumman and several government agencies, executed a sophisticated forensic response. Following the event, it is probable that ANU has boosted its investment and implementation of cybersecurity measures, however the particular long-term goals were not explicitly outlined.	ANU had standard cybersecurity measures in place, which were insufficient to prevent the sophisticated attack. The response was effective in uncovering the breach; however, it was not timely enough to prevent data exfiltration. The incident has prompted a reassessment of cybersecurity practices at ANU, indicating a shift toward more robust defenses.
Australia	A privacy breach occurred at the Australian Research Council (ARC) from a possible insider, leading to the unintended disclosure of residency details of grant applicants to assessors.	This incident represents an insider threat to privacy, possibly due to a process or system flaw. Although not specified, the breach could result from a technical oversight or human error in the data handling process. The breach directly impacts the confidentiality aspect of the research grant application process.	The breach could affect the trust and integrity of the grant application process and the privacy of applicants.	The ARC's immediate action was to instruct assessors to delete the files containing the breached information and initiate an internal investigation. Depending on the outcome of the investigation, the ARC will likely revise its data handling procedures to prevent future breaches.	It appears there may have been vulnerabilities in the ARC's data management systems that allowed the breach to occur. The effectiveness of the ARC's response will depend on the thoroughness of the investigation and the implementation of corrective measures. The ARC's ability to adapt its policies and practices in light of this breach will be critical in restoring confidence in its data and research security measures.
Australia	A data breach occurred at QIMR Berghofer Medical Research Institute due to a compromised third-party file-sharing service, Accellion, which led to unauthorized access to clinical trial data. Announced in February 2021, the breach impacted the Brisbane-based research institute. QIMR Berghofer, Accellion (the third-party service provider), and unknown attackers, with links suggested to the Iranian government.	This was a foreign state-led cyberattack exploiting a zero-day vulnerability in Accellion's software. The attackers utilized a sophisticated cyber intrusion technique to exploit the vulnerability and access data. Data related to clinical trials for anti-malaria drugs, as well as resumes of research staff, were accessed.	Unauthorized access to de-identified clinical trial participant information and staff resumes, leading to potential intellectual property theft and privacy concerns. The breach has wider implications for data security in medical research and raises concerns about the security of third-party services.	The institute implemented a security patch provided by Accellion and began an internal investigation; QIMR Berghofer has expressed intentions to review and enhance protocols for using third-party file-sharing services.	Accellion provided QIMR Berghofer with services that were believed to be safe until flaws were discovered during the hack. Although the breach did occur, the prompt installation of the security patch and the investigation show a proactive reaction. The institution demonstrates flexibility in fortifying their defenses with their dedication to reviewing third-party service procedures and guaranteeing safe storage.
Australia	After Australian Clinical Laboratories was the target of a cyberattack, over 200,000 client records, private data, and clinical research data were leaked to the dark web .	The attack, executed by the Quantum hacker group, involved data exfiltration.	Immediate impact included the breach of customer privacy and potential financial fraud. Broader implications involve the erosion of trust in data security practices.	An internal investigation was initiated, and the Office of the Australian Information Commissioner (OAIC) took legal action due to systemic failures in cybersecurity.	Pre-incident measures were found to be inadequate, with an absence of a dedicated cybersecurity team.
Australia	Unauthorized access to Deakin University's system via a third-party provider led to the theft of 46,980 students' personal information along with scholarly work from various databases.	Cyberattack exploiting a third-party service through phishing to obtain login credentials and subsequent data theft. There are reports of this infiltration being facilitated by an insider.	Risk of identity theft and payment fraud for affected students. Highlights vulnerabilities in university data security, particularly related to third-party services.	Investigation launched; affected individuals notified. Review of third-party service use and security enhancements, including the consideration of multi-factor authentication (MFA) to prevent similar breaches.	Potential lack of stringent cybersecurity measures for third-party services. The thorough investigation and public acknowledgment are positive steps, but the delayed response and initial security gaps suggest room for improvement. Deakin's response includes working to strengthen security practices, indicating a willingness to adapt and improve RS measures.
Australia	A breach in the University of Western Australia's Callista system exposed sensitive student and alumni data, including scholarly research, due to unauthorized access, marking a significant security incident within the educational sector.	This cyberattack, facilitated possibly through a phishing scheme or insider, represents a severe intrusion, leveraging a third-party vulnerability to compromise data integrity and privacy.	The immediate impact involved the risk of identity theft for individuals whose data was compromised; broader implications concern the potential exposure of sensitive research and academic achievements, affecting the institution's reputation and trust.	The university promptly initiated an investigation, involving law enforcement, and advised the affected community to monitor for suspicious activity, indicating a responsive and responsible approach to the breach.	This case evidences potential pre-existing vulnerabilities within the university's data security framework, especially concerning third-party services - the institution's adaptability to strengthen its cybersecurity measures post-incident will be crucial for future resilience.
US	Dr. Charles Lieber, the Chair of Harvard University's Chemistry and Chemical Biology Department, along with two Chinese nationals, were charged with aiding the People's Republic of China. Dr. Lieber was arrested on January 28, 2020, with court proceedings and further developments occurring throughout 2020 and 2021 in Boston, Massachusetts. Other entities involved included two Chinese nationals—Yanqing Ye and Zaosong Zheng.	This case presents a blend of insider risk and foreign interference, with Dr. Lieber accused of concealing his involvement with the Chinese Thousand Talents Plan. The tactics involved Dr. Lieber receiving financial incentives to collaborate with Wuhan University of Technology (WUT) in China without proper disclosure to US federal agencies. Nanoscience was the targeted research area with significant grant funding from the National Institute of Health (NIH) and the Department of Defense (DoD) involved.	The incident led to the arrest and charging of Dr. Lieber, disruption of research activities, and potential reputational damage to Harvard University; this breach has increased concerns over the integrity of academic research, potential loss of sensitive technology, and financial conflicts of interest within higher education and research institutions.	The immediate arrest of Dr. Lieber and charges against the involved parties. Ongoing investigations and trials, along with increased scrutiny on international collaborations by research institutions.	The measures appear to have gaps, as significant foreign affiliations and financial conflicts of interest went undisclosed. The response was robust with legal action, but the effectiveness of the pre-existing RS framework is in question. The incident likely prompted a re-evaluation of disclosure policies and the need for greater oversight of international collaborations by research institutions and funding provisions by granting agencies.
US	Two veteran researchers at Emory University were removed from their positions for failing to disclose foreign sources of research funding and the extent of their work with research institutions in China. The case involves undisclosed foreign financial conflicts of interest. The incident came to light on May 23, 2019, at Emory University in Atlanta, Georgia. The researchers, Li Xiao-Jiang and Li Shihua, geneticists specializing in CRISPR gene editing, were found to have ties with Chinese research institutions.	This incident represents a combination of insider risk and foreign interference due to undisclosed financial ties and collaboration with foreign entities that could potentially conflict with US interests. The researchers received undisclosed funds from Chinese sources and were involved in collaborative work with research institutions in China without proper disclosure. Their work in the field of genetics involved using CRISPR technology to create engineered animal models for studying human diseases.	The immediate impact was the dismissal of the researchers from Emory University, the closure of their laboratory, and the confiscation of computers and documents. This case heightened concerns about foreign influence in academia and the need for transparency in disclosing foreign collaborations and funding.	Emory University conducted an internal investigation after receiving communication from NIH and terminated the employment of the researchers. The university also stated its commitment to the free exchange of ideas and research collaboration. In the broader context, since this incident, there has been an increased effort to enforce disclosure requirements for federally funded researchers in accordance with federal RS requirements, as well as a general tightening of rules regarding foreign influence in research.	The framework at Emory University, as with many US research institutions prior to NSPM-33, was likely not fully prepared to detect and prevent the kind of undisclosed foreign involvement that occurred in this case. Responses from Emory University were decisive in terminating the researchers and communicating with NIH, indicating an effective immediate reaction to the incident.
US	MD Anderson Cancer Center terminated three senior researchers after being informed by NIH that they may have violated rules involving the confidentiality of peer review and disclosure of foreign ties. The disclosures occurred in Houston, Texas, with the terminations coming to light in April 2019. MD Anderson Cancer Center, NIH, the researchers involved (who remain unnamed in the reports but are described as ethnically Chinese).	The case indicates a mix of potential insider risk, given the confidentiality breach, coupled with foreign interference due to undisclosed foreign ties. Alleged inappropriate sharing of confidential grant information and failure to disclose foreign relationships and resources. Though not specified in the case details, the research likely pertained to areas funded by NIH grants at MD Anderson Cancer Center.	The immediate result was the initiation of termination proceedings against the researchers and heightened scrutiny of faculty members' foreign connections, with implications for research integrity and institutional trust. This incident contributes to an atmosphere of increased vigilance concerning foreign influence within US research institutions, potentially affecting international collaborations and the research community at large.	MD Anderson responded to NIH's concerns by conducting internal investigations and initiating termination procedures for the implicated researchers. Following federal RS requirements, there have been ongoing efforts by NIH to ensure transparency and mitigate risks associated with foreign ties, along with institutional actions to address and safeguard against such threats.	The presence of undisclosed foreign ties suggests that pre-existing measures may have been insufficient to detect or prevent breaches of this nature.

US	Huajun Zhao, a researcher at the Medical College of Wisconsin, was charged with economic espionage, accused of stealing research data and materials for a cancer-fighting compound, C-25.	This case is classified as economic espionage, where a researcher exploited his position to misappropriate proprietary research material with the intent to benefit a foreign entity. Zhao allegedly stole vials of a substance called C-25 and took steps to provide it to Zhejiang University in China. He is also accused of copying and deleting research files from MCOW computers. The targeted research was in the field of cancer treatment, specifically related to the compound C-25, a potential anticancer agent.	The incident led to the arrest of Zhao, disruption of research activities at the Medical College of Wisconsin, and potential loss of proprietary research material. After this case there was an increase in concerns regarding the vulnerability of US research institutions to economic espionage, particularly involving foreign entities.	The Medical College of Wisconsin cooperated with the FBI, and law enforcement actions led to Zhao's arrest. The investigation and legal proceedings against Zhao served as a deterrent against similar acts of espionage. It highlighted the need for stringent security measures and thorough vetting of research personnel.	The fact that Zhao was able to access and delete research data suggests that there were vulnerabilities in the pre-existing RS framework. The swift response by the FBI and the institution's cooperation signify a robust approach to handling the detected threat; the incident likely prompted the Medical College of Wisconsin and other institutions to bolster their security protocols and monitoring systems to prevent future incidents of espionage.
US	Emory University terminated two faculty members in the Department of Genetics for failing to disclose foreign sources of funding and their involvement with institutions in China. The terminations were announced in June 2019, at Emory University in Atlanta, Georgia.	The incident represents a blend of insider risk due to the failure to disclose significant foreign affiliations and potential foreign interference by leveraging undisclosed foreign ties. Again, the non-disclosure of foreign sources of funding and extent of work for research institutions and universities in China put genetics research, specifically research using CRISPR gene editing in animal models for human diseases, under risk.	This case contributes to the national dialogue on the integrity of federally funded research and the potential for foreign influence, impacting trust in academic and research institutions.	Prompt investigation by Emory University in response to an NIH inquiry, led to the termination of the involved faculty members. Emory University minimized disruption within the department and ensure the continuity of research projects, along with increased awareness and compliance measures regarding funding disclosure requirements.	The incident highlights potential gaps in the institutional framework for monitoring and ensuring full disclosure of foreign affiliations and funding sources by faculty members .
US	Idaho National Laboratory, a leading US facility for cybersecurity, nuclear, and clean energy research, experienced a significant data breach. An unauthorized access targeted its HR systems, leading to the exposure of both employee and research data. The breach was detected and reported in early 2023.	This incident combines elements of cyber-espionage with insider risk, given the focus on HR systems and potential access to sensitive employee data.The breach involved unauthorized access to INL's Oracle HCM system, supporting human resources applications, likely through cybersecurity vulnerabilities. While directly impacting HR systems, the breach poses a secondary threat to the broader research initiatives at INL by potentially exposing research personnel's sensitive data.	The breach led to the exposure of personal and employment information for potentially thousands of employees and research data, affecting their privacy and INL's operational security. The incident undermines trust in INL's capability to secure critical infrastructure, especially given its role in cybersecurity. It raises questions about the effectiveness of current security measures against sophisticated cyber threats.	INL promptly initiated protective measures to secure employee data and collaborated with federal law enforcement for investigation. Mitigation steps included reviewing and enhancing cybersecurity practices, potentially increasing multi-factor authentication measures, and educating employees on cybersecurity hygiene.	The incident reveals potential vulnerabilities in the pre-existing cybersecurity framework, particularly concerning the protection of HR systems and sensitive employee data. The quick action to engage law enforcement and secure systems reflects a strong response capability. However, the breach's occurrence indicates a need for review and reinforcement of existing security measures. This event prompted a reevaluation of cybersecurity strategies at INL, emphasizing the need for continuous adaptation to emerging cyber threats and strengthening the resilience of HR and research data systems.
US	Xiwen Huang, a Chinese businessman and naturalized US citizen, was charged with theft of trade secrets after engaging in a scheme to steal confidential information from US government research facilities, with the intent to benefit a Chinese company and himself .	The immediate repercussions of Huang's theft on the research facilities included potential compromise of proprietary technologies and methodologies critical to US defense and energy sectors. The broader implications resonate with the risk of undermining US technological leadership and jeopardizing the security of critical infrastructure, given the military applications of the stolen research.	The theft put at risk the economic interests and jobs in North Carolina by potentially allowing foreign competitors to gain an unfair advantage.	Federal custody of Huang following his arrest upon returning from China, with cooperation between the FBI and the US Attorney's Office leading to charges. Mitigation measures included legal prosecution of Huang, including a plea agreement with expectations of a formal guilty plea to be entered in court .	Vulnerabilities in protecting trade secrets and the need for enhanced security and vigilance within companies and government research facilities are highlighted by this case.
US	Li Chen pleaded guilty to conspiring to steal scientific trade secrets related to exosomes and their isolation from Nationwide Children's Hospital's Research Institute. The stolen trade secrets were intended for personal financial gain and sale in China.	This particular case illustrates examples of economic misconduct and the unauthorized acquisition of intellectual property, specifically pertaining to trade secrets associated with medical research. Mr. Chen and Zhou engaged in a conspiracy to illicitly acquire a minimum of five trade secrets pertaining to exosome research, capitalizing on their authority inside the research organization. This incident might be classified as an instance of insider threat. The study of exosomes has great importance in the realm of pediatric medicine as it aids in the detection and treatment of many medical disorders.	The theft directly compromised the confidentiality and integrity of sensitive research developments at Nationwide Children's Hospital, leading to financial and reputational damage. This case illustrates the broader issue of economic espionage related to the PRC, contributing to the global dialogue on protecting intellectual property against foreign theft.	Nationwide Children's Hospital cooperated with the investigation, which led to Chen's guilty plea. The FBI and other federal agencies were involved in the investigation and legal process. Li Chen agreed to forfeit approximately $1.4 million, along with significant shares in related corporations, as part of her plea agreement.	The incident exposes possible deficiencies in Nationwide Children's Hospital's measures to safeguard its intellectual property, namely with the comprehensive evaluation and supervision of research personnel who have access to confidential data.
US	Yu Zhou pleaded guilty to conspiring to steal scientific trade secrets related to exosomes from Nationwide Children's Hospital's Research Institute, aiming to personally profit in China.	This is a case of economic espionage with the intent to transfer American scientific innovations to China for personal gain. Zhou, alongside his wife, engaged in a conspiracy to misappropriate research findings and methodologies for isolating exosomes—a critical area of pediatric medical research. The targeted research area was exosome research significant for identifying and treating various medical conditions, including necrotizing enterocolitis in premature babies, liver fibrosis, and liver cancer.	The theft of trade secrets undermines the research integrity at Nationwide Children's Hospital and represents a financial and competitive loss and poses a risk to the US' national economic security.	The prompt legal action leading to the guilty pleas of Zhou and Chen illustrates the US commitment to countering intellectual property theft.	Vulnerabilities in detecting and preventing the misappropriation of sensitive research were prevalent within this research institution.
US	Chenyan Wu and Lianchun Chen, both research scientists, pleaded guilty to charges related to illegally importing lab chemicals and sharing confidential mRNA vaccine research from a major American pharmaceutical company with China. Wu moved to China and opened TheraMab to focus on mRNA vaccine research, while Chen remained in the US, working for the same company and sending confidential materials to Wu.	The actions of Wu and Chen represent economic espionage and intellectual property theft. They conspired to advance competing laboratory research in China by stealing trade secrets from an American pharmaceutical company.	The immediate impact of their actions includes the breach of confidential research data, which could have advanced scientific knowledge and commercial interests in China at the expense of American innovation. The broader implications include heightened concerns over the security of sensitive research data and international trust in collaboration.	The Department of Justice is committed to protecting American intellectual property and the concerted efforts by law enforcement agencies to curb the illegal transfer of trade secrets to foreign entities.	This case illustrates the ongoing challenge of safeguarding sensitive research data against espionage. It highlights the importance of stringent security protocols within research institutions and pharmaceutical companies to detect and prevent unauthorized access and transmission of proprietary information.
Canada	Dr. Xiangguo Qiu and her husband Keding Cheng were dismissed from the National Microbiology Lab after an investigation revealed they might have been working to benefit China, including sharing sensitive scientific information without authorization. The couple was removed from the lab in July 2019, with their firing announced in January 2021. The investigation and full public revelation occurred over several years, concluding around March 2024.	The incident represents a combination of insider risk and foreign interference, highlighting potential espionage and unauthorized transfer of sensitive information to China. Activities included unauthorized sharing of scientific data, such as genetic sequences of pathogens like Ebola, and potentially breaching security policies regarding lab access and material shipment.	The incident raised serious national security concerns, led to the termination of the involved researchers, and potentially compromised sensitive research.	Suspension of security clearances and employment termination followed PHAC's administrative report and CSIS's security reassessment. Mitigation measures include an ongoing RCMP investigation, enhanced security protocols at the NML, and broader national efforts to secure intellectual property and sensitive research from foreign interference.	The case indicates gaps in the oversight of international collaborations and employee conduct within high-security research settings. The response highlights the challenges of detecting and mitigating insider threats, especially when they involve complex national security considerations .Such an incident has likely prompted a reevaluation of security measures within Canada's scientific research community, emphasizing the need for rigorous vetting, monitoring, and enforcement of compliance with security policies.
Canada	The University of Winnipeg experienced a cyberattack targeting its network, causing significant disruptions including class cancellations, internet outages, and exam delays. It is highly possible that research was targeted by the threat actors, though personal information of students was the main target.	This threat is still being investigated.	Cyberattacks aimed at disrupting educational operations and potentially accessing sensitive information. The specific methods used in the attack were not detailed, but such attacks typically involve phishing, malware, or exploiting network vulnerabilities.	Immediate impacts included the cancellation of classes, internet downtime, and delays in exams, causing significant disruption to academic activities. The attack is part of a growing trend of cyberattacks against educational institutions, underscoring the vulnerability of such entities to cybersecurity threats and the potential long-term impacts on institutional reputation and trust.	The University of Winnipeg initiated an investigation to understand the impact and took steps to mitigate further damage. They also planned a town hall to update the community.
Canada	Dr. Klaus Nielsen, a scientist at the Canadian Food Inspection Agency (CFIA), was targeted by espionage to obtain his research on brucellosis. He was arrested while attempting to transport vials of brucella bacteria to China.	This case represents a direct act of espionage with the intent to transfer sensitive scientific research from Canada to China for commercial gain.	The immediate impacts included the arrest of Dr. Nielsen, the disruption of his research activities, and legal proceedings that led to his conviction.	Apart from the arrest, no other major responses were noted.	Prior to the incident, there may have been insufficient safeguards to prevent such a breach of security and espionage within the CFIA. The response, while ultimately successful in apprehending Nielsen, highlighted gaps in detecting and preventing espionage activities within government research entities.
Canada	A highly sophisticated Chinese state-sponsored actor successfully hacked into the NRC's (National Research Council's) computer systems. This cyberattack was identified by the Communications Security Establishment Canada.	The attack was a targeted cyber-espionage effort aimed at stealing scientific research and data from the NRC. The exact methods used in the cyberattack were not disclosed, but it involved sophisticated techniques indicative of a state-sponsored actor. the NRC engages in various fields of scientific research and technological development, making it a valuable target for cyber-espionage activities.	The cyberattack led to the isolation of the NRC's IT system from the rest of the government's networks to prevent further breaches. It disrupted the NRC's operations, including its collaborations with private businesses.	The NRC and Canadian officials took immediate steps to isolate the compromised systems and began efforts to rebuild the NRC's IT infrastructure, a process that took up to a year. The incident prompted discussions at the highest levels between Canada and China, with Canadian officials raising the issue directly with their Chinese counterparts.	Such a cyberattack revealed the gaps in cybersecurity measures at the NRC.

Canada	The LockBit ransomware gang claimed responsibility for a cyberattack on the University of Sherbrooke, compromising data from one laboratory.	This incident is categorized as a ransomware attack, a malicious attempt to deny access to the institution's data or systems, often with a demand for payment in exchange for restoring access or not leaking the data. The specific techniques used by the LockBit gang were not detailed but typically involve encrypting files on the victim's network and demanding a ransom for the decryption key. Data from one laboratory was compromised, though details on whether this included personal information or intellectual property were not disclosed.	The attack led to the compromise of critical data, but the university stated that its activities had not been impacted. Ongoing investigations aim to assess the full scope of the breach.	The University of Sherbrooke isolated the affected systems to prevent further compromise and initiated an investigation into the breach.	The attack indicates that, despite existing precautions, the university's cybersecurity measures were insufficient to prevent a breach by a sophisticated ransomware gang.

Bibliography

Australian Government. “Countering the Insider Threat: A Guide for Australian Government,” n.d. https://www.ag.gov.au/integrity/publications/countering-insider-threat-guide-australian-government.

Australian Research Council. "Research Security." www.arc.gov.au/funding-research/research-security.

Barton, Rosemary. "Highly Sophisticated’ Chinese Cyber Attack Hits Canada’s Research Agency." CBC News, July 30, 2014. www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241.

Blevins, Emily, and Marcy Gallo. Research Security Policies: An Overview. Congressional Research Service.

Borys, Stephanie. “The ANU Hack Came Down to a Single Email — Here’s What We Know.” ABC News, October 2, 2019. https://www.abc.net.au/news/2019-10-02/the-sophisticated-anu-hack-that-compromised-private-details/11566540.

Center for Strategic and International Studies. "Survey of Chinese Espionage in the United States since 2000." www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000.

"Chinese Agent Targeted Canadian Scientist in Bacteria-Smuggling Plot: RCMP Documents." Business in Vancouver, 2024. www.biv.com/news/economy-law-politics/chinese-agent-targeted-canadian-scientist-bacteria-smuggling-plot-rcmp-documents-8265093.

Chu, Tammy. "The Complex Challenge of Foreign Interference in Research Administration and Compliance." Research Management Review, 2020.

Communications and Marketing Branch. "Government of Canada." Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Communications and Marketing Branch, March 31, 2023. science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/csis-and-research-security#2.

Croft, Daniel. “Australia the ‘Weakest Link’ in AUKUS on Cyber Security.” Defence Connect, March 23, 2023. https://www.defenceconnect.com.au/intel-cyber/11670-australia-the-weakest-link-in-aukus-on-cyber-security.

Department of Education. “Guidelines to Counter Foreign Interference in the Australian University Sector,” 2019. https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector.

Diamond, Larry, and Orville Schell, eds. China’s Influence & American Interests: Promoting Constructive Vigilance. Hoover Institution, Stanford University, 2018.

Doherty, Ben. "Chinese Academic Raided by Australian Police and Offered $2,000 for Information during Trip." The Guardian, September 10, 2023. www.theguardian.com/australia-news/2023/sep/10/chinese-academic-raided-asio-af.

Edwards, Lee. “Confucius Institutes: China’s Trojan Horse | the Heritage Foundation.” The Heritage Foundation, n.d. https://www.heritage.org/homeland-security/commentary/confucius-institutes-chinas-trojan-horse.

"Feds: Man Stole Cancer-Fighting Compound to Study in China." NBCNews.Com. NBCUniversal News Group. www.nbcnews.com/health/health-news/feds-man-stole-cancer-fighting-compound-study-china-flna1c9386619.

Flagg, Melissa, and Zachary Arnold. "A New Institutional Approach to Research Security in the United States." Center for Security and Emerging Technology, June 9, 2021. cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states.

“Former Harvard University Professor Sentenced for Lying About His Affiliation With Wuhan University of Technology; China’s Thousand Talents Program; and Filing False Tax Returns,” April 26, 2023. https://www.justice.gov/usao-ma/pr/former-harvard-university-professor-sentenced-lying-about-his-affiliation-wuhan.

Friesen, Joe. "Two-Thirds of Research-Grant Requests Sent to Canadian Security Agencies Rejected." The Globe and Mail, January 2023. www.theglobeandmail.com/canada/article-nserc-research-grants-sensitive/.

Goldberg, P. "MD Anderson Researchers Ousted as NIH and FBI Target Diversion of Intellectual Property." The Cancer Letter 45, no. 17 (2019): 4–8.

Government of Australia. "Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector." Last modified December 8, 2023. www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks.

Government of Canada. "National Security Guidelines for Research Partnerships." January 11, 2024. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships.

Government of Canada. “Policy on Sensitive Technology Research and Affiliations of Concern.” January 9, 2024. science.gc.ca/site/science/sites/default/files/documents/2024-01/1154-policy-strac-en-final-09Jan2024.pdf.

Government of Canada. “Research Security - Tri-agency Guidance on the National Security Guidelines for Research Partnerships (NSGRP),” 2024. https://www.nserc-crsng.gc.ca/InterAgency-Interorganismes/RS-SR/nsgrp-ldsnpr_eng.asp#a3.

Groch, Sherryn, and Daniella White. "Australia Underspends on This Key Area. It May Put National Security at Risk." The Sydney Morning Herald, November 20, 2023. www.smh.com.au/education/australia-underspends-on-this-key-area-it-may-put-national-security-at-risk-20231111-p5ej93.html.

Hart, A. "2 Emory Researchers Didn’t Disclose Chinese Funding Ties." The Atlanta Journal-Constitution, 2019. https://www.ajc.com/news/state--regional-govt--politics/new-findings-emory-researchers-didn-disclose-chinese-funding-ties/QQ58XiznSllTLYv5rARfjL/.

Happ, Stefan. "Insider Threat Programs at Universities: A Necessary Reality." https://www.utph.org/index/docs/Insider-Threat-Programs-at-Universities.pdf?language_id=1.

“Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases,” July 22, 2022. https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

Horowitz, Michael, and Lauren Kahn. "Dod’s 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China’s Military." Council on Foreign Relations, 2021. www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape.

Hurst, Daniel, and Dan Sabbagh. "Visiting Professor Used PhD Students to Gather Intelligence for China, ASIO Boss Alleges." The Guardian, October 18, 2023. www.theguardian.com/australia-news/2023/oct/18/visiting-professor-used-phd-students-to-gather-intelligence-for-china-asio-boss-alleges.

Hvistendahl, M. "Major U.S. Cancer Center Ousts ‘Asian’ Researchers After NIH Flags Their Foreign Ties." Science, 2019. https://www.sciencemag.org/news/2019/04/exclusive-major-us-cancer-center-ousts-asian-researchers-after-nih-flags-their-foreign.

"Like a Diamond Heist: How Hackers Got into Australia's Top Uni." The Canberra Times, October 28, 2019. www.canberratimes.com.au/story/6414841/like-a-diamond-heist-how-hackers-got-into-australias-top-uni/.
Libusby. "Deakin Has Been Targeted in a Cyber Attack This Week – Here's What Happened and What You Should Do." Deakin Life, July 13, 2022. blogs.deakin.edu.au/deakinlife/2022/07/12/deakin-has-been-targeted-in-a-cyber-attack-this-week-heres-what-happened-and-what-you-should-do/.
Long, Gordon. Fundamental Research Security. National Science Foundation, 2019. www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.
Malakoff, D. "Emory Ousts Two Chinese American Researchers After Investigation into Foreign Ties." Science, 2019. https://www.sciencemag.org/news/2019/05/emory-ousts-two-chinese-american-researchers-after-investigation-foreign-ties.
"Medical Test Company's 'Serious and Systemic Failures' Led to Cyber-Attack, Watchdog Says." The Guardian, November 29, 2023. www.theguardian.com/australia-news/2023/nov/29/australian-clinical-labs-hack-quantum-cyber-attack-oaic.
Mercer, Phil. "Australian University Warns of Foreign Interference on Campus." Voice of America, August 16, 2023. https://www.voanews.com/a/australian-university-warns-of-foreign-interference-on-campus-/7227177.html.
National Science Foundation. "Research Security Guidelines." 2023. new.nsf.gov/research-security/guidelines.
National Science and Technology Council. "NSPM-33-Implementation-Guidance." Last modified January 4, 2022. www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.
Office of Public Affairs. "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." United States Department of Justice, July 22, 2022. www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.
Office of Public Affairs. "Husband-and-Wife Scientists Plead Guilty to Illegally Importing Potentially Toxic Lab Chemicals and Illegally Forwarding Confidential mRNA Vaccine Research to China." United States Department of Justice, May 20, 2022. www.justice.gov/usao-sdca/pr/husband-and-wife-scientists-plead-guilty-illegally-importing-potentially-toxic-lab.
Owens, Brian. "A New Era of Research Security." University Affairs. universityaffairs.ca/features/feature-article/a-new-era-of-research-security/.
Parliament of Australia. "PJCIS List of Recommendations," 2022. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report/section?id=committees%2Freportjnt%2F024611%2F75668.
Perkuhn, Josie-Marie. "Alex Joske: Picking Flowers, Making Honey. The Chinese Military's Collaboration with Foreign Universities." SIRIUS – Zeitschrift Für Strategische Analysen 3, No. 3 (September 1, 2019): 306–307. https://doi.org/10.1515/sirius-2019-3023.
"Protective Security Policy Framework." Protective Security Policy Framework, 2024. www.protectivesecurity.gov.au/.
Public Safety Canada. "Enhancing Canada's Critical Infrastructure Resilience to Insider Risk," July 28, 2022. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx.
Public Safety Canada. "The Insider Risk Assessment Tool," October 24, 2022.

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/irat-oari-en.aspx.
QIMR Berghofer. "QIMR Berghofer Investigates Suspected Accellion Data Breach." February 2021. www.qimrberghofer.edu.au/media-releases/qimr-berghofer-investigates-suspected-accellion-data-breach/.
Ravlic, Tom. “ASIO Opposes Publication of Its University Monitoring Activities.” The Mandarin, February 16, 2023. https://www.themandarin.com.au/212476-asio-opposes-publication-of-its-university-monitoring-activities/.
"Sensitive Student Information Exposed in University of Western Australia Data Breach." CDP Institute, August 25, 2022. www.cdpinstitute.org/news/sensitive-student-information-exposed-in-university-of-western-australia-data-breach/.
Shepherd, Tory. "University Students and Staff Face Increasing Threats, Foreign Interference Inquiry Finds." The Guardian, March 25, 2022. www.theguardian.com/australia-news/2022/mar/25/university-students-and-staff-face-increasing-threats-foreign-interference-inquiry-finds.
Solomon et al. "Ransomware Gang Starts Leaking Data Stolen from Quebec University: IT World Canada News." IT World Canada, January 4, 2024. www.itworldcanada.com/article/ransomware-gang-starts-leaking-data-stolen-from-quebec-university/555809.
Stoff, Jeffrey. "Should Democracies Draw Red Lines around Research Collaboration with China? A Case Study of Germany." Gemeinsamer Ausschuss Zum Umgang Mit Sicherheitsrelevanter Forschung, September 1, 2023. www.security-relevant-research.org/should-democracies-draw-redlines-around-research-collaboration-with-china-a-case-study-of-germany/.
The National Counterintelligence and Security Center. “Research Security,” 2024. https://www.dni.gov/index.php/safeguarding-science/research-security?highlight=WyJzIiwiJ3MiXQ.
The White House. "An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity." Last modified September 1, 2022. www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/.
Trager, Rebecca. “Two Canadian Scientists Were Fired in 2021 for Passing Information to China.” Chemistry World, June 10, 2024. https://www.chemistryworld.com/news/two-canadian-scientists-were-fired-in-2021-for-passing-information-to-china/4019098.article.
Tunney, Catharine. "Canada Names 100 Chinese, Russian, Iranian Research Institutions It Says Pose a Threat to National Security." CBC News, January 16, 2024. www.cbc.ca/news/politics/reserach-canada-china-russia-iran-1.7085391.
Tunney, Catherine. "Scientist Fired from Winnipeg Disease Lab Intentionally Worked to Benefit China: CSIS Report." CBC News, February 29, 2024. www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7128865.
U.S. Department of the Treasury. "Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities." March 23, 2018. home.treasury.gov/news/press-releases/sm0332.
"University of Winnipeg Extends Semester after Confirming It Was Targeted by Cyberattack." CBC News, March 27, 2024. www.cbc.ca/news/canada/manitoba/cyber-attack-university-winnipeg-classes-network-1.7157650.
Walker-Munro, Brendan. “Australia Risks Falling Behind Allies on Research Security. Will It

Take a Spy Scandal in Our Universities to Catch Up?" The Conversation, n.d. https://theconversation.com/australia-risks-falling-behind-allies-on-research-security-will-it-take-a-spy-scandal-in-our-universities-to-catch-up-221602.
Walker-Munro, Brendan. "Submission to the Department of Education Interim Report on the Universities Accord." 2023. https://www.education.gov.au/system/files/2023-08/AUA_inter_tranche3_040%20Brendan%20Walker-Munro.pdf.
Walker-Munro, Brendan. "Why Isn't Australia Securing Its Critical Research?" EduResearch Matters, January 17, 2024. https://blog.aare.edu.au/why-isnt-australia-securing-its-critical-research/.
Walker-Munro, Brendan, Leanne Jorari, Robert E Kelly, and Roland Rajah. "Why Universities Are Still at Risk for Foreign Interference." Lowy Institute, April 1, 2021. https://www.lowyinstitute.org/why-universities-are-still-risk-foreign-interference.
Walker-Munro, David Mount, and Ruby Ioannou. "Are We Training Potential Adversaries? Australian Universities and National Security Challenges to Education." TC Beirne School of Law Publications, n.d.
Wilner, A., S. Beach-Vaive, C. Carbonneau, G. Hopkins, and F. Leblanc. "Research at Risk: Global Challenges, International Perspectives, and Canadian Solutions." International Journal 77, no. 1 (2022): 26-50. https://doi.org/10.1177/00207020221118504.

Country	Incident Overview	Nature of the Threat	Impact Assessment	Response and Mitigation	Evaluation
Australia	A Chinese national, acting as a spy under the guise of a visiting professor, attempted to infiltrate a prestigious Australian research institution to collect sensitive information. The spy was provided with funding and a list of intelligence requirements from their government. The individual involved was a Chinese national recruited by Chinese intelligence. The targeted entity was an Australian research institution, which was not named .	The incident is categorized as foreign interference, as a spy was strategically placed inside an educational establishment to carry out espionage activities. The strategy included enlisting an academic who thereafter used their role to allocate studies that were in line with the intelligence objectives of a foreign nation. Although the specific field of research was not disclosed, it involved an area valuable enough to attract international espionage efforts.	The swift action by the Australian Security Intelligence Organization (ASIO) thwarted the attempt before any known damage could be inflicted on the integrity of the research institution's work or intellectual property .	ASIO intervened promptly, removing the academic from Australia and preventing the espionage plan from succeeding.	Preceding the incident, it is evident that there were protocols designed to detect and address potential espionage risks inside the scientific establishments of Australia. The incident's public exposure and the actions of the ASIO demonstrate a response to the changing landscape of research espionage, namely from players such as China. However, the research institution in question should have had the framework to detect this threat.
Australia	A sophisticated spear-phishing attack, allegedly funded by the Iranian government, targeted multiple Australian universities, stealing a vast amount of academic data. The perpetrators were associated with the Iran-based Mabna Institute. The targets included 26 Australian universities, with the Group of Eight as prominent victims (Australia's research-oriented universities similar to the U15 – the University of Melbourne, the Australian National University, the University of Sydney, the University of Queensland, the University of Western Australia, the University of Adelaide, Monash University and UNSW Sydney).	This incident is classified as foreign cyber espionage; the campaign involved spear-phishing to trick academics into providing login credentials, which were then used to access and exfiltrate academic resources materials.	The immediate impact was the unauthorized access and theft of over 31 terabytes of data, potentially undermining the research integrity and intellectual property of the targeted institutions; the state-sponsored nature of the attack and the scale of the theft highlight the vulnerability of academic institutions to cyber espionage and the potential implications for national security.	The US Department of Justice, given that American institutions were targeted as well, charged nine Iranians in connection with the theft, suggesting a law enforcement and diplomatic response to the incident. While specific mitigation measures taken by the Australian universities and the government are not detailed, the scale of the incident likely prompted a reassessment of cybersecurity protocols and defenses against such phishing campaigns.	The success of the spear-phishing campaign suggests that existing measures were not fully effective in preventing such sophisticated social engineering attacks. The response led to legal action against the perpetrators, indicating international collaboration in addressing the threat.
Australia	Australian National University (ANU) suffered a sophisticated cyberattack targeting personal data and potentially research data. Detected in April 2019, the attack occurred between November 2018 and May 2019 in Canberra, Australia.	This was indicative foreign interference: the attack employed credential theft, infrastructure compromise, and advanced malware, demonstrating high capability and persistence. Personal data from the ANU's systems, with potential interest in research data.	Unauthorized access to personal data and sensitive material, with the extent of data theft initially feared to be 19 years of records but later reassessed. Implications were severe for individuals whose data was compromised.	Upon the detection of the compromise, the cyber team at ANU, in collaboration with Northrop Grumman and several government agencies, executed a sophisticated forensic response. Following the event, it is probable that ANU has boosted its investment and implementation of cybersecurity measures, however the particular long-term goals were not explicitly outlined.	ANU had standard cybersecurity measures in place, which were insufficient to prevent the sophisticated attack. The response was effective in uncovering the breach; however, it was not timely enough to prevent data exfiltration. The incident has prompted a reassessment of cybersecurity practices at ANU, indicating a shift toward more robust defenses.
Australia	A privacy breach occurred at the Australian Research Council (ARC) from a possible insider, leading to the unintended disclosure of residency details of grant applicants to assessors.	This incident represents an insider threat to privacy, possibly due to a process or system flaw. Although not specified, the breach could result from a technical oversight or human error in the data handling process. The breach directly impacts the confidentiality aspect of the research grant application process.	The breach could affect the trust and integrity of the grant application process and the privacy of applicants.	The ARC's immediate action was to instruct assessors to delete the files containing the breached information and initiate an internal investigation. Depending on the outcome of the investigation, the ARC will likely revise its data handling procedures to prevent future breaches.	It appears there may have been vulnerabilities in the ARC's data management systems that allowed the breach to occur. The effectiveness of the ARC's response will depend on the thoroughness of the investigation and the implementation of corrective measures. The ARC's ability to adapt its policies and practices in light of this breach will be critical in restoring confidence in its data and research security measures.

Australia	A data breach occurred at QIMR Berghofer Medical Research Institute due to a compromised third-party file-sharing service, Accellion, which led to unauthorized access to clinical trial data. Announced in February 2021, the breach impacted the Brisbane-based research institute. QIMR Berghofer, Accellion (the third-party service provider), and unknown attackers, with links suggested to the Iranian government.	This was a foreign state-led cyberattack exploiting a zero-day vulnerability in Accellion's software. The attackers utilized a sophisticated cyber intrusion technique to exploit the vulnerability and access data. Data related to clinical trials for anti-malaria drugs, as well as resumes of research staff, were accessed.	Unauthorized access to de-identified clinical trial participant information and staff resumes, leading to potential intellectual property theft and privacy concerns. The breach has wider implications for data security in medical research and raises concerns about the security of third-party services.	The institute implemented a security patch provided by Accellion and began an internal investigation; QIMR Berghofer has expressed intentions to review and enhance protocols for using third-party file-sharing services.	Accellion provided QIMR Berghofer with services that were believed to be safe until flaws were discovered during the hack. Although the breach did occur, the prompt installation of the security patch and the investigation show a proactive reaction. The institution demonstrates flexibility in fortifying their defenses with their dedication to reviewing third-party service procedures and guaranteeing safe storage.
Australia	After Australian Clinical Laboratories was the target of a cyberattack, over 200,000 client records, private data, and clinical research data were leaked to the dark web .	The attack, executed by the Quantum hacker group, involved data exfiltration.	Immediate impact included the breach of customer privacy and potential financial fraud. Broader implications involve the erosion of trust in data security practices.	An internal investigation was initiated, and the Office of the Australian Information Commissioner (OAIC) took legal action due to systemic failures in cybersecurity.	Pre-incident measures were found to be inadequate, with an absence of a dedicated cybersecurity team.
Australia	Unauthorized access to Deakin University's system via a third-party provider led to the theft of 46,980 students' personal information along with scholarly work from various databases.	Cyberattack exploiting a third-party service through phishing to obtain login credentials and subsequent data theft. There are reports of this infiltration being facilitated by an insider.	Risk of identity theft and payment fraud for affected students. Highlights vulnerabilities in university data security, particularly related to third-party services.	Investigation launched; affected individuals notified. Review of third-party service use and security enhancements, including the consideration of multi-factor authentication (MFA) to prevent similar breaches.	Potential lack of stringent cybersecurity measures for third-party services. The thorough investigation and public acknowledgment are positive steps, but the delayed response and initial security gaps suggest room for improvement. Deakin's response includes working to strengthen security practices, indicating a willingness to adapt and improve RS measures.
Australia	A breach in the University of Western Australia's Callista system exposed sensitive student and alumni data, including scholarly research, due to unauthorized access, marking a significant security incident within the educational sector.	This cyberattack, facilitated possibly through a phishing scheme or insider, represents a severe intrusion, leveraging a third-party vulnerability to compromise data integrity and privacy.	The immediate impact involved the risk of identity theft for individuals whose data was compromised; broader implications concern the potential exposure of sensitive research and academic achievements, affecting the institution's reputation and trust.	The university promptly initiated an investigation, involving law enforcement, and advised the affected community to monitor for suspicious activity, indicating a responsive and responsible approach to the breach.	This case evidences potential pre-existing vulnerabilities within the university's data security framework, especially concerning third-party services - the institution's adaptability to strengthen its cybersecurity measures post-incident will be crucial for future resilience.
US	Dr. Charles Lieber, the Chair of Harvard University’s Chemistry and Chemical Biology Department, along with two Chinese nationals, were charged with aiding the People’s Republic of China. Dr. Lieber was arrested on January 28, 2020, with court proceedings and further developments occurring throughout 2020 and 2021 in Boston, Massachusetts. Other entities involved included two Chinese nationals—Yanqing Ye and Zaosong Zheng.	This case presents a blend of insider risk and foreign interference, with Dr. Lieber accused of concealing his involvement with the Chinese Thousand Talents Plan. The tactics involved Dr. Lieber receiving financial incentives to collaborate with Wuhan University of Technology (WUT) in China without proper disclosure to US federal agencies. Nanoscience was the targeted research area with significant grant funding from the National Institute of Health (NIH) and the Department of Defense (DoD) involved.	The incident led to the arrest and charging of Dr. Lieber, disruption of research activities, and potential reputational damage to Harvard University; this breach has increased concerns over the integrity of academic research, potential loss of sensitive technology, and financial conflicts of interest within higher education and research institutions.	The immediate arrest of Dr. Lieber and charges against the involved parties. Ongoing investigations and trials, along with increased scrutiny on international collaborations by research institutions.	The measures appear to have gaps, as significant foreign affiliations and financial conflicts of interest went undisclosed. The response was robust with legal action, but the effectiveness of the pre-existing RS framework is in question. The incident likely prompted a re-evaluation of disclosure policies and the need for greater oversight of international collaborations by research institutions and funding provisions by granting agencies.

US	Two veteran researchers at Emory University were removed from their positions for failing to disclose foreign sources of research funding and the extent of their work with research institutions in China. The case involves undisclosed foreign financial conflicts of interest. The incident came to light on May 23, 2019, at Emory University in Atlanta, Georgia. The researchers, Li Xiao-Jiang and Li Shihua, geneticists specializing in CRISPR gene editing, were found to have ties with Chinese research institutions.	This incident represents a combination of insider risk and foreign interference due to undisclosed financial ties and collaboration with foreign entities that could potentially conflict with US interests. The researchers received undisclosed funds from Chinese sources and were involved in collaborative work with research institutions in China without proper disclosure. Their work in the field of genetics involved using CRISPR technology to create engineered animal models for studying human diseases.	The immediate impact was the dismissal of the researchers from Emory University, the closure of their laboratory, and the confiscation of computers and documents. This case heightened concerns about foreign influence in academia and the need for transparency in disclosing foreign collaborations and funding.	Emory University conducted an internal investigation after receiving communication from NIH and terminated the employment of the researchers. The university also stated its commitment to the free exchange of ideas and research collaboration. In the broader context, since this incident, there has been an increased effort to enforce disclosure requirements for federally funded researchers in accordance with federal RS requirements, as well as a general tightening of rules regarding foreign influence in research.	The framework at Emory University, as with many US research institutions prior to NSPM-33, was likely not fully prepared to detect and prevent the kind of undisclosed foreign involvement that occurred in this case. Responses from Emory University were decisive in terminating the researchers and communicating with NIH, indicating an effective immediate reaction to the incident.
US	MD Anderson Cancer Center terminated three senior researchers after being informed by NIH that they may have violated rules involving the confidentiality of peer review and disclosure of foreign ties. The disclosures occurred in Houston, Texas, with the terminations coming to light in April 2019. MD Anderson Cancer Center, NIH, the researchers involved (who remain unnamed in the reports but are described as ethnically Chinese).	The case indicates a mix of potential insider risk, given the confidentiality breach, coupled with foreign interference due to undisclosed foreign ties. Alleged inappropriate sharing of confidential grant information and failure to disclose foreign relationships and resources. Though not specified in the case details, the research likely pertained to areas funded by NIH grants at MD Anderson Cancer Center.	The immediate result was the initiation of termination proceedings against the researchers and heightened scrutiny of faculty members' foreign connections, with implications for research integrity and institutional trust. This incident contributes to an atmosphere of increased vigilance concerning foreign influence within US research institutions, potentially affecting international collaborations and the research community at large.	MD Anderson responded to NIH's concerns by conducting internal investigations and initiating termination procedures for the implicated researchers. Following federal RS requirements, there have been ongoing efforts by NIH to ensure transparency and mitigate risks associated with foreign ties, along with institutional actions to address and safeguard against such threats.	The presence of undisclosed foreign ties suggests that pre-existing measures may have been insufficient to detect or prevent breaches of this nature.
US	Huajun Zhao, a researcher at the Medical College of Wisconsin, was charged with economic espionage, accused of stealing research data and materials for a cancer-fighting compound, C-25.	This case is classified as economic espionage, where a researcher exploited his position to misappropriate proprietary research material with the intent to benefit a foreign entity. Zhao allegedly stole vials of a substance called C-25 and took steps to provide it to Zhejiang University in China. He is also accused of copying and deleting research files from MCOW computers. The targeted research was in the field of cancer treatment, specifically related to the compound C-25, a potential anticancer agent.	The incident led to the arrest of Zhao, disruption of research activities at the Medical College of Wisconsin, and potential loss of proprietary research material. After this case there was an increase in concerns regarding the vulnerability of US research institutions to economic espionage, particularly involving foreign entities.	The Medical College of Wisconsin cooperated with the FBI, and law enforcement actions led to Zhao's arrest. The investigation and legal proceedings against Zhao served as a deterrent against similar acts of espionage. It highlighted the need for stringent security measures and thorough vetting of research personnel.	The fact that Zhao was able to access and delete research data suggests that there were vulnerabilities in the pre-existing RS framework. The swift response by the FBI and the institution's cooperation signify a robust approach to handling the detected threat; the incident likely prompted the Medical College of Wisconsin and other institutions to bolster their security protocols and monitoring systems to prevent future incidents of espionage.
US	Emory University terminated two faculty members in the Department of Genetics for failing to disclose foreign sources of funding and their involvement with institutions in China. The terminations were announced in June 2019, at Emory University in Atlanta, Georgia.	The incident represents a blend of insider risk due to the failure to disclose significant foreign affiliations and potential foreign interference by leveraging undisclosed foreign ties. Again, the non-disclosure of foreign sources of funding and extent of work for research institutions and universities in China put genetics research, specifically research using CRISPR gene editing in animal models for human diseases, under risk.	This case contributes to the national dialogue on the integrity of federally funded research and the potential for foreign influence, impacting trust in academic and research institutions.	Prompt investigation by Emory University in response to an NIH inquiry, led to the termination of the involved faculty members. Emory University minimized disruption within the department and ensure the continuity of research projects, along with increased awareness and compliance measures regarding funding disclosure requirements.	The incident highlights potential gaps in the institutional framework for monitoring and ensuring full disclosure of foreign affiliations and funding sources by faculty members .

US	Idaho National Laboratory, a leading US facility for cybersecurity, nuclear, and clean energy research, experienced a significant data breach. An unauthorized access targeted its HR systems, leading to the exposure of both employee and research data. The breach was detected and reported in early 2023.	This incident combines elements of cyber-espionage with insider risk, given the focus on HR systems and potential access to sensitive employee data.The breach involved unauthorized access to INL's Oracle HCM system, supporting human resources applications, likely through cybersecurity vulnerabilities. While directly impacting HR systems, the breach poses a secondary threat to the broader research initiatives at INL by potentially exposing research personnel's sensitive data.	The breach led to the exposure of personal and employment information for potentially thousands of employees and research data, affecting their privacy and INL's operational security. The incident undermines trust in INL's capability to secure critical infrastructure, especially given its role in cybersecurity. It raises questions about the effectiveness of current security measures against sophisticated cyber threats.	INL promptly initiated protective measures to secure employee data and collaborated with federal law enforcement for investigation. Mitigation steps included reviewing and enhancing cybersecurity practices, potentially increasing multi-factor authentication measures, and educating employees on cybersecurity hygiene.	The incident reveals potential vulnerabilities in the pre-existing cybersecurity framework, particularly concerning the protection of HR systems and sensitive employee data. The quick action to engage law enforcement and secure systems reflects a strong response capability. However, the breach's occurrence indicates a need for review and reinforcement of existing security measures. This event prompted a reevaluation of cybersecurity strategies at INL, emphasizing the need for continuous adaptation to emerging cyber threats and strengthening the resilience of HR and research data systems.
US	Xiwen Huang, a Chinese businessman and naturalized US citizen, was charged with theft of trade secrets after engaging in a scheme to steal confidential information from US government research facilities, with the intent to benefit a Chinese company and himself .	The immediate repercussions of Huang's theft on the research facilities included potential compromise of proprietary technologies and methodologies critical to US defense and energy sectors. The broader implications resonate with the risk of undermining US technological leadership and jeopardizing the security of critical infrastructure, given the military applications of the stolen research.	The theft put at risk the economic interests and jobs in North Carolina by potentially allowing foreign competitors to gain an unfair advantage.	Federal custody of Huang following his arrest upon returning from China, with cooperation between the FBI and the US Attorney's Office leading to charges. Mitigation measures included legal prosecution of Huang, including a plea agreement with expectations of a formal guilty plea to be entered in court .	Vulnerabilities in protecting trade secrets and the need for enhanced security and vigilance within companies and government research facilities are highlighted by this case.
US	Li Chen pleaded guilty to conspiring to steal scientific trade secrets related to exosomes and their isolation from Nationwide Children's Hospital's Research Institute. The stolen trade secrets were intended for personal financial gain and sale in China.	This particular case illustrates examples of economic misconduct and the unauthorized acquisition of intellectual property, specifically pertaining to trade secrets associated with medical research. Mr. Chen and Zhou engaged in a conspiracy to illicitly acquire a minimum of five trade secrets pertaining to exosome research, capitalizing on their authority inside the research organization. This incident might be classified as an instance of insider threat. The study of exosomes has great importance in the realm of pediatric medicine as it aids in the detection and treatment of many medical disorders.	The theft directly compromised the confidentiality and integrity of sensitive research developments at Nationwide Children's Hospital, leading to financial and reputational damage. This case illustrates the broader issue of economic espionage related to the PRC, contributing to the global dialogue on protecting intellectual property against foreign theft.	Nationwide Children's Hospital cooperated with the investigation, which led to Chen's guilty plea. The FBI and other federal agencies were involved in the investigation and legal process. Li Chen agreed to forfeit approximately $1.4 million, along with significant shares in related corporations, as part of her plea agreement.	The incident exposes possible deficiencies in Nationwide Children's Hospital's measures to safeguard its intellectual property, namely with the comprehensive evaluation and supervision of research personnel who have access to confidential data.
US	Yu Zhou pleaded guilty to conspiring to steal scientific trade secrets related to exosomes from Nationwide Children's Hospital's Research Institute, aiming to personally profit in China.	This is a case of economic espionage with the intent to transfer American scientific innovations to China for personal gain. Zhou, alongside his wife, engaged in a conspiracy to misappropriate research findings and methodologies for isolating exosomes—a critical area of pediatric medical research. The targeted research area was exosome research significant for identifying and treating various medical conditions, including necrotizing enterocolitis in premature babies, liver fibrosis, and liver cancer.	The theft of trade secrets undermines the research integrity at Nationwide Children's Hospital and represents a financial and competitive loss and poses a risk to the US' national economic security.	The prompt legal action leading to the guilty pleas of Zhou and Chen illustrates the US commitment to countering intellectual property theft.	Vulnerabilities in detecting and preventing the misappropriation of sensitive research were prevalent within this research institution.

US	Chenyan Wu and Lianchun Chen, both research scientists, pleaded guilty to charges related to illegally importing lab chemicals and sharing confidential mRNA vaccine research from a major American pharmaceutical company with China. Wu moved to China and opened TheraMab to focus on mRNA vaccine research, while Chen remained in the US, working for the same company and sending confidential materials to Wu.	The actions of Wu and Chen represent economic espionage and intellectual property theft. They conspired to advance competing laboratory research in China by stealing trade secrets from an American pharmaceutical company.	The immediate impact of their actions includes the breach of confidential research data, which could have advanced scientific knowledge and commercial interests in China at the expense of American innovation. The broader implications include heightened concerns over the security of sensitive research data and international trust in collaboration.	The Department of Justice is committed to protecting American intellectual property and the concerted efforts by law enforcement agencies to curb the illegal transfer of trade secrets to foreign entities.	This case illustrates the ongoing challenge of safeguarding sensitive research data against espionage. It highlights the importance of stringent security protocols within research institutions and pharmaceutical companies to detect and prevent unauthorized access and transmission of proprietary information.
Canada	Dr. Xiangguo Qiu and her husband Keding Cheng were dismissed from the National Microbiology Lab after an investigation revealed they might have been working to benefit China, including sharing sensitive scientific information without authorization. The couple was removed from the lab in July 2019, with their firing announced in January 2021. The investigation and full public revelation occurred over several years, concluding around March 2024.	The incident represents a combination of insider risk and foreign interference, highlighting potential espionage and unauthorized transfer of sensitive information to China. Activities included unauthorized sharing of scientific data, such as genetic sequences of pathogens like Ebola, and potentially breaching security policies regarding lab access and material shipment.	The incident raised serious national security concerns, led to the termination of the involved researchers, and potentially compromised sensitive research.	Suspension of security clearances and employment termination followed PHAC's administrative report and CSIS's security reassessment. Mitigation measures include an ongoing RCMP investigation, enhanced security protocols at the NML, and broader national efforts to secure intellectual property and sensitive research from foreign interference.	The case indicates gaps in the oversight of international collaborations and employee conduct within high-security research settings. The response highlights the challenges of detecting and mitigating insider threats, especially when they involve complex national security considerations .Such an incident has likely prompted a reevaluation of security measures within Canada's scientific research community, emphasizing the need for rigorous vetting, monitoring, and enforcement of compliance with security policies.
Canada	The University of Winnipeg experienced a cyberattack targeting its network, causing significant disruptions including class cancellations, internet outages, and exam delays. It is highly possible that research was targeted by the threat actors, though personal information of students was the main target.	This threat is still being investigated.	Cyberattacks aimed at disrupting educational operations and potentially accessing sensitive information. The specific methods used in the attack were not detailed, but such attacks typically involve phishing, malware, or exploiting network vulnerabilities.	Immediate impacts included the cancellation of classes, internet downtime, and delays in exams, causing significant disruption to academic activities. The attack is part of a growing trend of cyberattacks against educational institutions, underscoring the vulnerability of such entities to cybersecurity threats and the potential long-term impacts on institutional reputation and trust.	The University of Winnipeg initiated an investigation to understand the impact and took steps to mitigate further damage. They also planned a town hall to update the community.
Canada	Dr. Klaus Nielsen, a scientist at the Canadian Food Inspection Agency (CFIA), was targeted by espionage to obtain his research on brucellosis. He was arrested while attempting to transport vials of brucella bacteria to China.	This case represents a direct act of espionage with the intent to transfer sensitive scientific research from Canada to China for commercial gain.	The immediate impacts included the arrest of Dr. Nielsen, the disruption of his research activities, and legal proceedings that led to his conviction.	Apart from the arrest, no other major responses were noted.	Prior to the incident, there may have been insufficient safeguards to prevent such a breach of security and espionage within the CFIA. The response, while ultimately successful in apprehending Nielsen, highlighted gaps in detecting and preventing espionage activities within government research entities.
Canada	A highly sophisticated Chinese state-sponsored actor successfully hacked into the NRC's (National Research Council's) computer systems. This cyberattack was identified by the Communications Security Establishment Canada.	The attack was a targeted cyber-espionage effort aimed at stealing scientific research and data from the NRC. The exact methods used in the cyberattack were not disclosed, but it involved sophisticated techniques indicative of a state-sponsored actor. the NRC engages in various fields of scientific research and technological development, making it a valuable target for cyber-espionage activities.	The cyberattack led to the isolation of the NRC's IT system from the rest of the government's networks to prevent further breaches. It disrupted the NRC's operations, including its collaborations with private businesses.	The NRC and Canadian officials took immediate steps to isolate the compromised systems and began efforts to rebuild the NRC's IT infrastructure, a process that took up to a year. The incident prompted discussions at the highest levels between Canada and China, with Canadian officials raising the issue directly with their Chinese counterparts.	Such a cyberattack revealed the gaps in cybersecurity measures at the NRC.

Canada	The LockBit ransomware gang claimed responsibility for a cyberattack on the University of Sherbrooke, compromising data from one laboratory.	This incident is categorized as a ransomware attack, a malicious attempt to deny access to the institution's data or systems, often with a demand for payment in exchange for restoring access or not leaking the data. The specific techniques used by the LockBit gang were not detailed but typically involve encrypting files on the victim's network and demanding a ransom for the decryption key. Data from one laboratory was compromised, though details on whether this included personal information or intellectual property were not disclosed.	The attack led to the compromise of critical data, but the university stated that its activities had not been impacted. Ongoing investigations aim to assess the full scope of the breach.	The University of Sherbrooke isolated the affected systems to prevent further compromise and initiated an investigation into the breach.	The attack indicates that, despite existing precautions, the university's cybersecurity measures were insufficient to prevent a breach by a sophisticated ransomware gang.