University Foreign Interference Case Studies

Examples of Foreign interference

What can foreign interference look like in universities?

- Seeking to inappropriately influence:
  - course content
  - research directions
  - staff and student actions.
- theft of intellectual property or gain of an undue commercial, technical, or intellectual advantage over Australian universities.
- threats, intimidation, harassment of students or university staff, either online or in person; and
- cultivation of university staff or students for espionage or further foreign interference against Australia.

In an effort to enhance awareness of foreign interference, security professionals within the university sector have provided the Counter Foreign Interference Centre with the following anonymised case studies:

Case Study: Academic Targeted for Disruption

Summary

- A senior academic researcher was targeted by a foreign state actor.
- The target was likely targeted due to their research area specifically relating to maritime defence policy and anti-piracy, and / or previous work in cooperation with the Royal Australian Navy in an academic/research capacity.
- The user was targeted by a spear phishing campaign (eight emails) impersonated the s. 37(2)(b) s. 37(2)(b)
- The attack was unsuccessful.

Identification

- An initial anonymous complaint highlighted the first case.
- Subsequent cases of secondary employment were uncovered by the due diligence process.
- The spear phishing campaign impersonated the s. 37(2)(b) a legitimate organisation, s. 37(2)(b) s. 37(2)(b)
- No data was exfiltrated as part of this attack.

Released by Department of Home Affairs under the Freedom of Information Act 1982

Link to Foreign Interference
• The target of the attack was an academic involved in research areas likely determined to be of value to a foreign threat actor, specifically relating to maritime defence policy and anti-piracy. • The academic had previously worked in cooperation with the Royal Australian Navy in an academic/research capacity.
Action
• An initial anonymous complaint highlighted the first case • Subsequent cases of secondary employment were uncovered by due diligence process • The spear phishing campaign impersonated the Council on Foreign Relations, a legitimate organisation, and used a theme of claiming that the Council wanted to be involved in writing a book with the target's involvement. • No data was exfiltrated as part of this attack.
Lessons Learnt
• The targeting of researchers is not uncommon. • Researchers, unless they work in areas of obvious sensitivity, do not expect this type of event to occur to them or their colleagues.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Academic Visitor Request

Summary

- Request from overseas academic to visit a Faculty for period one year to conduct collaborative research
- Area of research in cyber science - cryptography
- Academic home institution identified as high risk for foreign interference through publicly available due diligence resources
- The University conducted due diligence - assessed cyber, research and FI risks, guidance was provided to the Dean of host faculty, visitor request was declined

Identification

- Faculty has received ongoing education about FI risk, through leadership roadshow sessions and in the due diligence process of individual activities.
- The activity was identified by a member of the Faculty and raised in the request to HR for consideration. HR escalated the visit request for further consideration.
- Risks around the proposed visitors home institution were identified through due diligence conducted utilising open source resources

Link to Foreign Interference

- The request was assessed high risk against the UFIT Due Diligence Assistance Framework for FI risk.
- The home institution of the proposed visitor identified as very high FI risk.
- The area of research - cryptography has dual use potential in defence/warfare

Action

In consideration of the cyber risks associated with hosting this proposed visitor for a year, the University cyber risk team did consider how to mitigate the risks and made recommendations should they be required. As the visit did not proceed no actions were required.

Lessons Learnt

The potential impacts of the activity could have been:

- Compromise the University's IT systems, creation of potential vulnerabilities
- Loss/misuse of valuable or sensitive research or data
- Research funding impacts e.g. impact on confidence of Australian funding bodies to fund the University/academic, or directly restrict eligibility for US Government funding opportunities
- Reputational damage to the University as a trusted partner in research, education and innovation

s. 37(2)(b)

Released by Department of Home Affairs under the Freedom of Information Act 1982

Case Study: Alleged Intimidation of Staff

Summary

- Request by international students (via a post in a subject discussion forum) to alter a list of countries (provided for an assignment task) by removing Taiwan from the list of countries on the basis that China claims sovereignty over Taiwan and that it should therefore not be listed as a 'country.'
- It was alleged by another student that the students making this request attempted to intimidate the teaching team into making this change.

Identification

- The University was alerted by a student to the alleged conduct.

Link to Foreign Interference

- The concerns were that the alleged behaviour was possibly organised, and intimidatory towards staff members and potentially other students in the class. These concerns triggered further investigation internally.

Action

Prior to this matter occurring, the University had published public and student facing communications material indicating the University's approach to mitigating the risk of foreign interference, examples of how foreign interference may manifest, and information on how members of the University community could report any concerns.

After the matter occurred, a review of the alleged incident was undertaken under the authority of the relevant Faculty Dean. This found that the staff member had removed Taiwan from the list after consulting DFAT material. The investigation found that none of the teaching staff felt intimidated or unduly pressured to alter the country list. However, it was noted that the staff member made the change without discussing this matter with other staff, and without explaining the reason behind the removal to students.

The Chair of the University's Committee overseeing the University's response to the UFIT guidelines determined that while there was no evidence meeting a threshold of 'foreign interference', there was scope to improve guidance and advice given to teaching academics encountering such requests.

Lessons Learnt

The potential impacts of the activity could have been:

- Restriction of freedom of speech
- The possibility of harassment of staff and students
- Loss of confidence by students and staff if it appeared the University would tolerate any of the above.

The University's Deputy Vice Chancellor overseeing teaching discussed the matter with all faculty deans. This provided the University with an opportunity to:

- underline its commitment to freedom of speech and academic freedom;

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

- to provide further guidance for teaching staff encountering students raising sensitive geopolitical issues - staff were recommended to seek advice from senior faculty staff in the first instance before acting, noting these staff can discuss and
- escalate the matter if required; and
- to remind faculty leadership of sources of guidance and support within the University available to help the faculties discuss and act on any allegations of foreign interference.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Coordinated Suspicious Applications for Study Exchanges

Summary

- Over a period of 12 months, an Australian University received several requests from foreign students who sought to visit the university as part of their PhD studies. These students were all undertaking research at the same foreign research institute and publication data indicated that they were part of the same research group.
- s. 37(2)(b)
- Each student disclosed that their visit would be financially supported by a scholarship administered by their government.

Identification

- These visits were referred by various academics to the Australian
- University's research security function for enhanced due diligence.

Link to Foreign Interference

- In conducting enhanced due diligence, the Australian University established that the foreign research institute where the students were studying at had significant institutional ties to their domestic defence and aerospace sector. Moreover, this foreign research institute had promoted career opportunities related to air-to-air missile systems. The Australian University determined that hosting students affiliated with this foreign research institute was inconsistent with Australia's national interests.
- s. 37(2)(b)

s. 37(2)(b) The Australian University determined that hosting students who had co-authored these publications was inconsistent with Australia's national interests.

Action

- The University conducted enhanced due diligence in relation to these visits and determined that it exceeded enterprise tolerances for foreign interference risk. Accordingly, the University did not allow for these visits to proceed.

Lessons Learnt

- This incident has advanced the University's understanding of the threat landscape

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Digital Repression

Summary

Lisa (not real name) is an international student who resides on campus at an Australian university.

Lisa believes that her home country has digitally targeted her due to her political advocacy work. Lisa has written a number of student articles that support pro-democracy values and have critically fact checked official media reports from her home country. Lisa has also participated in a number of peaceful protests on campus and engaged in respectful discussion in university forums and debates.

Lisa recounts that following this advocacy work she has received:

- multiple suspicious emails asking to discuss her articles. These emails encourage Lisa to click on hyperlinks in order to arrange a time to discuss.
- An email that contained a photo of Lisa at a university protest. The email also included Lisa's full name, phone number, social media accounts and physical address in Australia.
- A post-it note on her university door, which said traitor.
- A number of notifications of unsuccessful and unauthorised attempts to log into Lisa's social media accounts.
- A large number of negative reviews on her student articles. The reviews often include personal threats to Lisa or contain misinformation. Lisa believes that these reviews are from troll and bot accounts as the accounts were recently created, are not verified and have very few followers.
- A video call from her home country to discuss Lisa's visa arrangements. During the call, it was made clear that the foreign government official was sitting with Lisa's parents at her family home. The official also described Lisa's participation in protests as problematic and encouraged Lisa to cease her involvement in such activities.
- Messages from Lisa's family that they have been followed and harassed in the home country. Lisa's family also advise that they have been denied travel visas and are unable to come and visit Lisa.

Lisa has outlined that these experiences have affected her mental health. Lisa no longer feels safe on campus and is in a state of constant anxiety and stress. Lisa has expressed that she will not post any more articles over fears of what will happen to her or her family.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Pressure for Collaboration in Dual Use Research

Summary

An overseas-born Australian academic whose research has possible dual use applications is pressured to accept a visiting junior academic from their country of origin for a year-long 'Visiting Academic' position.

s. 37(2)(b)

The Australian academic is approached by a former senior colleague from a university that they have previously worked at in their country of origin, and asked if they will accept a recent PhD graduate as a visiting academic researcher in their lab and for fieldwork for twelve months. They are told that this will be paid for by the foreign government, but a decision has to be made quickly, as the closing date for the funding program is approaching.

When the Head of School reviews the application they realise that there are military dual-use applications of the research, and when they review the proposed Visiting Academic's CV they see that they are employed at a university with strong defence and military links. The Head of School refers the case to the university's foreign interference team for advice.

The foreign interference team contacts the Australian academic, who reveals that they feel unable to refuse the Visiting Academic because of the involvement of a former colleague, and also because they still have family in their country of origin. They had also not realized that their research has a potential military use.

The foreign interference team explains the risks associated with accepting the Visiting Academic, and that because the university's policies do not bar research links with the foreign university, the decision rests with the Australian academic and the Head of School. The Australian academic is not sure what they should do.

Identification

s. 37(2)(b)

Link to Foreign Interference

The proposal may have been deliberately targeted by the foreign government to take advantage of Australian expertise and data in an area with defence and national security impacts. If so, it:

- took advantage of the fact that the research outcomes are dual use, and the Australian academic may not have been aware of or focused on the defence use;
- put pressure on the Australian academic by making the approach through a former senior colleague, who would be difficult to refuse;
- took advantage of the likely unwillingness of the Australian academic to refuse a formal request from their country of origin, as they still had family there;
- s. 37(2)(b)

Action

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

If the visit took place, it would have resulted in the Visiting Academic:

- building trusted relationships with academics at the Australian university, which could then be exploited later;
- having access for one year to the team's research data and facilities, possibly including work that they were not personally involved in;
- having access to the wider IT systems and physical infrastructure of the university;
- being able to share information and data they access with officials from their home country.

Discussions between the Australian academic, the Head of School, and the foreign interference team resulted in the proposed visit being rejected by s. 37(2)(b)

s. 37(2)(b)

The foreign interference team and the university's UFIT Accountable Authority reviewed the Visiting Academic and Visiting Student application forms, and inserted additional information and links to help academics and Heads of Schools identify and mitigate foreign interference risks. In person training was provided to Heads of Schools and at-risk research teams.

The foreign interference team contacted appropriate government agencies to share information about the incident.

Lessons Learnt

This incident helped the foreign interference team and Accountable Authority better understand the social pressures which can be applied to some overseas-born Australian academics, and how listening to the academic and understanding their concerns can help provide a suitable mitigation.

s. 37(2)(b)

The incident also led to discussion about how academic freedom interfaces with the university's risk appetite. s. 37(2)(b)

s. 37(2)(b)

s. 37(2)(b) The university began internal discussions about how to resolve these issues.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Foreign Military Industry Links

Summary

- An Australian University was approached by a foreign company specialising in the provision of cloud services and AI computing to establish a commercial services agreement.
- Under the terms of the commercial services agreement, the foreign company would establish an exaflop AI supercomputer at the Australian University.
- The Australian University would be responsible for brokering access between the foreign company and Australian clients, including government clients.
- Under the terms of the agreement, the foreign company would have provided its own workforce to set up the facility on campus.

Identification

- This agreement was referred to the Australian University's research security function for enhanced due diligence.

Link to Foreign Interference

- In conducting enhanced due diligence, the Australian University identified that the foreign company was established and operated by several individuals who had linkages to their respective country's military-industrial complex.

Impact

- Potential transfer of knowledge and know-how related to a sensitive research area.
- Potential access to datasets with sensitive equities into Australia's critical infrastructures.
- Possible attempt to use Australia as proxy to bypass US sanctions and export control restrictions on semiconductors.
- Potential reputational harm to the academic and University had the visit occurred.
- Potential harm to Australia's national interests and security.

Action

- The University conducted enhanced due diligence in relation to this agreement and determined that it exceeded enterprise tolerances for foreign interference risk. Accordingly, the University did not allow for this engagement to proceed.

Lessons Learnt

- This incident has advanced the University's understanding of the threat landscape.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Fraud of Visa Documentation

Summary

- A foreign PhD student sought to visit an Australian University to undertake research related to metamaterials. In correspondence with the Australian University, this student proposed to visit for a period of 24 months with their stay to be financially supported by a scholarship administered by their government.
- This student sought to be supervised by an academic at the Australian University who was the recipient of grants from both Australian and allied defence and intelligence organisations.
- In correspondence with this academic, this student demonstrated a sophisticated understanding of the Australian University's internal procedures and processes.
- Finally, this student explicitly requested the Australian University to modify an invitation letter to exclude mention of metamaterials and other keywords relating to potentially sensitive research areas so as to bypass scrutiny from an Australian Visa Officer.

Identification

- This visit was referred by the academic to the Australian University's research security function for enhanced due diligence.

Link to Foreign Interference

- s. 37(2)(b)

  s. 37(2)(b) However, this student was studying at a university with significant institutional integration with foreign defence research.
- The student's contact with an academic who was the recipient of grants from both Australian and allied defence and intelligence organisations was assessed as a potential indicator of conduct which was contrary to Australia's national security.
- s. 37(2)(b)
- The request to amend the invitation letter so as to bypass scrutiny from an Australian Visa Officer was assessed as indicative of deceptive and clandestine conduct.

Impact

- Potential transfer of knowledge and know-how related to a sensitive research area with dual-use applications.
- Potential reputational harm to the academic and University had the visit occurred.
- Potential harm to Australia's national interests and security

Action

- The University conducted enhanced due diligence in relation to this visit and determined that it exceeded enterprise tolerances for foreign interference risk. Accordingly, the University did not allow for this visit to proceed.
- Given the request to amend an invitation letter to bypass scrutiny from an Australian Visa Officer, the University reported this visit to relevant stakeholders in the Commonwealth Government.

Lessons Learnt

- This incident has advanced the University's understanding of the threat landscape.

Released by Department of Home Affairs under the Freedom of Information Act 1982

Case Study: Visiting Academic in Human Social Studies conducting Oppressive Research

Summary

A foreign academic applied to be a Visiting Academic at an Australian university. In their application, the academic proposed to continue their research into the use of social media by their country's ethnic minority groups, studying its influence on self-identity and national identity.

Their proposal detailed an intention to conduct undefined 'field work' while in Australia and collaborate on relevant research being conducted separately by the Australian university. All funding would be covered by their home country's government scholarship council while the Australian university would need only provide visa recommendation, library access and office space.

Identification

As per University procedure for foreign Visiting Academics, a summary of the proposal was referred to the University's Foreign Risk team for review whilst a formal invitation was being drafted.

Foreign Risk identified that the research involved 'sensitive topics' that were of significant domestic and international strategic interest to the funding government. These interests were noted as being potentially misaligned with University and Australian values. Initial risk indicators prompted a pause in the invitation process while further due diligence and risk assessment were conducted.

Link to Foreign Interference

Due diligence identified several risk indicators in the context of widespread allegations of significant

Human Rights abuses of ethnic minority groups by the funding government. An analysis of the proposed Visiting Academic's past publications suggested probable connections to intelligence applications and public policy.

It was noted that the visit and 'field work' were proposed in an environment widely reported of monitoring and influence by the foreign government, who maintain a priority interest in the affairs of their ethnic minority communities overseas. Allegations of transnational repression, foreign government harassment, and intimidation of Australian citizens with relevant ethnic minority heritage persist in this context.

Action

Whilst the exact nature of the research and eventual outcomes could not be assessed, it was determined that collaboration may indirectly support relevant oppressive laws, policies and practices of the foreign government. Regardless of the researchers' intent, it was anticipated that the project could have direct application in the foreign government's continued efforts to monitor and influence diaspora communities.

References to planned fieldwork and the potential for this to involve the University Community, as well as the wider Australian public, raised concerns around the potential for direct interference of ethnic minority communities.

The relevant school was presented with a risk assessment and informed that the agreement sat beyond the University's Foreign Risk Appetite, which meant approval would need to be sought from the University's Foreign Interference Accountable Authority should they wish to proceed.

The school's supervisors concluded that the proposal's value did not outweigh cumulative risks and decided not to progress the invitation.

Lessons Learnt

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

This event supports rationale for embedded processes which trigger a formal foreign risk review. Ideally, a triage system to flag basic risk indicators should be integrated to ensure manageable workloads and efficient response times.

In this event, while the researcher may not have had malicious intent, the area of research combined with the history and current affairs of the foreign government meant that this proposed activity fell outside the scope of the University's Foreign Risk Appetite. A Risk Appetite is crucial to providing rationale and scope to risk reviews, ensuring consistent, measurable, and equitable outcomes.

- Processes should be robust to ensure Foreign Risk consideration and that due diligence will be conducted.
- Processes can be built into university documentation and formalised as a procedure.
- Diverse areas of impact should be considered when making an assessment, and subject matter expertise is critical to identifying potential for misuse of research.
- Safety and security against Foreign Interference should be a whole-of-university responsibility with individual accountability.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Threats Against Students

Summary

The University encountered a situation involving foreign interference when a group of students from a particular country published a research article in the university's student journal, which criticized the political practices of their home country. Following the publication, these students began receiving messages from individuals claiming to be from their home country, pressuring them to retract the article. The messages included subtle threats regarding their families back home and hints at potential academic consequences, creating a climate of fear among the student authors.

Identification

The university identified this activity through reports from the affected students, who approached their academic advisors, supervisors and the university's complaints unit about the threatening messages they received.

Link to Foreign Interference

- The coordinated nature of the messages and the references to the students' families back home suggested involvement by individuals with ties to the foreign government.
- The behaviour was coercive and aimed at intimidating the students into retracting their critical publication.
- These actions, while not overtly severe, were contrary to Australia's values of free speech and academic freedom. Restriction of freedom of speech among the student body, as the student authors felt pressured to retract their publication.
- Mental distress among the student authors due to the fear for their families and potential academic repercussions.
- Erosion of trust within the student community and a chilling effect on future publications addressing sensitive topics.
- Potential reputational damage to the university if the interference was perceived as tolerated or unaddressed.

Action

The university took several actions to mitigate the risk and address the incident:

- The student support services were mobilized to provide counselling and guidance to the affected students, ensuring they felt safe and supported.
- The university administration issued additional training to coursework and research students, emphasising code of conduct, and support opportunities for students if they feel that they are being targeted or impacted.
- The university increased its monitoring of communications and provided workshops on digital safety and how to handle online harassment.

Lessons Learnt

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

The incident led to several changes within the university:

- The university recognized the need for better protection measures and support systems for students engaging in potentially controversial research or publications.
- There was an identified need for improved awareness among students about the risks of foreign interference and the importance of reporting such incidents.
- The university plans to implement regular training sessions on handling harassment and understanding the signs of foreign interference.
- A review of the university's policies on protecting student journalists and researchers was initiated to ensure robust safeguards are in place.
- The university established a protocol for quick response to future incidents, ensuring timely support and clear communication to the affected parties and the broader student community.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Undisclosed Employment Threatening IP

Summary

- An anonymous complaint was made to the University that alleged an academic staff member had an additional paid appointment in a foreign country, and also had a commercial company operating in that country.
- The staff member's research was in a sensitive area that had potential dual uses
- After investigation, it was established that both allegations were substantiated.
- It was not possible to ascertain if University IP had been commericalized by the staff member's company as the staff member had left the University.

Identification

- An initial anonymous complaint highlighted the first case
- Subsequent cases of secondary employment were uncovered by due diligence process

Link to Foreign Interference

- University policy was not followed, and disclosure of the staff members activities was not forthcoming
- Commercialisation of University IP may have taken place without the proper attribution and return to the Australian public.

Action

- The University put in place mandatory annual disclosures for all academic staff in relation to secondary employment, sensitive research and conflicts of interest, including commercialisation activities.
- The University conducted an investigation into secondary employment of academic staff who may have been holding additional academic appointments in foreign countries using analysis of publications
- A small number of staff left the University as a consequence of these actions.

Lessons Learnt

- Annual disclosures are the first line of defence
- Additional regular due diligence using the analysis of publications is essential in ensuring holding additional academic appointments in foreign countries does not occur.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Case Study: Undisclosed Military Employment

Summary

A foreign doctoral student researching Artificial Intelligence learning in robots expressed interest in applying for a joint PhD program with an academic at an Australian university.

The PhD proposal was viewed as a positive outcome of a recent articulation agreement between the Australian university and the student's enrolled institution, and the Australian academic communicated agreement to supervise under the program.

Identification

Prior to the articulation agreement being approved, a control had been implemented requiring all projects under the agreement undergo individual foreign risk assessment from the University's Foreign Risk office.

Despite recognition that the proposed research would involve Critical Technology and potential dual-use applications, the summary information provided to the Foreign Risk office initially indicated an acceptable level of risk when appropriate permits were secured and controls in place. However, upon requesting the applicant's CV and a full project description, due diligence discovered key discrepancies and some unusual findings.

Link to Foreign Interference

Enhanced due diligence revealed undisclosed current employment with a foreign government ministry; concurrent enrolment in a Master and PhD course in two separate disciplines at two separate institutions in two separate countries; and multiple videos showcasing the applicant's regular guest appearances on a prominent state-controlled international news channel in a recurring segment on military and strategic technologies. Topics of their interviews included cybersecurity techniques in espionage operations, military-purpose 'killer robots', the role of AI tools in assassinations, cyber warfare, and weaponizing technologies.

Action

The applicant's undisclosed employment with a foreign government ministry, as well as concurrent enrolments and further private associations, indicated a web of opaque obligations and loyalties. A lack of transparency around potential conflicts of interest reduced the confidence that associated risks could be sufficiently managed.

The applicant's demonstrated subject-matter expertise in technologies with military applications, in connection with the proposed research, raised concerns around the likelihood that research outputs could lead to foreign military end-use. Furthermore, University association with a student prominently involved in discussing military technologies with a foreign state-controlled media outlet may present reputational risks. This reputational impact, however, must be considered alongside the principle of academic freedom and general right to freedom of speech.

Foreign Risk engaged in consultations with relevant University supervisors and line managers to develop a risk assessment. Foreign Risk also progressed a provisional assessment with the Department of Defence's Office of Defence Export Controls (DEC), who advised that a permit would be required. As the DEC permit process may be subject to extended wait times, a permit application was submitted in the interim as Foreign Risk continued to follow up details with the candidate's proposed supervisors.

s. 37(2)(b)

Released by Department of Home Affairs under the *Freedom of Information Act 1982*

Lessons Learnt
This case study highlights the importance of thorough due diligence and the benefit of adopting a proactive approach to identifying foreign risks. The inclusion of a trigger for foreign risk review in the articulation agreement ensured that there was a formal process of assessment for individual projects. Furthermore, although summary information and baseline due diligence may indicate that an activity could fall within a university's foreign risk appetite, a full examination can be a valuable investment where dual-use and/or Critical Technologies are involved, to ensure comprehensive assessments and informed prescribing of appropriate controls. • Processes for review can be built into individual contracts. • Delays and requests for additional information may contribute to the withdrawal of applications. • A balanced and informed risk assessment should include engagement with all relevant stakeholders.

Released by Department of Home Affairs under the *Freedom of Information Act 1982*