Framework for the development of principles-based guidelines to counter foreign interference in the Australian university sector

The university sector plays a special role in public diplomacy, nation building and civil society. The Australian university sector is taking a thought leadership role in partnership with the Australian Government, to ensure the sector continues to be an attractive education destination while mitigating risks. The development of principles-based guidelines to counter foreign interference in the university sector will ensure a balanced and appropriate response to risk and has the capacity to be used as an exemplar model to extend to other knowledge and innovation heavy industries.

Executive Summary

The Australian university sector and the broader Australian community benefit significantly from the presence of international students and collaboration with international researchers and scholars. This level of engagement contributes to the success and achievement enjoyed by the sector, which produces advanced research, cutting-edge technology, closer partnerships with a range of countries and truly insightful scholarship – which, by extension, contributes significantly to the competitiveness of Australian companies and growth of the Australian economy.

However, this open environment of international collaboration has the potential to put the university sector at risk of exploitation by foreign actors who do not follow the same rules of academic integrity as we do, or share our values.

Foreign actors can use a range of coercive, clandestine and deceptive means to achieve their aims in the university sector. Those aims include:

- the acquisition of Australian research and technology for transfer overseas;
- suppression of ideas that they see as dissident, and promotion of narratives which support their strategic goals;
- gaining commercial advantage; and
- enabling long-term access to information.

Foreign actors can use a range of vectors to achieve their aims in the university sector. These may include:

- academic collaboration;
- economic pressure;
- solicitation and recruitment of post-doctoral researchers and academic staff;
- cyber intrusions; and
- direct foreign investment.

Fostering a positive security culture through a principles-based approach to risk management can help to ensure the university sector continues to produce world-class research while protecting academic freedom and minimising risks.

Such an approach would enhance transparency, integrity and reciprocity while maintaining productive relationships with international institutions, students, researchers and scholars.

This Framework is intended to guide the development of principles-based guidelines to counter foreign interference in the Australian university sector. The Framework consists of the following sections:

- Executive summary
- Environmental context
    - Vectors of foreign interference
    - Potential harm of foreign interference
- Scope
    - Overarching principles
    - Governance arrangements
    - Expected timeframes for delivery
    - Potential mitigation activities
    - Resources and guidance available

Understanding and responding to foreign interference in the Australian university sector requires **closer engagement between the Commonwealth and the sector**. Enhanced engagement will ensure the sector preserves its reputation for excellence while recognising and mitigating the risks of foreign interference.

Environmental Context

Foreign interference threat

Australia's Director-General of Security has noted the current scale of foreign interference activity against Australia's interests is unprecedented.[1]

Foreign interference occurs when activities are carried out by, or on behalf of a foreign actor, which are coercive, covert, deceptive or corrupting and are contrary to Australia's sovereignty, our values and national interests. Foreign interference is distinct from foreign influence, which is conducted in an open and transparent manner and is a normal aspect of international relations and diplomacy.

In some cases, foreign actors are pursuing opportunities to interfere with Australian decision-makers across a range of sectors in Australian society – including the university and research sectors.

Failure to respond to the threat of foreign interference within the university sector has the potential to damage the reputations of Australian universities; impinge upon academic freedom; and deny our academic institutions and the Australian economy the benefit of their research endeavours.

Foreign actors can use a range of coercive, clandestine and deceptive means to achieve their aims in the university sector. Those aims include:

- the acquisition of Australian research and technology for transfer overseas;
- suppression of ideas that they see as dissident, and promotion of narratives which support their strategic goals;
- gaining commercial advantage; and
- enabling long-term access to information.

Foreign actors can use a range of vectors to achieve their aims in the university sector. These may include:

- academic collaboration;
- economic pressure;
- solicitation and recruitment of post-doctoral researchers and academic staff;
- cyber intrusions; and
- direct foreign investment.

The below examples are provided to illustrate how these vectors could be used to facilitate foreign interference activities.

Potential harm

Acquisition of Australian research and technology

The collaborative work undertaken by the Australian university sector and international institutions, students, researchers and scholars, is critical in the promotion of new ideas and expertise. However, in some cases, foreign actors can engage in efforts to target Australian research and development deemed critical to their scientific, economic or military interests.

[1] ASIO, Director General's Review, https://www.asio.gov.au/AR2018-01.html

Some foreign actors seek to bypass the research and development phase of scientific endeavour by covertly obtaining research, technical information and intellectual property, particularly from universities.

Risks arise when foreign actors seek to fast track the advancement of knowledge through clandestine or coercive means. By doing so, these foreign actors can save their countries time, money and resources while achieving advances in research and development.

When foreign actors unfairly take advantage of Australia's open education and research environment, they do so at a cost to Australia.

Economic pressure

The Australian university sector encourages robust and critically minded teaching and research, where research and scholarship is conducted without fear or influence. When it works to enhance mutual interests, partnerships and co-investment increase the return to investment in research and innovation by leveraging further opportunities for technical and knowledge exchanges. This is a critical element of how Australia's research system maximises the opportunities created by research and scholarship within our universities. Foreign investment may assist universities to establish centres, support academic programs or facilitate joint research, while also fostering valuable goodwill and trust between the donor organisation and university sector institutions.

Receipt of foreign investment may also result in pressure to placate foreign governments and actors who have different values and objectives. Robust governance arrangements and other mechanisms can help protect against opportunities for these actors to engage in foreign interference activities.

There is a risk to robust and critically minded teaching and research when vested interests, supported by foreign actors, seek to use economic pressure to stifle academic autonomy, academic freedom and freedom of expression – in pursuit of their own agenda.

Solicitation and recruitment of post-doctoral researchers and academic staff

Academic solicitation is the exploitation of academics and researchers, in an attempt to obtain sensitive or classified information under false pretences. It can be effective because it is often difficult to detect deceptive approaches among a plethora of genuine requests for collaboration.

Foreign intelligence officers may obscure their true affiliations and intentions by using cover, including posing as diplomats, journalists, academics, or members of research or policy institutes/think tanks.

Foreign actors may seek to exert inappropriate interference against post graduate and/or post-doctoral researchers to gain access to intellectual property or research.

Foreign actors may be interested in Australian researchers traveling overseas who are sponsored by the Australian government; conducting research with future potentially classified applications; or seeking future Australian innovation and technology. Methods such as luggage searches, extensive questioning, and confiscation of electronic devices may be used to coerce the supply of sensitive information.

Suppression of dissident voices

International experience has shown that some foreign actors may seek to interfere with a vibrant university experience by:

- shutting down discordant voices and providing incentives to develop ones that are more favourable;
- exerting pressure on families in home countries, aimed at censoring discussion and debate; or
- appealing to students' loyalty or nationalism to elicit information.

Cyber intrusions

Australian universities constitute a core hub of research and teaching activity, which entails the holding of a range of data assets, ranging from sensitive personal information to research data, outputs and Intellectual Property.

Australian universities have seen a number of cyber intrusions into their systems in recent years. Cyber targeting can be conducted through:

- exploiting software and network vulnerabilities;
- installing malicious software through socially engineered emails (known as spear phishing) in order to get an individual to reveal sensitive information;
- hiding malware in a website or the dynamic content it displays (e.g. malvertising) with the intent of compromising the computers used to visit that website;
- establishing physical access to a system through portable media – such as USB drives, compact disks or other hardware, including gifted devices to unsuspecting recipients; or
- exploiting vulnerabilities in supply chains software and managed services in addition to hardware.

The activities identified above are foreign interference/espionage – that is, they are deceptive, coercive, clandestine or corrupting, and do not align with our national values or interests.

Scope

Principles-based guidelines to counter foreign interference (the guidelines) will support an environment of trust and confidence in a consistent manner across the sector, to guide decision-making, based on potential risks. The guidelines articulate overarching principles, to ensure they are consistent across key domains within the sector, support active collaboration, and are fit for purpose.

Overarching principles

Universities play a key role in the development of new knowledge and technological innovation that is vital to continued productivity and economic growth. University autonomy brings with it the responsibility to proactively manage and engage with risk, supported by Government and security agencies, mindful of the national interest. The guidelines are intended to empower institutions in a way that is both durable and responsive to emerging threats and pressures as these develop and change over time.

The overarching principles represent the fundamental values that guide decision-making. There is no single measure that can be taken. The overarching principles are:

- **Security must safeguard academic freedom, values and research collaboration;**
- **Research, collaboration and education activities mindful of the national interest;**
- **Security is a collective responsibility with individual accountability**;
- **Security should be proportionate to organisational risk; and**
- **The safety of our university community is paramount.**

Governance arrangements

To support the development of the guidelines, a University Foreign Interference Taskforce (the Taskforce) will be established. The Taskforce will be comprised of a Steering Group, supported by four working groups as described below. Together, the Steering Group and Working Groups will be responsible for the development and implementation of the guidelines. These guidelines should be updated periodically to reflect environmental context.

The Taskforce will be supported by the following governance arrangements:

Tier 1 Steering Group

Role and Purpose

The Steering Group is responsible for:

- Developing for Government consideration, guidelines to counter foreign interference in the university sector;
- Providing advice to Government and the university sector in relation to how to counter foreign interference in the university sector;
- Ensuring delivery of guidelines in the agreed timeframe;
- Ensuring the guidelines are consistent across domains;
- Develop a mechanism to ensure ongoing evaluation of the guidelines; and
- Providing strategic oversight of the working groups.

Membership

The Steering Group will be comprised of the following representatives from:

- Representatives from the university sector
- Universities Australia
- The Group of 8
- Department of Education
- Department of Home Affairs
- Australian Cyber Security Centre
- Attorney-General's Department
- Australian Security Intelligence Organisation
- Department of Defence

Tier 2 Working Groups

Supporting the Steering Group, **four working groups**, comprising of subject matter experts from across the Commonwealth and the university sector, will be responsible for leading the development and providing advice on the implementation of the guidelines.

Role and Purpose

The working groups are responsible for:

- The development of the guidelines;
- Ensuring the guidelines are consistent with the overarching principles;
- Ensuring guidelines are broadly applicable as possible;
- Supporting the development of advice to the sector on concrete steps and actions to be taken to counter foreign interference matters in the university sector across each of the four domains; and
- Providing advice, as required, to the Steering Group.

Membership and outcomes

The working groups will comprise selected subject matter experts across the university sector and Commonwealth agencies. Each working group will be co-chaired by a representative from the university sector and the Commonwealth. The working groups will draw on expertise from both the university sector as well as from across government, as required in the development of each of the guidelines.

- **Cyber security**
    - Objective: our digital ecosystem will be resilient to unauthorised access, manipulation, disruption or damage; and ensure the confidentiality, integrity and availability of our information through the adoption of a principles-based framework helping us to better manage and protect our networks, as well as detect and respond to cyber security incidents should they occur.
- **Research and intellectual property**
    - Objective: as a sector, we will work in partnership with government to deter and detect deception, undue influence, unauthorised disclosure or disruption to our research, intellectual property and research community, while protecting academic freedom.
- **Foreign collaboration**
    - Objective: the nature and purpose of our collaboration with foreign entities will be transparent, undertaken with full knowledge and consent, and in a manner that avoids harm to Australia's interests.
- **Culture and communication**
    - Objective: we will foster a positive security culture through engagement with government and the broader community to educate, uplift awareness and improve research and cyber resiliency.