



INTERNATIONAL RISK & ACADEMIC SECURITY

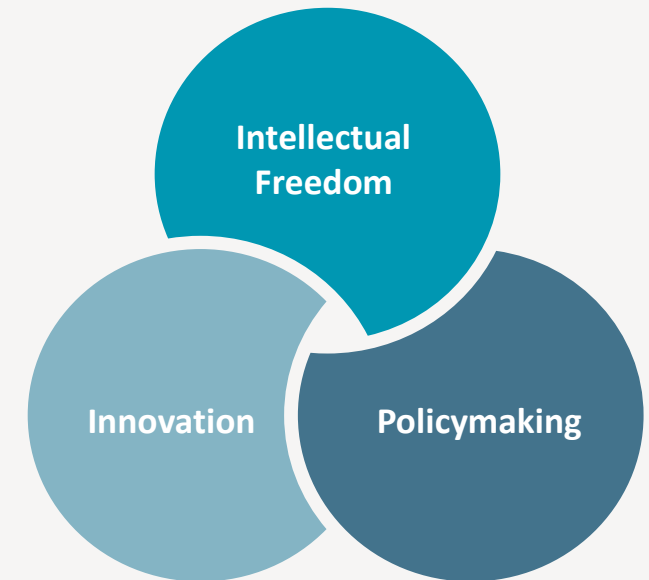


WHAT WE KNOW

- Espionage activity is higher than any point during the Cold War
- Scale, scope and sophistication is unprecedented
- Higher education remains a major target
 - **'23/24 - estimated \$628 million in IP theft**
- Foreign powers seeking access to:
 - Defence intelligence
 - Dual-use technologies
 - Cutting-edge knowledge, information, expertise
 - Personal information (contact details, biometric data, medical, financial records)
 - IT systems
 - **'23/24 - estimated \$14.5 million in cyber-security incidents**

Universities offer access to:

- Research pipelines
- Strategic thinking insights
- Government/industry relationships



Research & Higher Ed

Foreign government may attempt to:

- **Recruit** academics to steal IP
- **Influence** research for geostrategic or economic goals
- Economically **pressure** universities to sign unfavourable agreements
- **Influence** or **restrict** academic freedom, discourse, research topics, course content
- Attempt to **silence** freedom of expression on campus
- **Covertly** shape curriculum to align with their interests
- **Monitor** and **intimidate** international students



Case Study

An academic conducting research on defence-related technology attends a conference overseas with all expenses covered.

While there, the organisers target the academic for recruitment by offering more benefits.

Once back in Australia, the academic begins providing information about Australian defence capabilities to the organisers, undermining Australia's national security.

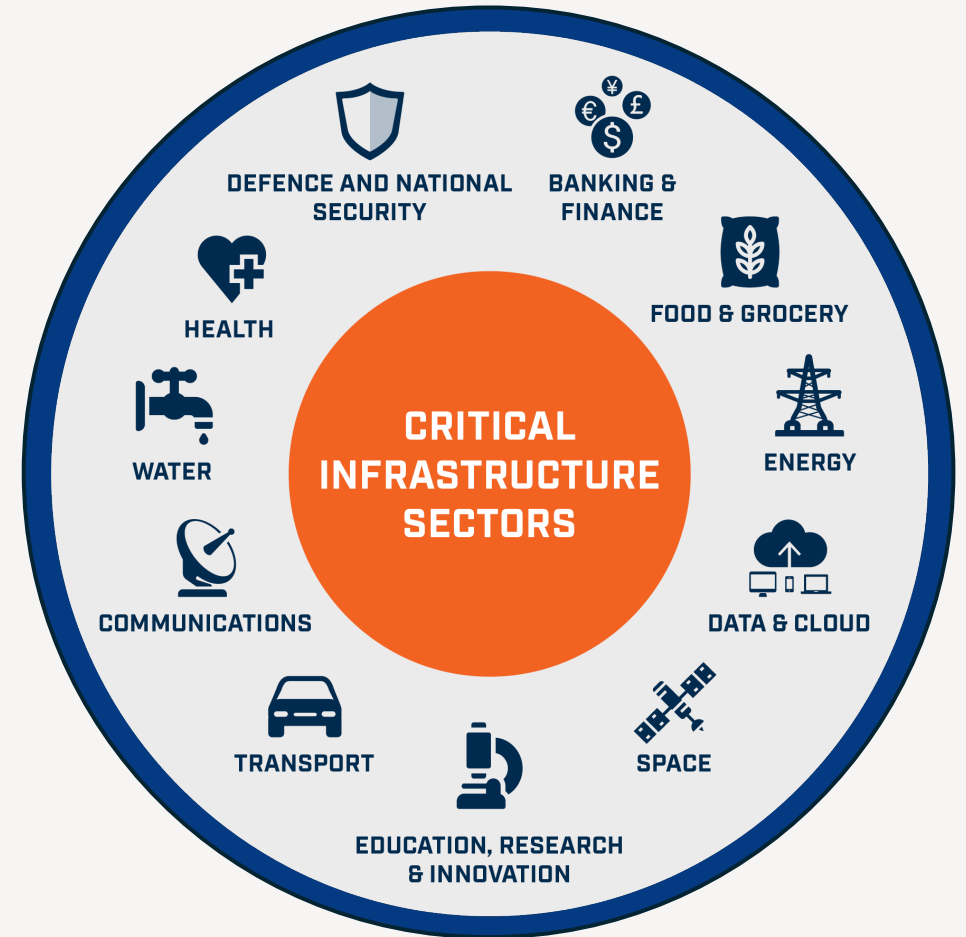
INCREASED FOREIGN INTERFERENCE RISKS

Research areas

- *Dual-use* research
- *Critical Technologies in the national interest*
- Critical infrastructure
- Human Ethics approval (inc. Social media)

Activities

- Collaboration with military aligned institutes/entities
- External funding
 - Equipment, overseas travel, gifts & benefits, government scholarships
- Restrictions on academic freedom
 - External pressure, intimidation, enticement, withhold data



What can government-linked harassment and **foreign interference** look like?

Demands

Demanding changes to subject matter, or events and activities to be cancelled.

Censorship

Preventing free speech and freedom of expression through intimidation or threats.

Harassment

Harassment, hostility, intimidation or other negative conduct either face-to-face or online. This can include threats or harassment of family and friends living abroad.

Surveillance

Monitoring or stalking staff, students or researchers

Doxing

Sharing personal details about someone without permission or consent.
This includes reporting, or threatening to report on, fellow staff or students to foreign government bodies.

Curtin can help.

Everyone at Curtin has the right to work and study in a safe space, without interference by foreign governments or their agents.

Follow our QR code to **get help**, **seek advice** or **share your story**.

Anonymous submissions accepted.



curtin.edu/foreign_interference

FOREIGN RISK CLINIC



Weekly drop-in counter for face-to-face discussions:

- Questions on referral and review processes
- Reporting incidents related to foreign interference
- Booking foreign risk awareness sessions
- Accessing information materials
- General queries related to foreign risk

HDR students are more vulnerable to foreign interference:

- Focus on establishing academic career
- Less aware of suspicious approaches
- Avoid challenging senior researchers
- Personal financial pressures
- Threats or coercion from foreign governments
- Insufficient awareness of disclosure and transparency requirements

10-2 Thursdays @ GRS (Bldg 101)

Curtin is ready to help you



Lodge a formal complaint

Students, staff and researchers can **submit a report** about a concern or incident. This is the best option for making your complaint formal and seeking further action.

Anonymous submissions are accepted.



Discuss your concerns

Talk directly to our team about your concerns. This is the best option for receiving confidential and personalised support, assistance or guidance.



Share your story

Privately and securely **share your experience**. Your story can shine a light on this issue and build our understanding of how to help the Curtin community.

Anonymous submissions are accepted.

curtin.edu/foreign_interference

Travel ICT

► Curtin ICT not authorised to be taken to specific jurisdictions

► Why?

- Broad, opaque National Security laws
- Expansive data protection laws
- Increase in arbitrary detention
- Cyber attacks

► How will this protect me/Curtin?

- Aligns with government/industry policy
- Avoids violating laws overseas
- Protects individual & Curtin's data/systems

Jurisdictions

- Afghanistan
- Belarus
- China
 - Hong Kong
 - Macau
- Iran
- Iraq
- Lebanon
- Libya
- Mali
- Myanmar
- North Korea
- Russia
- Saudi Arabia
- Somalia
- South Sudan
- Sudan
- Syria
- Ukraine
- Venezuela
- Yemen
- Zimbabwe



STAY UP TO DATE



Foreign Risk Clinic

Weekly drop-in counter for all foreign risk related questions
Thursdays @ GRS (Bldg. 101, Level 1)



iPerform

Foreign Interference Awareness Training (~20 mins)
Sanctions Training (~25 mins)



Sign up for our bimonthly e-newsletter

Declassified case studies, news updates and analysis,
due diligence reports, resources for academic use

Email foreign.risk@curtin.edu.au to be added

Or sign up here →



CASE STUDY

A PhD student at an Australian university is undertaking a research project in the field of **geospatial data science**. Their research involves developing mapping data and modelling techniques that can be applied to **critical infrastructure** – such as ports, energy networks or telecommunications networks. The topic of their research is **sensitive** and has a **dual-use** application.

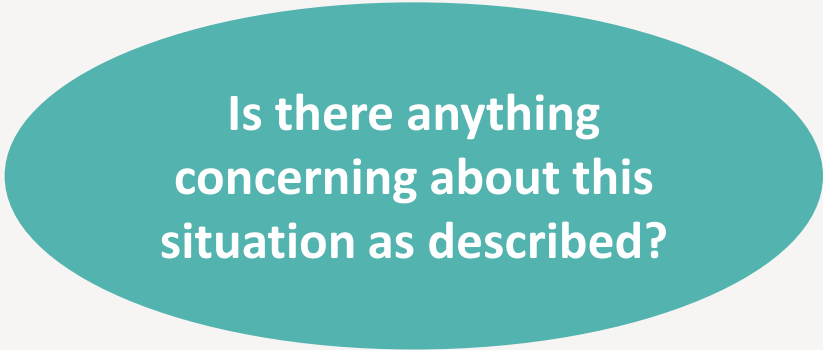
Why might this research be considered sensitive or dual-use?

What value might this research have to a foreign government or state-linked actor?

CASE STUDY

The PhD student is supervised by a senior academic at the Australian university.

They also work closely with researchers at an **overseas university** and have a friendly working relationship with a **researcher** who works on a different project with no sensitive dual-use application.



Is there anything concerning about this situation as described?

CASE STUDY

The researcher begins persistently asking about the PhD student's findings, requesting to **read** project materials and offering to **collaborate** on parts of the project.

When asked why they're interested in this unrelated area, the researcher is **reluctant** to explain. **Flattered** by the interest from a senior colleague, and mindful of the career benefits, the PhD student says they *may* be interested in future collaboration.

The researcher keeps pushing for the findings to be shared and offers **financial rewards** – including expenses-paid research trips.

At what point did this situation shift from “*normal collaboration*” to “*cause for concern*”?

What should the student do?