



FOREIGN INTERFERENCE

HDR INDUCTION 2025



Foreign influence vs interference

Foreign Influence

- Activities directed by a foreign principle, conducted in an **open and transparent** manner

Foreign Interference

- Activities directed by a foreign principle which are **coercive, clandestine, deceptive or corrupting**, and are contrary to Australia's sovereignty, values and national interests



‘More Australians are being targeted for espionage and foreign interference than at any time in Australia’s history – more hostile foreign intelligence services, more spies, more targeting... From where I sit, it feels like hand-to-hand combat.’

Michael P. Burgess, ASIO Director-General (21 February 2023)

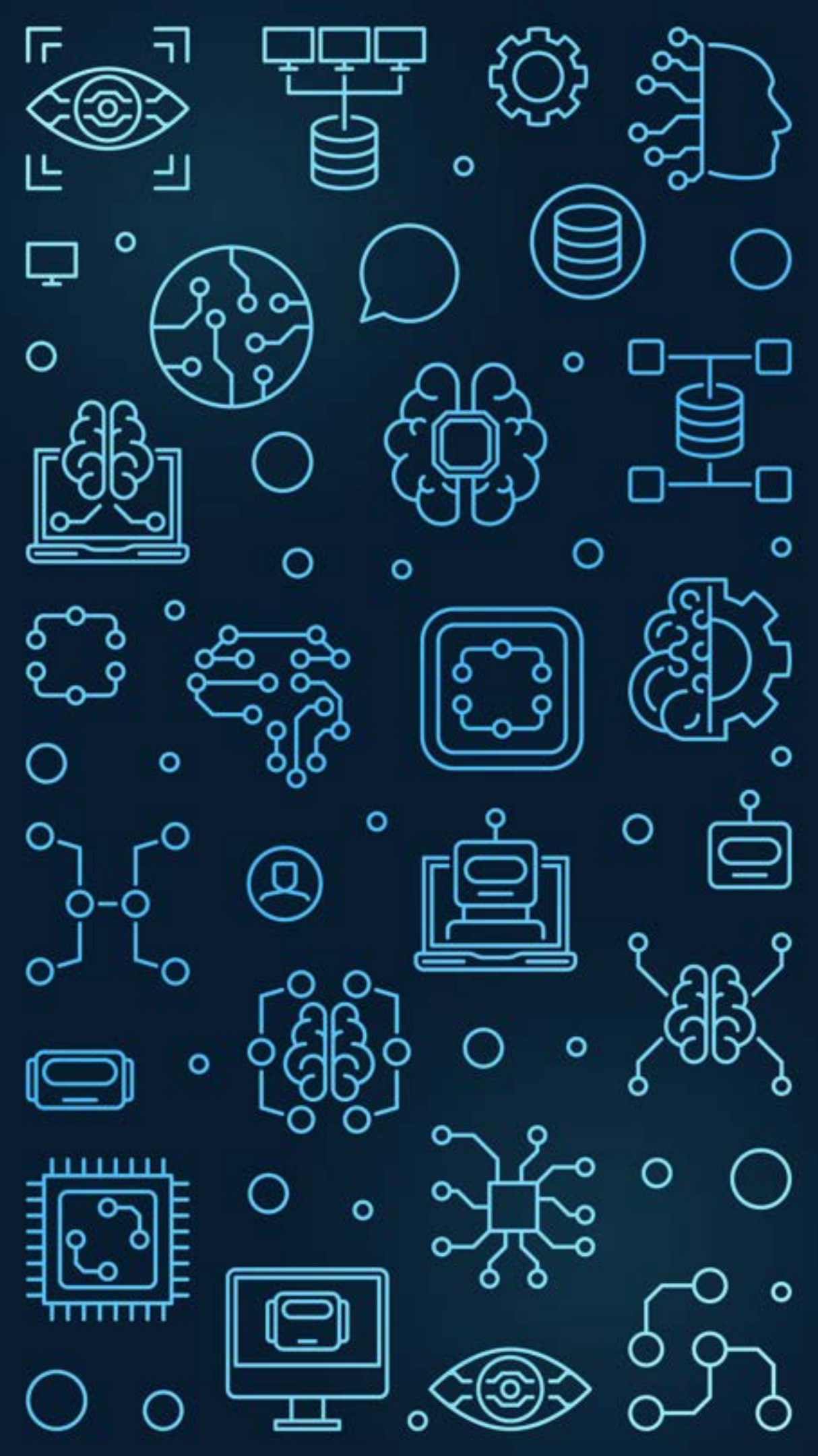
Unwanted Knowledge Transfers

It is in Curtin & Australia's interest to prevent **unwanted knowledge transfers**.

These can occur via:

- Leveraging individuals with links to a foreign jurisdictions
- Poor personal security measures
- Social engineering
- Digital espionage and cyber attacks
- Collaborations with academic or industry partners

If you suspect you are being targeted for unwanted knowledge transfer, reach out to foreign.risk@curtin.edu.au



CRITICAL TECHNOLOGIES



Impact Australia’s national interest via:

- 💰 Economic prosperity
- 🛡️ National security
- 👥 Social cohesion

Represent technologies for which Australia:

- 🧪 Has research, intellectual or industrial strengths, and capabilities to be supported and championed
- 🔗 Needs uninterrupted access through trusted supply chains
- 📅 Must retain strategic capability or maintain awareness

POTENTIALRISKS

- 🛡️ Increased risk of cyber attacks
- 🔗 IP theft
- 📖 Unwanted knowledge transfer
- 🔗 Compromised critical functions, systems or supply chains
- 🏢 Monopolisation reducing transparency and collaboration
- 🏛️ Undermining of Australia’s sovereign decision making

Advanced information and communications technologies	Advanced information and communications technologies	
	Advanced data analytics	Advanced optical communications
Advanced materials and manufacturing	High performance computing	Protective cyber security technologies
	Advanced materials and manufacturing	
AI technologies	Additive manufacturing (incl. 3D printing)	Critical minerals extraction and processing
	Artificial Intelligence (AI) technologies	
Autonomous systems, robotics, positioning, timing and sensing	Machine learning, (incl. neural networks and deep learning)	Natural language processing, including speech and text recognition, analysis and generation
	Autonomous systems, robotics, positioning, timing and sensing	
Biotechnologies	Aerospace technologies (incl. propulsion, hypersonics and guidance systems)	Drones, swarming and collaborative robots
	Biotechnologies	
Clean energy generation and storage technologies	Synthetic biology (Incl. biological manufacturing)	Neural engineering and brain–computer interfaces
	Genome and genetic sequencing and analysis	Vaccines and medical countermeasures
Quantum technologies	Clean energy generation and storage technologies	
	Emissions reduction technologies	Advanced energy storage
	Quantum technologies	
	Quantum computing	Post-quantum cryptography

DEFENCE EXPORT CONTROLS (DSGL)



The **Defence and Strategic Goods List (DSGL)** is a comprehensive inventory that designates **goods**, **software** or technology that is regulated when **exported**, **supplied**, **brokered** or **published**.

The DSGL is divided into two parts:

Part 1: Defence and related goods - goods and technologies for use by armed forces or are inherently lethal.

Part 2: Dual-use goods - equipment and technologies developed to meet commercial needs but which may be used in the development or production of military systems.

HOW TO READ THE DSGL

Part 2 Categories

Category 0 - Nuclear Materials;
Category 1 - Materials, Chemicals, Microorganisms and Toxins;
Category 2 - Materials Processing;
Category 3 - Electronics;
Category 4 - Computers;
Category 5 - Telecommunications and Information Security;
Category 6 - Sensors and Lasers;
Category 7 - Navigation and Avionics;
Category 8 - Marine;
Category 9 - Aerospace and Propulsion;

Permit Required For:

Category A - Systems, Equipment, Components
Category B - Inspection, Production Equipment
Category C - Materials
Category D - Software
Category E - Technology related to items

Identifying Technology on the DSGL

E.g. **3A**233 - Mass Spectrometers

Category A - Systems, Equipment, Components

Category 3 - Electronics

∴ **Permit required if exporting a mass spectrometer**

Processing of permits generally take **up to 15 days**. More complex applications may take **35 days or longer**. *Processing time is based on **government assessments**. Staff are encouraged to be prepared **well in advance** to account for potential governmental delays.*

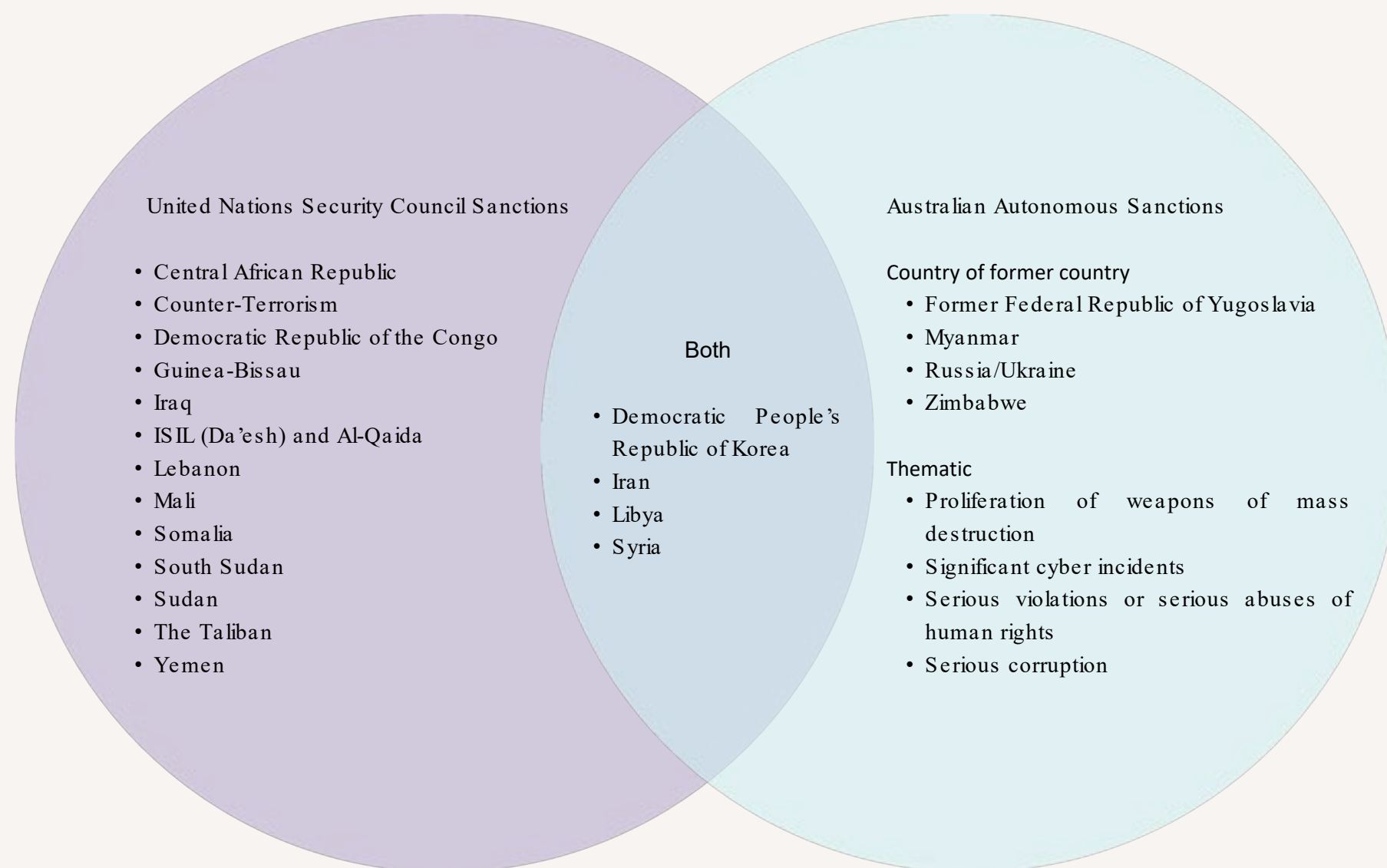
If you require assistance, please contact foreign.arrangements@curtin.edu.au



Curtin University

Further Considerations

Sanctions



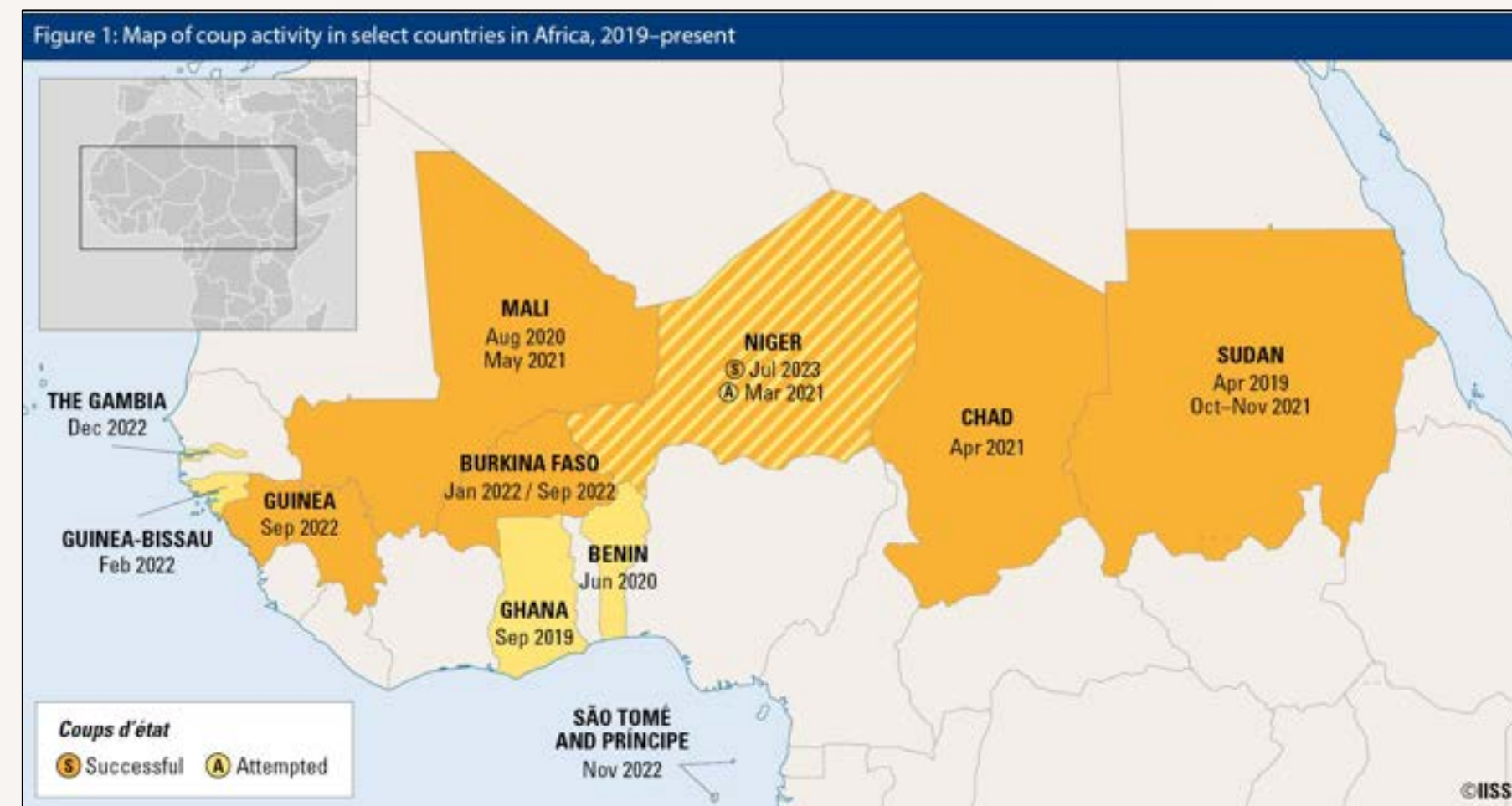
Valuable IP/Patents

- Commercial viability
- Potential patent applications



Geopolitical Risk

- Disputed territories/regions
- Repressed minority groups
- Human Rights abuse claims
- Adverse media potential



Check out the Foreign Risk page for more information on 'Sensitive Topics'

Due Diligence Checklist for International Collaboration

Completing this checklist when beginning an international collaboration helps identify potential key risk indicators. Informing the Foreign Risk Management Team early in the project lifecycle allows them to provide initial guidance, highlight unforeseen risks, and ensure a safer and more efficient process as the collaboration progresses.

Identifying foreign interference risks does not prohibit the activity from taking place; however, it may require Curtin to implement specific project-level controls to mitigate these risks. A proactive approach to countering foreign interference helps improve efficiency, protects staff and students, safeguards Curtin’s reputation and ensures Curtin continues to benefit from international collaboration.

If you have identified potential foreign risks on the sheet below and would like further guidance, please contact foreign.risk@curtin.edu.au

What	No	?	Yes
Select No, Unsure (?), or Yes for each question			
Does my research relate to an area of critical technology (listed here)?			
Does my research involve dual-use technologies (potential military application)? These may be regulated under the Defence Strategic Goods List 2024 here ?			
Does my research relate to sensitive topics or geopolitically sensitive regions here ?			
Could my research be readily applied to a military, intelligence, policing or security application (including through misuse)?			
Could my research be of significant commercial, strategic or economic interest?			

With Whom	No	?	Yes
Select No, Unsure (?), or Yes for each question			
Do any of my partners or their host countries lack openness or transparency?			
Am I significantly more advanced than any of my partners in this area or research?			
Do any of my partners have significant links to an Australian or UN sanctioned country here , a sanctioned individual here , or a 'specified international jurisdiction' here ?			
Did due diligence into relevant collaborators identify any issues or concerns?			
Have any relevant partners, including you, not yet disclosed your foreign relationships and interests here ?			

Please list any additional relevant information below (Research topic, collaborating institution, etc.)

If you have selected :yes: from options under both “What” and “With Whom” categories above OR would like further guidance, please contact: foreign.risk@curtin.edu.au

- **Informal research** risk assessment
- Identify risks early
- Awareness of future controls
- Ensure transparency
- Downloadable & fillable copy [available here](#)

Suspicious Approaches

- Foreign powers and their proxies may pose as **journalists, academics, industry figures** etc.
- Approaches may be **indistinguishable** from networking or collaboration opportunities

Signs of a potential suspicious approach:

- **Repeated** encounters or coincidences
- **Unusual, unsolicited, or persistent** attempts to discuss research papers, unpublished data
- Offers of **excessive** gifts and hospitality
- **Sudden** and **uncharacteristic** friendliness
- **Persistent** requests to move communication to less secure platforms
- **Unusual** questions about your work or institution
- **Foreign delegations** wanting to enter sensitive facilities
- Requests to **collaborate** with foreign institutions associated with **sensitive technology** or are **politically sensitive**

Remember, report anything



Suspicious
Ongoing
Unusual
Persistent

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



Arranging Travel ICT

- ▶ Submit travel through TOP
 - ▶ FRMT notified, contact traveller to confirm dates
 - ▶ FRMT organise travel device with DTS
 - ▶ DTS informs traveller when device ready
 - ▶ FRMT will reach out to organise pre-travel briefing

Returning

- ▶ Return device to DTS ASAP
- ▶ Avoid using device in Australia
 - ▶ Procedure applies to personal travel/OWA, based on available stock

staffportal.curtin.edu.au/governance/foreign-risk/travel/curtin-travel-ict/

More information →



As a Curtin team member, your awareness and understanding of Foreign Interference (FI) is key to:

- Identifying risks;
- Protect our brand and reputation;
- manage sensitive and secure activities appropriately;
- Enhance our security culture

Curtin's fraud and corruption framework is linked to Curtin's value of integrity – to act ethically, honestly and with fairness; act with due care and make informed decisions.

Contact us: foreign.risk@curtin.edu.au

QUESTIONS?



Professor Melinda Fitzgerald
FI Accountable Authority
lindy.fitzgerald@curtin.edu.au



Mr Paul Riley
Director of Foreign Risk
paul.riley@curtin.edu.au



Curtin University