Curtin University

FOREIGN INTERFERENCE

HDR INDUCTION 2024

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*)

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

POTENTIAL RISKS

- 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 data analytics	Advanced optical communications
High performance computing	Protective cyber security technologies

Advanced materials and manufacturing	
Additive manufacturing (incl. 3D printing)	Critical minerals extraction and processing

Artificial Intelligence (AI) technologies	
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	
Aerospace technologies (incl. propulsion, hypersonics and guidance systems)	Drones, swarming and collaborative robots

Biotechnologies	
Synthetic biology (Incl. biological manufacturing)	Neural engineering and brain–computer interfaces
Genome and genetic sequencing and analysis	Vaccines and medical countermeasures

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. 3 A 233 - Mass Spectrometers

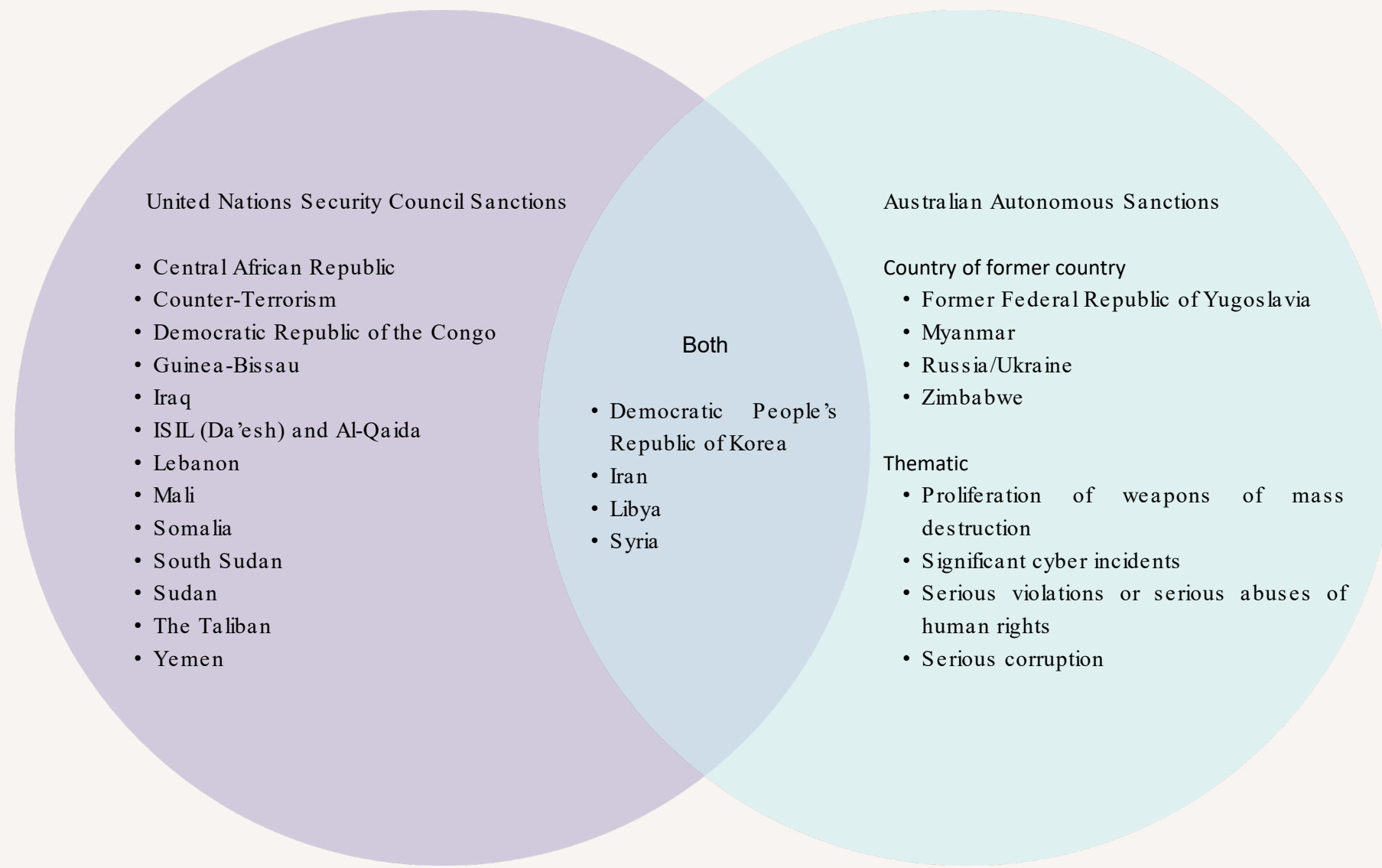Category A - Systems, Equipment, Components

Category 3 - Electronics

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

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

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

Curtin University

Further Considerations

Sanctions

United Nations Security Council Sanctions

- Central African Republic
- Counter-Terrorism
- Democratic Republic of the Congo
- Guinea-Bissau
- Iraq
- ISIL (Da'esh) and Al-Qaida
- Lebanon
- Mali
- Somalia
- South Sudan
- Sudan
- The Taliban
- Yemen

Both

- Democratic People's Republic of Korea
- Iran
- Libya
- Syria

Australian Autonomous Sanctions

Country of former country
- Former Federal Republic of Yugoslavia
- Myanmar
- Russia/Ukraine
- Zimbabwe

Thematic
- Proliferation of weapons of mass destruction
- Significant cyber incidents
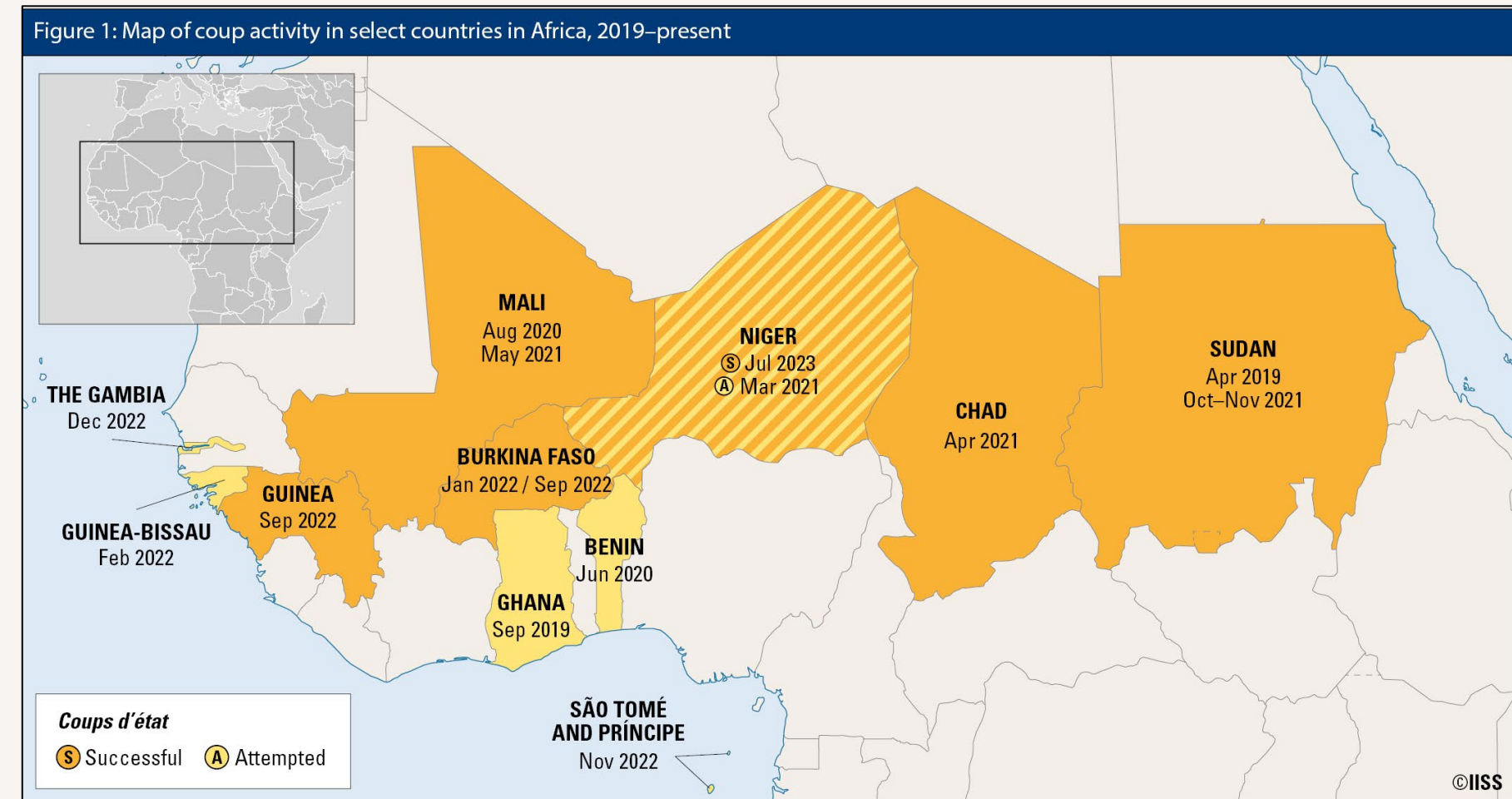- Serious violations or serious abuses of human rights
- Serious corruption

Geopolitical Risk

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

Figure 1: Map of coup activity in select countries in Africa, 2019–present

MALI
Aug 2020
May 2021

NIGER
Ⓢ Jul 2023
Ⓐ Mar 2021

SUDAN
Apr 2019
Oct–Nov 2021

THE GAMBIA
Dec 2022

CHAD
Apr 2021

BURKINA FASO
Jan 2022 / Sep 2022

GUINEA
Sep 2022

GUINEA-BISSAU
Feb 2022

BENIN
Jun 2020

GHANA
Sep 2019

Coups d'état
Ⓢ Successful   Ⓐ Attempted

SÃO TOMÉ
AND PRÍNCIPE
Nov 2022

©IISS

Valuable IP/Patents

- Commercial viability
- Potential patent applications

INTELLECTUAL PROPERTY
PATENTED
INTELLECTUAL PROPERTY

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

International Collaboration

Consider the following questions to determine whether a proposed collaboration is a higher risk of being targeting by foreign actors.

Does the activity involve **research, development** or **commercialisation** of a technology that could be relevant to Australia's national interest or security?

- *e.g. Critical Technology, DSGL, cutting-edge/unique technology*

Does the activity involve any other **sensitive information** or **data**, such as:

- personally identifiable information?
- health or genetic data?
- confidential commercial or financial information?

What **access** could the activity/project give to a partner, third party or individuals?

- Could it be used to gain access to your IT networks or IP?

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 potentially suspicious approaches:

- **Unsolicited requests** for your expert opinion

- Requests to **collaborate** with foreign institutions associated with **critical technology** or are **politically sensitive**

- Receiving **financial donations** from **foreign-linked entities**

- **Unusual, unsolicited,** or **persistent attempts** to access research papers, unpublished data

- Invitations to **international conferences** with excessive offers of gifts and hospitality

- **Persistent** requests to move communication to **less secure platforms**

- **Foreign delegations** wanting to enter sensitive facilities

Predatory Journals

Some journals charge academics to publish their research without ethical or editorial standards. They regularly misrepresent their publishing practices.

Indicators

- Legitimate journals charge a small amount, or no fee at all
- **Deception** used to gain submissions - e.g. false promises of peer review, lacking transparency around charges
- Prey on **junior faculty** under pressure from universities to publish
- Undertake **aggressive marketing**, mostly via email
- Articles **rarely read or cited**, sometimes never published, despite payment
- Unusually **large breadth of topics** - nonpredatory publishers more focused
- Often have generic names - e.g. *"Academic Sciences"* or *"BioMed Press"*
- Some scholars have been listed without their permission

Consequences

- Little exposure for academic work
- Weaken public confidence in the validity of research
- Poor research could mislead others, produce untrue findings

Online Presence

- Research profile demonstrates your value

  o Can raise interest to foreign intelligence

- Social media can make you a target (vector)

  o **Think before you link**

- Increase **privacy** settings

- Consider removing:

  o Comments/posts online referencing access to

  sensitive research, locations or contacts

  o Specifics of **industry collaboration** projects

Arranging Travel ICT

➤ Submit travel request through TOP

➤ Additional travel declaration has been added:

➤ Once approved, traveller(s) will be contacted by the Foreign Risk Management Team (FRMT)

➤ DTS will deliver Travel ICT to traveller

➤ If a pre-travel briefing required, FRMT will reach out to traveller to organise

Last Minute Travel

➤ Contact foreign.arrangements@curtin.edu.au as soon as possible to ensure sufficient time for their provision of designated Curtin Travel ICT.

Upon Return

➤ Return Travel ICT to DTS as soon as possible after returning

➤ If required, attend post-travel debrief with FRMT

Non-Official Curtin Travel

➤ Staff travelling to a specific international jurisdiction organised outside of TOP (e.g. personal travel, OWA) are not authorised to take standard issue Curtin ICT

➤ Staff may be eligible to borrow Travel ICT where a sufficient business need is identified.

More Information

➤ Staff Portal

➤ Foreign Risk

➤ Curtin Travel ICT

Curtin University

Disclosure of relationships and interests (DORI)

- **Complete if you have Staff Portal access**

- Curtin's Conflict of Interest (COI) procedures have been revised and renamed

- New category of disclosure: '**Foreign Relationships and Interests**' (FITS and UFIT compliance)

- Disclosures **do not** indicate a concern or necessarily mean that a relationship or activity must stop

- Many arrangements contribute positively to Curtin, and should continue to be promoted transparently

DORI will help protect staff and Curtin by:

- Demonstrating **transparency**

- Enabling centralised **assessment** for potential risks and registration requirements

- **Informing** tailored training, advice, support and mitigation

- Support staff should problems arise – **paper trail essential!**

IF IN DOUBT, DISCLOSE

Disclosure Details

Disclosure Type

Declaration of Relationship or Interest

For disclosures relating to Foreign Relationships and Interests, please select this category below.

For all other disclosures, please refer to the guidelines Appendix 2 for determining if a Conflict of Interest exists prior to completing this form.

Category *

Close personal relationships between individuals
Close personal relationships between individuals and students
Financial interests
Foreign relationships and interests
Multiple Roles / Conflicts of Duty
Personal beliefs
Personal views of individuals towards others
Public comment
Research
Secondary employment
Sponsorships and other agreements
Use of University facilities and equipment
Use of official information

Choose file   No file chosen

Tackling Foreign Interference

- **Transparency** and **awareness** are key mitigators to foreign interference

- Recognise the **value of the information and access you hold** – and your expertise

- **Protecting Curtin's reputation** is essential in securing future industry collaboration

- **Fulsome disclosure** of relationships and interests is expected

- If you feel **coerced, intimidated** or **pressured** contrary to yours or Curtin's interests **let us know**

- **S.O.U.P** – Report anything **Suspicious, Ongoing, Unusual, Persistent**

- The Foreign Risk Management Team can offer support, advice and guidance to staff in a safe and secure manner.

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