COUNTERING FOREIGN INTERFERENCE IN YOUR ORGANISATION

There has been much media coverage regarding the threat of foreign meddling in international democratic processes and, most recently, in attempts to undermine elections. Most strikingly, the report released by US Special Counsel Robert Mueller in March 2019 detailed how Russian intelligence agencies conducted ‘sweeping and systematic’ interference in the 2016 US Presidential election.\(^1\) But what of the risk of foreign interference that may exist within our organisations?

Foreign interference, as distinct from legitimate and transparent forms of foreign influence, involves activities that are covert, deceptive, corrupting or coercive\(^2\) that are intended to advance the interests or objectives of foreign actors.

Clearly, multinational corporations and other institutions are not immune from being used by authoritarian regimes to manipulate democratic political processes.\(^3\) The Mueller Report, for example, documents dozens of examples of Russian intelligence agencies using major corporations, non-governmental organisations and other organisations as vehicles for interfering in the US Presidential elections.\(^4\) In November 2018, the Australian Security Intelligence Organisation (ASIO) reportedly ordered the cancellation of the Australian resident visa of a prominent Chinese citizen businessman on the grounds that he was amenable to conducting foreign interference.\(^5\)

However, there may be less awareness of how foreign interference is being used to distort commercial decision-making, obtain intellectual property and undermine corporate profitability. ASIO has recently warned that foreign states are engaging in espionage and interference to gain commercial advantage over Australian businesses, obtain access to our innovations in science and technology and shape the actions of Australian decision-makers and public opinion.\(^6\)

Authoritarian states are engaging in increasingly invasive efforts to shape and exploit the international environment through political interference and espionage. Countering foreign interference has become a top-tier national security concern across developed world countries, with particular focus on Russia, the People’s Republic of China and other authoritarian states.\(^7\)

In Australia, Federal Government officials from ASIO and the Departments of Foreign Affairs and Trade, Defence and Home Affairs have been delivering foreign interference briefings to major corporations and universities. Official concerns are focused on the theft of intellectual property, the theft and manipulation of personal data and the manipulation of decision-making.

Foreign actors may seek to obtain confidential or sensitive information about your organisation’s strategies, technology, research and development, intellectual property, mergers and acquisitions’ activity or trade negotiations. They may exert influence on employees to develop strategies or make decisions that advance their interests or objectives. They may also operate ‘front organisations’ that are intended to influence public debate, business decisions and governments to support foreign policies or undermine government policies.

The mechanisms of foreign interference include:
- Arbitrary detentions of personnel abroad\(^8\)
- Harassment and obstruction of personnel and commercial partners\(^9\)
- Manipulation of trusted insiders\(^10\)
- Cyber attacks\(^11\)
- Espionage\(^12\)
- Expropriation and manipulation of commercial information\(^13\)
- Expropriation of personal data and information\(^14\)
- Coerced political advocacy\(^15\)
- Propaganda attack campaigns and orchestrated consumer boycotts
- Economic coercion\(^16\)

How Foreign Interference can affect your organisation

Analysing the impact of foreign actors on Australian public and private organisations may be defined with reference to commercial, reputational, financial and legal risks.
- Direct commercial risks can manifest as forced intellectual property transfer, coercive partnership arrangements and export embargoes. Commercial risks can also stem from the unravelling of supply chains or Australian Government-instituted security audits regarding research funding, procurement contracts and other forms of international collaboration.
- Reputational risks may flow from parliamentary inquiries or investigations by the media, ASIO, think tanks, cyber consultants or US enforcement agencies.
- Legal risks can flow from class actions and other claims relating to directors’ duties as well as direct compliance risks under the new legal regime.

What are your compliance obligations under the legislation?

In June 2018, the Australian Parliament passed some of the toughest and most targeted counter-interference laws in the Western world. The National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 introduced a new crime of ‘foreign interference’ as well as a series of tiered provisions for espionage, sabotage, secrecy and treason. These offences are targeted at foreign intelligence agencies and those who knowingly collaborate. Those who engage in foreign interference aimed at influencing elections or supporting foreign intelligence face up to 20 years’ jail.

A separate law, which is targeted at indirect influence, creates a new transparency regime that builds upon the US Foreign Agents Registration Act. This Foreign Influence Transparency Scheme (FITS), enabled under the Foreign Influence Transparency Scheme Act 2018, came into full force in March 2019. Under the FITS, businesses who have a ‘registrable arrangement’ (including a contract, agreement, understanding or other arrangement of any kind, whether written or
unwritten) with a ‘foreign principal’ who undertakes certain activities for the purpose of political or governmental influence are required to register, unless an exemption applies.\textsuperscript{17} Failing to register is a crime.

As at 1 August, 40 individuals and organisations have voluntarily added themselves to the public Transparency Register.'\textsuperscript{18} For example, former Cabinet Minister Brendan Nelson AO has registered that he is a board member of French subsidiary Thales Australia (since 17 March 2015). His record discloses his role, which is namely to advise management on issues facing them. The record also states ‘The Republic of France holds approximately 25% of the issues shares of Thales SA; which is listed on the Paris Stock Exchange.'\textsuperscript{19}

Similarly, energy companies such as Chevron Australia Pty Ltd, Shell Australia Pty Ltd, South32 Limited and Woodside Petroleum Limited have also registered. As operators or managers of joint ventures (JV), these entities act on behalf of all JV partners including foreign principals (either because they are state-owned entities or are partly owned by governments or government-related entities).

Categories of registrable activities include:

- parliamentary lobbying on behalf of a foreign government;
- parliamentary lobbying on behalf of other kinds of foreign principals for the purpose of political or governmental influence;
- general political lobbying for the purpose of political or governmental influence;
- communications activities for the purpose of political or governmental influence;
- disbursement activities for the purpose of political or governmental influence;
- activities undertaken by former Cabinet ministers on behalf of a foreign principal; and
- activities undertaken by recent designated position holders in the 15-year period immediately following their public role where those activities draw on the knowledge, skills or experience gained in their previous role.'\textsuperscript{20}

Most organisations have registered their engagement in one or a number of activities including general political lobbying activities, parliamentary lobbying activities and communications activities, on behalf of the JV participants.

These JV arrangements are obviously known to these companies and are in the public domain. However, what if your organisation is unaware of an agent of influence who is acting on behalf of a foreign principal? How would your organisation discern and respond appropriately to try and resist foreign interference?

Proactively managing Foreign Interference risks in your organisation

Understanding, managing and mitigating foreign interference risks as identified and targeted in the Australian Government’s counter-interference legislation and strategy is critical.'\textsuperscript{21} These risks can be substantially mitigated via a comprehensive and specialised programme of transparency, accountability, vetting, counterparty due diligence and risk awareness.

A carefully designed foreign interference risk review should be framed by clear positive principles that reflect and reinforce the organisation’s values, such as transparency and accountability. It should be informed by strategic due diligence ‘core samples’ in agreed priority areas.

Leading Australian and international financial institutions, investment banks, non-profit organisations and universities have commenced these reviews for the purposes of understanding and building resilience for:

- client relationships;
- supply chains;
- funding partners;
- intermediaries; and
- key personnel.

The due diligence performed should inform decisions on whether and how to engage counterparties, research partners and key personnel. More broadly, the foreign interference risk review should help to inform, adjust and extend the organisation’s existing risk management systems.

The objective is to mitigate legal, reputational, financial and commercial risks by applying standards of good governance without confronting staff, clients or partners. In turn, this will strengthen your organisation’s status as a trusted partner, improve commercial sustainability and build resilience within your organisation.

How to advise your board and senior leadership on mitigation strategies

Questions for the board:

- What is our foreign interference resilience strategy?
- Do we know who we are engaging with?
- Is our organisation compliant with the new legislation?

SUGGESTED CHECKLIST

1. Know your networks
   - Review your:
     - JV arrangements / partnerships;
     - client and supplier lists;
     - portfolio companies; and
     - investment targets.
   - Review key personnel (external and internal).
   - Educate your staff.
   - Ensure internal transparency, proper process and oversight.

2. Assess vulnerabilities
   - Perform enhanced due diligence for high risk entities
   - Conduct network mapping of intermediaries, counterparties and key individuals regarding political linkages and patronage networks.

3. Design tools and policy frameworks to proactively manage foreign interference risk
   - Increase awareness of the threat and implement effective mitigation strategies.
As a Senior Consultant, McGrathNicol Advisory John is one of Australia’s pre-eminent international strategy experts, specialising in advising Australian government and private sector clients on geopolitical risk and International Counter-Party Due Diligence.

A Partner at McGrathNicol Advisory, Matt is a highly regarded forensic expert with more than 25 years’ experience specialising in financial crime, corporate corruption and regulatory investigations, dispute advisory, enforceable undertakings and risk advisory.

Footnotes
3. Foreign Influence Transparency Scheme: Factsheet 2, Australian Government Attorney-General’s Department (February 2019)
19. The FITS applies to foreign government related entities including those where they:
   - control 15% shares or votes;
   - can appoint 20% board directors;
   - have directors accustomed to acting in accordance with their wishes; or
   - are able to exercise, in any other way, substantial control.