Headquarters
New Zealand Defence Force
Defence House
Private Bag 39997
Wellington Mail Centre
Lower Hutt 5045
New Zealand

OIA-2023-4739

16th June 2023

[redacted]
[redacted]gmail.com

Dear [redacted]

I refer to your email of 29 May 2023 requesting 'a list of all documents, briefings or events over the last three years relating to building resilience against hybrid interference targeting members of the New Zealand Defence Force'. Your request has been considered in accordance with the Official Information Act 1982 (OIA).

The New Zealand Defence Force (NZDF) has units throughout the organisation that are tasked to identify, respond, mitigate and reduce the risks and harm caused by the targeting of NZDF personnel. For example, the Defence Counter Intelligence unit works with other internal and external agencies to ensure processes are in place to build resilience against targeting measures.

In the last three years, the Defence Counter Intelligence unit has identified a range of threat vectors used when targeting NZDF Personnel. Work is undertaken across the organisation to ensure mitigation measures are put in place. At Enclosure 1 is a high-level threat summary for the first quarter of 2023. Enclosure 2 provides guidance on foreign interference for NZDF personnel and staff. Where indicated, an internal point of contact is withheld in accordance with section 9(2)(k) of the OIA to prevent this information being used for malicious or inappropriate purposes such as phishing, scams or unsolicited advertising.

Further information is withheld in full in accordance with section 6(a) of the OIA as the release of such information is likely to prejudice the security or defence of New Zealand.

You have the right, under section 28(3) of the OIA, to ask an Ombudsman to review this response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that responses to official information requests are proactively released where possible. This response to your request will be published shortly on the NZDF website, with your personal information removed.

Yours sincerely

**AJ WOODS**
Air Commodore
Chief of Staff HQNZDF

**Enclosures:**
1. Defence Counter Intelligence quarterly summary
2. Foreign Interference and Defence Industry

TE OPE KĀTUA O AOTEAROA
DEFENCE FORCE

DEFENCE
SECURITY

# DEFENCE COUNTER-INTELLIGENCE
## QUARTERLY SUMMARY – MARCH 2023

### Espionage

(U) The Espionage threat level as **HIGH**: *security threat activity will highly likely occur, which could cause harm to the NZDF mission.*

### Terrorism

(U) The NZDF Terrorism threat level has changed to **LOW**: *terrorist attack is assessed as a realistic possibility.* This is a revision from medium; *terrorist attack is assessed as feasible and could well occur.*

### Insider threat

(U) The new level for insider threat is **HIGH**: *security threat activity is occurring/will highly likely occur, which could cause major harm to the NZDF mission.* This is a revision from low.


### Subversion

(U) The Subversion threat level as **LOW**: *security threat activity is realistically possible, which could cause harm to the NZDF mission.*

### Organised Crime

(U) The new threat level for Organised Crime is **MEDIUM**: *security threat activity is occurring/will likely occur, which could cause harm to the NZDF mission.*

### Sabotage

(U) The Sabotage threat level as **VERY LOW**: *security threat activity is unlikely, however opportunistic targeting may occur and cause harm to the NZDF mission.*

**For more information see the DEFCI Quarterly.**
**For any comments, feedback, or specific requests please email Defence Counter-Intelligence:** s.9(2)(k)



DEFCI-23/09
*Information cut-off date:* 14 March 2023

# FOREIGN INTERFERENCE AND DEFENCE INDUSTRY

The world has become more complicated, complex and fragmented. Internationally, authoritarianism is on the rise. Adversarial and coercive actions are being used much more in the management of state affairs. Foreign interference is an example of this kind of activity. While all states engage in efforts to influence foreign partners, such activity becomes interference when it is **purposely misleading, deceptive, covert or secretively.** We are seeing an increasing willingness by foreign states to act against or within New Zealand in ways that undermine our sovereignty and security. Likeminded countries around the world are experiencing the same problem.

| ESPIONAGE | SUBVERSION | SABOTAGE |
|---|---|---|
| Foreign intelligence services (FIS) directed attempts to acquire sensitive or protectively marked information or to cultivate relationships with a view to generating access. | Subversion is the infiltration of people, information or ideas with the aim of influencing attitudes (including loyalty and allegiances), plans or outcomes. | Sabotage is the deliberate destruction or disruption of a target in order to cause degradation in capability for strategic advantage or to impose a cost against a target state or firm. |

## DUE DILIGENCE

Due diligence is a systematic assessment of the risks associated with any business, research, or investment decision with a new partner or collaborator. Due diligence also applies throughout the lifecycle of an existing business relationship, partnership, or investment. In today's world of complex global relationships, we need to take care when doing due diligence. This care ensures that we encourage and keep harmless and innocent relationships. These relationships include economic, cultural, research, scientific, diplomatic, and political relationships.

You may also need to determine how far down the supply chain your due diligence efforts should go. An organisation's third party may itself use a third party to perform their contract, and so push risks further down the supply chain. You should consider the potential business and compliance risks in third-party supply chains when deciding whether to extend due diligence efforts to the suppliers of suppliers.

## WHAT DOES FOREIGN INTELLIGENCE TARGETING LOOK LIKE?

Foreign spies are proactive, creative and well resourced. They are also opportunistic and are looking for small lapses in security practices-such as lax visitor-escorting policies or poor security controls in offices-that allow them to gain access to restricted areas. They might take photographs, or look through papers that have been left out.

Foreign spies are persistent and will often show an unusual level of interest in your work, and ask detailed questions about it-including what type of projects you are working on, and who else is working on them. They are looking to co-opt or coerce defence industry employees-or their contacts-to help them steal information. They are looking for individuals who work in sensitive areas-individuals who might be willing to work for them, or those who might be susceptible to being pressured to work for them.

**WHAT could make you susceptible to approaches by foreign spies?**

- Being stressed about personal or financial matters.
- Getting into situations where sensitive material could be easily compromised.

## MITIGATIONS

*Be aware of the information you share online.*

- Limit and regularly audit what personal and professional information is available about you online.
- Review your social media and other online security settings to limit who can access your information.

*Protect yourself – In New Zealand and overseas.*

- Where possible, do not take personal electronic devices overseas. Instead, consider taking a separate device with limited information on it that you format when you return.
- Do not discuss sensitive or classified information in non-secure areas.
- Do not leave electronic devices or sensitive documents unattended-including in hotel safes.

*Report suspicious approaches to your relevant security manager.*

**For Security Managers**

*Promote a security culture.*

- Show that you value good security practices-help staff to identify security breaches, and encourage them to report any security concerns they may have.
- Regularly review your employees in terms of their suitability to hold a security clearance-identify any sudden changes in their personal circumstances and/or behaviour.
- Ensure that your security clearance holders adhere to their obligations under the PSR.

*Promote IT security.*

- Conduct regular security training and refreshers for staff-emphasise their IT security responsibilities.
- Regularly update software and apply patches to company IT devices.
- Immediately report any unusual activity occurring on company IT devices.

To help you recognise the approaches you should report, remember the acronym **'SOUP'** and these examples:-

**Suspicious** You receive a social media request from a foreign national you've never met or heard of before, and they have an extensive list of foreign contacts, none of whom you know.

**Ongoing** You meet someone in an official capacity and they contact you afterwards to continue the association, either officially or unofficially.

**Unusual** You receive an unsolicited email from a professor in another country asking you to host a visiting scholar while they work with you for a period of time.

**Persistent** You attend a weekly social gathering where someone repeatedly asks detailed questions about your work duties.

**What can I do if I experience a suspicious approach?**

- Report the details to your Facilities Security Officer.
- Security Clearance holders – complete a contact report form.