Espionage and Foreign Interference Threats

Security advice for members of the New Zealand Parliament and Locally Elected Representatives

PSR | Protective Security Requirements

New Zealand Government

What you need to know

As a member of the New Zealand Parliament or a locally elected representative, you and people who work for you are of interest to foreign states.

Espionage and foreign interference are serious threats

Not every foreign state actor who seeks to engage with you will have benign intentions. Espionage and foreign interference could be their aim. If a foreign state actor targets you, following the advice in this booklet will help protect you and your staff from being compromised. Acting on this advice will also make it more difficult for criminals to target you and your staff.

Foreign state actors work under many guises

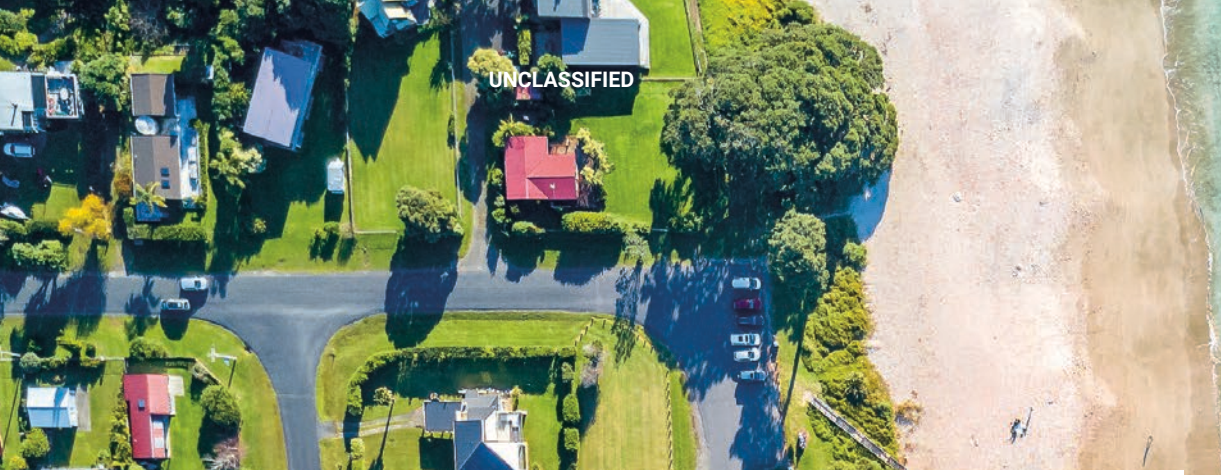
While foreign intelligence services usually lead and carry out espionage and foreign interference, they may also use a range of other actors to help them. These other actors include:

- diplomats
- academics
- military personnel
- media organisations
- community organisations
- business people
- online actors
- proxies.

You must consider the variety of ways you could be approached by foreign state actors to fully understand the nature of the threats you may be exposed to.

The sources of the threats change over time

The foreign states conducting espionage or interference against New Zealand change over time. That's why the advice in this booklet is not directed at any particular countries.



Why do foreign states target New Zealand?

Several countries undertake activities that are against us and our interests — at home and abroad. Foreign state actors operating in New Zealand may be interested in the following activities.

Influencing our democracy

They may try to covertly influence New Zealand government policies, democratic institutions, and processes.

Interfering in our foreign affairs

They may seek to affect New Zealand's foreign relations, and/or stifle our voice and media commentary on international issues and developments.

Gaining an economic advantage

They may attempt to gain a commercial advantage and damage the economic interests of New Zealand or its businesses.

Understanding our military capability and activity

They may monitor New Zealand's military capabilities and deployments and may use the information they obtain to inform future planning.

Seeking our technological and intellectual property

They may covertly obtain valuable insights into New Zealand's technological and intellectual property. They may then use those insights to inform economic and military research and development in their countries.

Spying on critics or former citizens

They may want to gather information on members of a diaspora community based in New Zealand, especially critics of the foreign state.

Why might foreign states be interested in you?

Foreign states know that as an elected representative, you're in a position of influence and have access to a wide range of sensitive information. Foreign state actors will be interested in using you to get access to that information or increase their influence.

Ability to steer policy making

They'll be interested in your ability to steer policy making, especially when it may relate to their country.

Access to people in positions of power

They may be interested in you in your own right, or may look to exploit your access to others in positions of power.

Knowledge of internal opinions

They'll see your inside knowledge as extremely valuable. Knowledge such as points of tension, split opinions, or off-the-record views held by fellow politicians or personal contacts.

Access to sensitive information

They may also be interested in obtaining sensitive information about you or those around you, so they can use it to coerce or discredit you if they believe you may be damaging their objectives.

What's the harm?

If, through targeting you, a foreign state actor manages to exert influence over New Zealand's Parliament or other elected bodies, this influence could not only damage New Zealand's democratic process and government, but also your reputation.

Other real-world impacts could include:

- undermining New Zealand's commercial edge over international competitors
- compromising negotiating positions
- damaging our national security.

UNCLASSIFIED

How might foreign state actors approach you?

Most people who approach you and your staff will have entirely legitimate reasons for doing so. However, in rare cases, you and your staff may be approached either directly by foreign intelligence officers or via 'agents' – intermediaries working knowingly or unknowingly to the direction and instruction of a foreign intelligence agency.

It's unlikely to be obvious (at least initially) that you have been approached by a foreign state actor. Intelligence officers are unlikely to declare themselves and are adept at operating undercover. For example, they may pose as journalists, academics, lobbyists, or diplomats. They're resilient, persistent, and patient. They use conferences, networking and social events to make and build contacts. They may also target your staff, family, colleagues, or constituents to collect information about you or gain access to you.

Be careful about the activities you get involved with

Be aware that intelligence officers may try to find or engineer opportunities to gain undue influence and leverage over you. Engaging in inappropriate activities, even if they are not illegal in New Zealand, could leave you vulnerable to coercion.

Be aware of organisations that foreign state actors may use

While the vast majority of organisations you interact with will be genuine, some grassroots, independent organisations who say they represent local communities may not be what they seem. Some of these organisations or people leading them may in fact be directed by foreign intelligence services, other arms of foreign governments, or foreign diplomatic staff in New Zealand. Offers of support from these organisations may be orchestrated to serve the interests of a foreign state.

How to deter approaches

Follow this advice to help protect yourself and your staff.

Be vigilant

Consider whether individuals who have initiated contact with you are showing an unusual or sustained level of interest in you, your work, or your colleagues. Ask yourself whether their interest feels unusual given your normal work or portfolio interests.

Check their identity and connections to foreign governments

Research any unknown individuals online and check whether the organisation they represent exists. Search for information about the organisation and whether it has connections to foreign governments. Check their social media profile is consistent with their stated role and the nature of their contact with you, and whether they have any unusual foreign links.

Take a trusted colleague with you when meeting someone new

Intelligence officers can sometimes be deterred by the presence of a third party at a planned meeting, so take someone you trust with you when meeting someone new. This tactic will also make it harder for you to be compromised.

Withdraw from the conversation

If you think you've been approached by someone who could be covertly working for a foreign state, withdraw from the conversation, politely refuse to engage, and report it to your security team.

Conduct due diligence on any offer you receive

Be vigilant when you receive offers of donations, gifts, or favours.

If an approach relates to accepting an honorary or advisory role, engaging in collaborations, or involves a financial or business venture, make sure you comply with transparency rules. For example, comply with the Register of Pecuniary and Other Specified Interests of Members of Parliament, the Conflicts of Interest register, and so on.

Consider the background and source of any proposed investment or donation

Before you accept any offers or donations, establish whether there are any links with foreign states. Independent financial advisers can provide advice on anti-money laundering risks and wider compliance and regulatory issues.

Report any suspicions you have to your security team immediately.

How to communicate more securely

Be mindful of the vulnerabilities associated with all forms of electronic communications; no mobile phone, tablet, telephone, or IT system is totally secure. Consider any system with an internet connection as vulnerable to the most capable attackers.

Foreign state actors have a range of sophisticated capabilities they can use to access your communications. Bear in mind that they may also target the communications of your staff, family, or friends.

The following pages provide sensible precautions you can take to enable you to work more securely — either at home, at work, or on the move.

Only use official IT devices

Official IT devices provided by government organisations are more secure than your personal devices because they run in a trusted operating environment, and are specifically configured and secured. For all official business purposes, only use official IT devices.

Keep your software secure

Ensure that all security settings on your personal devices and accounts are enabled, and keep software up to date and patched. Do not install any software on your official device unless it is approved by your organisation.

Make sure any software you install on your personal device is from a legitimate source. Fake apps are a common source of attack, especially on mobile devices.

UNCLASSIFIED

Keep passwords safe

Never give your full login or password details to anyone or any service that requests them.

Use different passwords for different accounts to prevent widespread compromise by a single attack. You can use a reputable password manager to make remembering your passwords easier.

Take care to protect your primary email account to which password reset emails are sent.

Use multi-factor authentication

Get your organisation to set up multi-factor authentication on your accounts whenever possible as it will give extra protection if your password is compromised.

Protect phone calls

Consider all conversations (and voicemails) over an open phone line as unprotected. Remember to change all default PINs on phone services such as voicemail, to ensure that no one can dial in and retrieve your messages.

Make family and staff aware of the risks

Educate your staff and family on the risks with devices and encourage them to adopt the same precautions as you.

UNCLASSIFIED

Be careful when working remotely

Modern IT provides the flexibility to work how and where it suits you, but you must pay attention to the environment you work in. Take care that your IT — or any hardcopy containing sensitive information — cannot be overseen, or your conversations overheard. Remember that foreign state actors might use sophisticated capabilities to follow, watch, and listen to you.

Do not connect your IT devices to free Wi-Fi offered in public places, such as hotels, airports, and coffee shops. There are multiple ways sophisticated actors can exploit these networks.

Ensure that your software (especially your web browser) is up to date and patched.

Prevent 'spear phishing' attacks

Because no IT security can guarantee total protection against sophisticated threats, you should be aware of how to identify attempts to compromise your IT. Many cyber attacks rely on tricking the user into doing something to enable the attack, such as encouraging you to visit a malicious website or open an attached file containing malicious code.

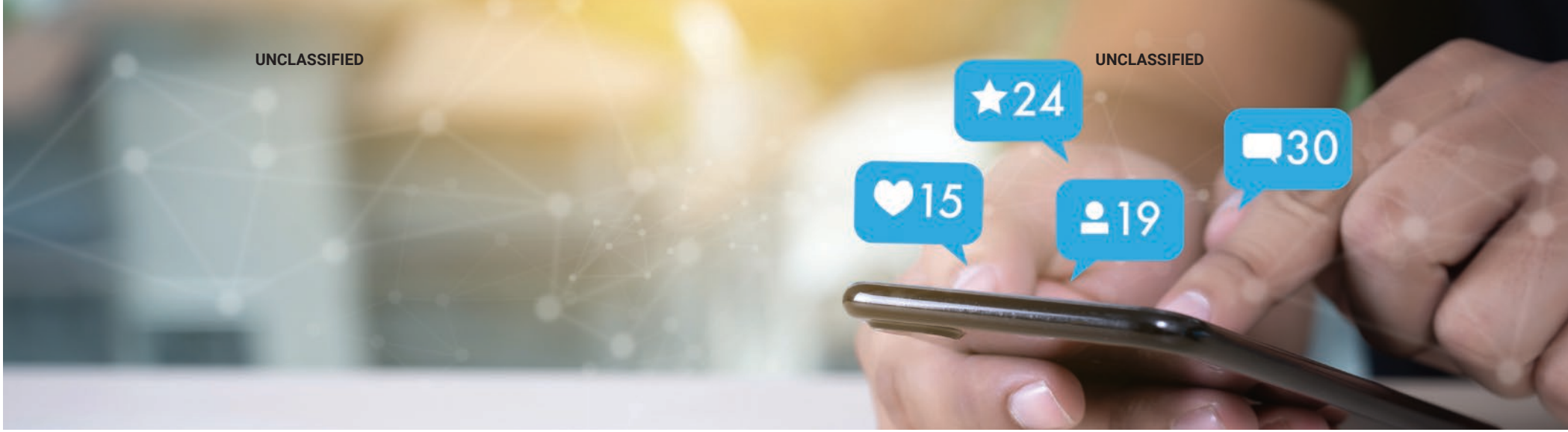
Attackers may craft emails tailored to appeal to your interests or make emails appear to be sent from a trusted source (a technique known as spear phishing). If you are suspicious of an email or attachment, don't click on any links or open the attachment. Delete the email and report it to your security team.

Where to find more advice

National Cyber Security Centre – www.ncsc.govt.nz/newsroom/working-remotely-advice-for-organisations-and-staff

Protective Security Requirements – www.protectivesecurity.govt.nz/information-security/managing-specific-scenarios/mobile-and-remote-working/

UNCLASSIFIED



How to protect your online profile

Having an online profile is an essential and unavoidable aspect of your public role. But foreign state actors and criminals may use the information you display in your profile to help shape approaches or to find opportunities to exert influence.

Foreign state actors and criminals have a range of sophisticated tools to identify, research, and exploit information online. Assume that all online information about you, your work, your family, and associates is visible and accessible to them.

Be aware too that some social networking applications employ sophisticated censorship. Your comments may be censored or appear in a manner that you did not intend.

Think carefully about what you share

Always think carefully about what you share online, and consider advising family and friends not to share private or personal information about you or your work.

Research your digital footprint

Research your digital footprint (the trail of data you leave behind when accessing the internet) to know what information about you exists online. Your footprint can be actively created by you, your family, colleagues, constituents, or the media (for example, when blogging or posting on social media). But data about you can also be created passively and without you necessarily being aware of it, such as a web server logging your computer's IP address when you visit a website.

If you can, separate the social media you use for your business from those you use for personal or social reasons.

Regularly review your passwords and privacy settings

Many publicised 'compromises' of social media accounts involve an authentication breach (the attacker logs into the service as you). Many social media services, including Twitter and Facebook, offer enhanced security options such as multi-factor authentication. Regularly review your passwords and privacy settings on devices, apps, and social media sites.

Where to find more advice

www.protectivesecurity.govt.nz/resources-centre/case-studies/making-personal-information-public-through-social-media/

How to protect yourself when travelling overseas

Espionage and foreign interference threats are likely to be higher when you travel overseas either for personal or business trips, as it is easier for foreign state actors to operate outside of New Zealand. Consult your security team before you travel overseas to receive appropriate security advice or briefings.

For guidance on protecting yourself and New Zealand's interests, refer to 'Security Advice for New Zealand Government officials travelling overseas on business'. It's available from: www.protectivesecurity.govt.nz

You can also research your travel destination on the Ministry of Foreign Affairs and Trade's Safe Travel website: www.safetravel.govt.nz. You'll find general advice on the safety and security situation in any countries you're planning to visit.

Taking care with electronic devices

Only take the minimum technology you need; phone and internet networks in overseas countries can easily be accessed.

Do not conduct sensitive business over the phone, via text, or via messaging apps due to the potential for these messages to be intercepted.

Consider using a 'pool' phone and/or laptop which:

- contains only the information you require while overseas
- can be wiped when you return to New Zealand.

If you need to use email, set up a new email account for the trip with a password you do not use for your other accounts.

UNCLASSIFIED

UNCLASSIFIED 21

Avoiding connections to public Wi-Fi, chargers, and USB sockets

Do not connect to public Wi-Fi unless it's unavoidable. In that case, activate a Virtual Private Network (VPN) service. Your IT department can provide advice on a VPN service.

Do not use public charging points or plug your device into USB sockets in planes, hotels, conference venues, airports, or devices that are not yours.

Protecting personal items and information at hotels

Limit the amount of personal information you provide to hotels and other organisations.

Don't leave passports, documents that contain personal or sensitive information, or any electronic devices unattended in hotel rooms. Be aware that hotel safes can be opened easily and don't provide much security.

Consider what you throw away in the hotel bin. If the hotel reception wants to hold your passport, give them a photocopy instead.

If you're separated from your device for any length of time while travelling (for example, at an airport) you should consider it compromised.

Being vigilant when you return

Foreign state actors may use information obtained about you during your overseas trip to make contact with you when you return. This contact may be made remotely (for example, via a spear phishing attack) or you may be subject to a face-to-face approach.

Remain vigilant about emails that may contain malicious links or attachments.

Be alert to any suspicious activity relating to your electronic devices. This includes your device acting unusually (such as running hot or its battery draining quickly).

Be wary of unknown LinkedIn requests, or suspicious activity on social media and messaging platforms.

Immediately report any suspicious activity to your security team.

Useful websites and contacts

Websites

Protective Security Requirements
www.protectivesecurity.govt.nz

National Cyber Security Centre
www.ncsc.govt.nz

Ministry of Foreign Affairs and Trade www.safetravel.govt.nz

Contacts

Your own security team

Protective Security Requirements
psr@protectivesecurity.govt.nz

National Cyber Security Centre
info@ncsc.govt.nz

For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

VERSION 1 / JUNE 2020

New Zealand Government