

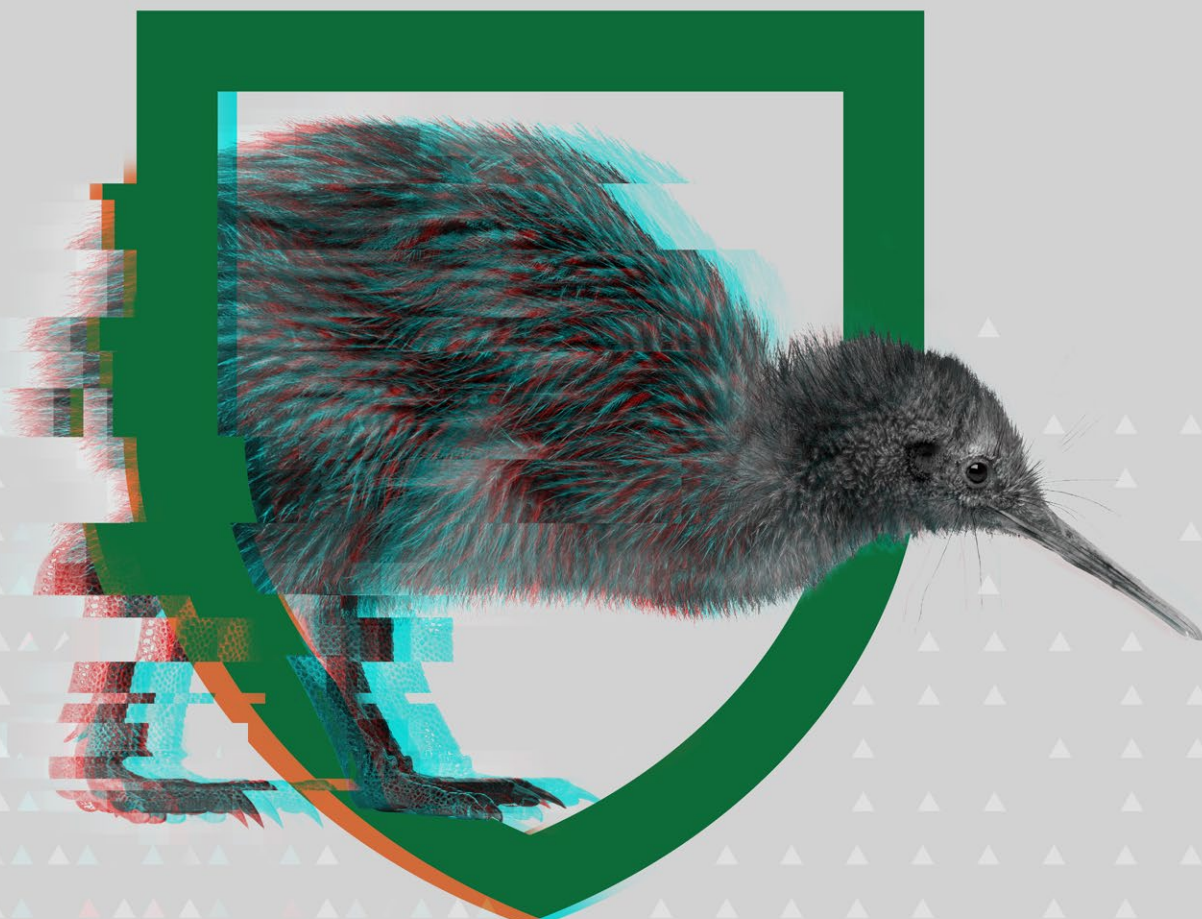
New Zealand's Security Threat Environment

2026

An assessment by the New Zealand
Security Intelligence Service



Te Pā Whakamarumarū
New Zealand Security
Intelligence Service



Contents

01. Foreword	4
Key assessments.....	5
02. Security challenges facing New Zealand	6
03. New Zealand's espionage environment	10
Chasing non-public information.....	11
Targeting New Zealand's Private Sector	12
Targeting academic research	12
Use of front companies	13
Targeting operators of Ground Based Space Infrastructure	13
Espionage activities in the wider Pacific	15
Recruiting New Zealanders with inside access	16
04. Insider Threat	17
Deliberate insiders	17
Influenced insiders	18
Unwitting insiders.....	18
Common factors in New Zealand insider threat cases.....	19
05. New Zealand's foreign interference environment	21
Political interference in New Zealand	21
Societal interference in New Zealand	22
06. New Zealand's violent extremism environment	26
Likely violent extremism scenario in New Zealand	27
Radicalisation in New Zealand	28
Violent online communities.....	28
Violent extremism in the mainstream	29
Emerging trend	30
Preventing and countering violent extremism in New Zealand	31
07. Resources	32
Commonly used terms.....	32
Methodology	34
National security careers.....	35
How to report a national security concern.....	37

Foreword by Andrew Hampton, Director-General of Security

New Zealand's national security challenges have intensified over the past year.

Our last report described the threat environment as being the most challenging of recent times. The kinds of malign behaviours and activities we have seen over the past 12 months are proving even more threatening for a country like New Zealand given its size and location in the South Pacific.

All countries are being buffeted by shifting geopolitical forces, polarised societies, ongoing economic pressures and rapid advances in artificial intelligence. This report describes the flow-on effects for New Zealand's national security. It is a complex and volatile picture.

In some respects, New Zealand will experience the current turbulence in different ways to other small countries. We are highly interconnected with the rest of the world, we produce leading innovations, we hold some important security partnerships, we are part of the strategically important Pacific region and we are located close to Antarctica with Christchurch being a key gateway. These factors in combination make New Zealand not only geopolitically relevant, but also attractive to threat actors.

As a result, NZSIS is seeing significant demand across government, the private sector and civil society for advice on how to navigate the current geopolitical turbulence and how to respond to the associated threats. Security risks can be managed in a way that builds resilience, defends New Zealand's interests and keeps us safe and secure.

Global events are not the sole source of New Zealand's security challenges – some of our concerns are homegrown. Extremist voices from within our shores are contributing to a polarised information environment, and we see some of these voices advocating for the use of violence. Young and vulnerable people in New Zealand are particularly susceptible to violent extremist narratives, which are more readily accessible online and now exacerbated by artificial intelligence.

Both Antisemitism and Islamophobia are among the concerning themes we see running through the violent extremist environment in New Zealand alongside other hateful narratives. Such harmful rhetoric should be called out early to stop it from festering and crossing the threshold to violence.

There are also New Zealanders, some deliberately and others unwittingly, acting in the interests of foreign states. This could be by handing over non-public information or influential New Zealanders self-censoring to stay onside with a foreign state. Such behaviour harms our democracy and our economy.

This year's report shares as much information as we can while protecting the information that must remain secret so the NZSIS can be effective. Our case studies are real and indicative of some of the threats we see but only represent a small proportion of the harmful activity we see through classified intelligence.

The aim of this report is to help New Zealanders to better understand the security threats we face and the risks that need to be managed. There is information here of particular relevance to communities, businesses, local and central government, universities and researchers, but many of the topics discussed have wider consequences for society and are deserving of your attention.

Finally, we are always on the lookout for curious and creative people who are keen to join our mission to keep New Zealand safe and secure. If reading this assessment sparks an interest, check out our careers page towards the end of this assessment.



Andrew Hampton
August 2026

Key assessments

The NZSIS makes six key assessments about New Zealand's threat environment in 2026:

1. Geopolitical upheaval is bringing downstream threats to New Zealand's safety and security.
2. New Zealand's public and private sectors are being targeted by foreign states and their proxies to gain access to critical assets including intellectual property, innovative technology and other non-public information.
3. Diaspora community groups in New Zealand are being unfairly targeted by foreign states and their proxies seeking to limit the democratic rights and freedoms they enjoy in New Zealand.
4. More insiders are causing harm to their organisations and our national security through actions that are either deliberate, influenced by outsiders or unwitting.
5. Another terrorist attack in New Zealand is assessed as Possible. The most likely attack scenario would involve a lone actor targeting people in a crowded place using weapons that are easily accessible. Their mobilisation to violence will likely happen with little to no intelligence forewarning.
6. Violent extremism in New Zealand is being influenced by a broad range of ideologies, a mix of domestic and international events, and the mainstreaming of extremist online rhetoric.

Security challenges facing New Zealand

This report identifies five security challenges facing New Zealand that are creating risks needing to be managed.

Addressing these challenges will require a stronger security mindset across New Zealand society.

Malign actors are seeking to take advantage of the deteriorating global threat environment in ways that are often counter to our national interests.

How New Zealand responds to these challenges will be crucial. Deeper thinking is needed about how we can all work together to best protect our people, our information, our assets and our values. A good starting point is to understand the threats we face and match those with the measures needed to help build our resilience.



Geopolitical uncertainty

As a small, geographically isolated country that depends on international trade and connectivity for our prosperity, the world is becoming increasingly challenging for New Zealand to navigate.

New Zealand's relationships and our innovation, our location in the South Pacific, and our close proximity to Antarctica all make our country geopolitically relevant. This has been positive for our international reputation and our economic prosperity, but that relevance is bringing downstream threats to our national security.

We have previously benefited from a generally stable global geopolitical outlook, in which our key interests could be pursued and maintained through diplomacy, structured cooperation, and engagement in multilateral forums. But many of the assumptions we have relied on in pursuing our interests are now being challenged. Norms and rules of importance

to us are being undermined. Overall, geopolitics is now more unstable and unpredictable. In this deteriorating global environment, New Zealanders need to consider how to maintain the national interest, protect what matters and continue to prosper.



Our 2025 report made a similar assessment of the global environment, and the downward trajectory will almost certainly continue for the immediate future.

Global upheaval brings with it acute national security threats for New Zealand, brought about by the downstream effects of aggressive competition between states for control over technology, resources, supply chains and increasingly regional influence.

States' pursuit of strategic advantage is affecting New Zealand's interests. Non-public information is increasingly sought, including policy insights, intellectual property or data sets. States are unsentimental in their pursuit of this information. They may seek to dupe a government insider with a lucrative job offer or try to bust through a cyber backdoor. Homegrown technological innovation, particularly that which has potential military uses like our rapidly expanding space sector, is also under threat from state-sponsored espionage.

Foreign interference activity ramps up during these periods of upheaval. Authoritarian states seek to keep diaspora populations abroad under tight control so they can maintain their official narrative and lower the

risk of perceived dissent. State proxies use deception and at times corruption to build long-term influence with decision makers.

States will also seek to exploit the already highly polarised online world to stoke social instability and further their global interests.

New Zealand can't opt out or completely shield itself from these global trends – our prosperity and way of life depends on being connected with the rest of the world. Instead, we all have a role in managing the risks and minimising the negative impacts.

A highly contested region

New Zealand's domestic security depends in no small part on the stability and security of our wider Pacific region.

New Zealand is fortunate the Pacific is generally a peaceful region. There is the potential, however, for our relatively small economies and government systems to become overwhelmed by the growing number of security challenges we collectively face.

All Pacific Island countries are faced with the challenge of navigating an unpredictable strategic environment in which the region has become a space contested by major powers.

Strategic competition happens in the Pacific due to the region's sheer size, the many maritime trade routes and critical ports, natural resources (especially fisheries, but increasingly also sea-bed minerals), and voting rights in international forums where foreign powers seek influence.

This contest brings opportunities as well as risks. Attention from major powers brings economic opportunities, but some states are also carrying out deceptive and corruptive efforts to influence government policy and decision-making in ways that undermine the country's sovereignty and national interests.



Balancing potential national security risks with opportunities for economic prosperity is an ongoing challenge for Pacific countries, including New Zealand, and will continue to be for the foreseeable future.

While there is naturally a range of approaches among Pacific Island countries on international issues, the region's continued emphasis on procedure, regionalism and consensus stands out against a global

backdrop marked in many places by polarisation, inertia and unilateral action.

Such an environment can make it difficult for malign external powers to conduct their deceptive influence campaigns with individual governments, but they will continue to try.

Many of the national security threats New Zealand faces that are outlined in this report are also experienced by our Pacific partners.

Offshore conflicts

Offshore conflicts, such as those in Iran, Gaza and Ukraine, are contributing to the deterioration in global security. Concerning trends from these events have filtered through to our domestic environment.

Most visible is the violent rhetoric online and threatening or intimidating behaviour directed toward people or groups perceived to represent, support or oppose the conflicts.



Surges in violent rhetoric can be stimulated by developments during conflicts, such as high-profile incidents.

Some foreign states and violent extremists seeking to advance their own interests take advantage of the strong emotional and polarised reactions that offshore conflicts can evoke. This involves creating and spreading false or inaccurate information that provokes social and political division.

New Zealand communities are exposed to this inflammatory rhetoric, which sometimes exposes social tensions here. Some groups become stigmatised when an 'us vs them' mentality discourages nuanced and moderate views. Social disruption will be welcomed by state actors or violent extremists who seek to gain from any breakdown in social cohesion.

States' use of proxies

States using criminal proxies or other third parties to threaten their rivals have drawn increasing global attention over the past year.

Considered a type of grey-zone operation or a hybrid threat, this tactic represents an addition to the toolkit for coercive statecraft. These activities lie below the level of direct warfare and can include information operations, political and economic coercion, cyber-attacks, and violence by state-controlled or state-funded actors.

The use of proxies is not a new phenomenon. States like Iran have used designated terrorist entities to undertake activities for decades - notably Hezbollah and Hamas.

The conflicts in Iran and Ukraine in particular have resulted in the emergence of several examples of this activity. Some states have used violent extremist and criminal groups to undertake attacks targeting people, religious sites and businesses in Western countries outside of conflict zones.

The use of proxies may be seen as especially appealing as it creates plausible deniability of the state's involvement while inflicting physical damage.

While New Zealand has not experienced high harm activities by proxies as seen in other Western countries, some recent cyber-attacks are likely to be examples of proxy criminal groups being used in the New Zealand context. The broader use of coercive tools by states will likely be an emerging security challenge in the coming years and we need to be alert to the risk.



Rapid advances in technology

Rapid advances in technology are constantly changing the nature of national security threats in New Zealand.

Generative artificial Intelligence (GenAI) systems, including large language models, offer major benefits for innovation, productivity and eventually prosperity. However, these tools can be also used to enable violent extremism, support state-sponsored foreign interference and to sow division within society.

Hostile states and violent extremist actors are seizing on GenAI capabilities to create and spread content that advances their ideological interests. GenAI makes it cheap and easy to create narratives that exploit psychological vulnerabilities and are tailored to resonate with personal interests or grievances. The technology also allows this information to be disseminated at scale.

GenAI is being used by some states to produce content that enables them to control narratives and villainise perceived opponents. It is also being designed to undermine government institutions and create divisions in society when doing so is useful to the state.

Similarly, violent extremists are using the same technology to create engaging material intended to evoke an emotional response in support of an ideological narrative.

Supporters of the Islamic State have used GenAI to generate and translate ideological content into multiple languages to appeal to a global audience, while white-identity motivated violent extremists have used GenAI to translate and modernise historical recordings of Adolf Hitler to appeal to a modern audience. New Zealanders are accessing this

material and this is a factor in the radicalisation of some individuals.

AI impacts our information environment by amplifying polarising narratives and hiding the source of the content. New Zealanders consuming AI-generated content will mostly be unaware if the narrative was generated offshore or represents genuinely held beliefs.

As AI tools continue to advance, they will become even more effective at tailoring content to specific communities and interested groups. Global conflicts have created fertile ground for both state and violent extremist actors to generate false or misleading content. Information is often curated in a way that frames crises as “good versus evil”.

Violent extremists will seek to capitalise on emotive issues to radicalise and recruit individuals to their cause, while state actors use such inflection points to covertly influence public opinion and create divisions in society to advance their own interests.

In addition to creating and spreading content, GenAI tools have improved the sophistication and accessibility of established technologies including 3D printing and drones. It is possible these technologies could be utilised by hostile actors for malicious purposes before enhancements can be made to policy and legislation to safeguard their use.

Opportunities created by rapid advances in GenAI tools will need to be balanced by greater understanding of how they can exacerbate national security threats such as espionage, foreign interference and violent extremism.



New Zealand's espionage environment

New Zealand's public and private sectors are being targeted by foreign states and their proxies to gain access to critical assets including intellectual property, innovative technology and other non-public information.

The activity NZSIS sees cannot be described as benign. It involves state actors with a voracious appetite for any information they can leverage to gain an advantage over New Zealand or our partners.

Espionage, or spying, is covertly accessing protected information. Foreign states frequently use proxies to do this, and recruit individuals who can provide insight into New Zealand's information and systems. Espionage techniques can also be used to support foreign interference activity.

We see the potential for real harm. The material sought could hand a foreign state access to valuable information relating to New Zealand's policies, decision-making, industry and international relations. Successfully accessing protected information provides foreign states with a strategic advantage against New Zealand and undermines both our national security and future prosperity.

New Zealand is of interest to foreign states seeking to advance their economic interests, military capabilities, technologies and foreign affairs objectives.

Some attempts at espionage will be made through legitimate channels such as open academic exchanges and commercial relationships, while others will use cyber infiltration, fake cover companies or straight-out theft. All will try to obscure any link back to the foreign state.

If the state is highly motivated to obtain a specific set of information, or achieve a specific outcome, they will often use any means at their disposal.

We expect espionage activity to increase in frequency over the next 12 months. Some attempts to gain information and access will likely be successful, but there are a range of simple, cost-effective measures that can make New Zealand a harder target. Please read the protective security information associated with this chapter.

There are several states that conduct espionage against New Zealand, but the People's Republic of China (PRC) is the only country we have detected doing it at scale.

The PRC's intelligence services may be the most active at espionage, but that should not prevent New Zealand organisations from engaging or doing business with entities in that country.

New Zealand businesses should take an eyes wide open approach to espionage across all international markets where they operate. Risks can be managed in a way that ensures future prosperity and preserves New Zealand's national interest.

Chasing non-public information

Foreign states continue to target the New Zealand Government and its officials for non-public information.

Protected information is particularly sought after to help states identify vulnerabilities that would provide it with an advantage over New Zealand and its international partners. However, the scope is much larger than just classified information. Sensitive data on New Zealanders and policy insights that may seem uninteresting could still be of value to a foreign state.

Information collected can also be used to support foreign interference activity or other covert operations conducted by the state.

State-sponsored cyber-attacks are an increasingly common means of accessing networks that hold important non-public information. Following a decline in 2022, the National Cyber Security Centre (NCSC) and its partners have detected a steady increase in espionage-motivated cyber activity against New Zealand over the last three years. The New Zealand Government has also spoken about specific incidents.

Another common tactic currently being used involves recruiting people with government connections or insider knowledge and pressuring them to provide insights.

Given the broad nature of the information being targeted, organisations will also need to take a broad approach to protect sensitive data.



Did you know?

The PRC's national security laws compel any individual or organisation in China to comply with requests from its intelligence services. This could involve handing over data or intellectual property and providing access to systems.

The National Cyber Security Centre, within the Government Communications Security Bureau, produces an annual threat report that includes key judgements on the cyber security environment in New Zealand. Organisations are recommended to use this report to assess their levels of preparedness.

Targeting academic research

New Zealand's universities and research institutions will need to stay alert to attempts by foreign states to secure technology which can be repurposed for military development.

The open and collaborative nature of New Zealand academics, and the cutting edge technology being created within our universities may be exploited under the banner of cooperation or partnership.

Collaboration and innovation drive academic progress and bring financial benefits, but when dual-use technologies are involved, the level of risk is elevated.

Dual-use technologies have both civilian and military functions, but the distinction has become increasingly blurred with modern warfare now weaponising commercial tools such as AI and off-the-shelf drones.

Academic exchanges and talent recruitment programmes are commonplace and are valuable opportunities for New Zealand universities and students. While the vast majority of students coming to study in New Zealand will have genuine intentions, these programmes are used by some states to covertly and illicitly access intellectual property and technology. They also use them as a way to disguise military or intelligence agencies' involvement.

These programmes and associated scholarships provide a powerful financial lever, which can be used by states to compel academics to undertake activities on behalf of the state, irrespective of how these activities could impact New Zealand and our interests.

New Zealand students on overseas exchanges would be surprised if asked to conduct espionage, but authoritarian countries operate with a different playbook.

SAFEGUARDING YOUR RESEARCH

Make informed decisions about who to collaborate with on sensitive research.

Trusted Research guidance, developed in 2022 in partnership with Universities New Zealand and Science New Zealand, remains highly relevant for safeguarding continued open collaboration through good risk management.

It includes advice on managing cyber risks, protecting personal and research data and how to stay compliant with the exports control regime.

Read the guidance at:

 [www.protectivesecurity.govt.nz/
trusted-research](https://www.protectivesecurity.govt.nz/trusted-research)

Targeting New Zealand's private sector

Academic researchers are not the only target. Over the last year, some foreign states have attempted to target New Zealand's businesses and non-government organisations to covertly gain access to intellectual property, innovative technology, and other resources.

Espionage has an economic cost. Losing control of crucial intellectual property can prevent commercialisation of an innovation or an idea. States targeting private businesses are usually looking to access technology that could accelerate their industrial or military capabilities at New Zealand's expense.

TIAKI PĀKIHI MĀORI

Māori businesses and entities also have espionage risks to manage.

NZSIS and NCSC worked with a group of Māori security professionals to develop Tiaki Pākihi Māori: protective security for Māori businesses and entities.

The guidance approaches security through a Te Ao Māori lens. It includes case studies to describe how entities have been compromised and shows the impact of weak practices.

Tiaki tangata, tiaki mātauranga, tiaki taonga. Read the guidance at:

 [www.protectivesecurity.govt.nz/
tiaki](https://www.protectivesecurity.govt.nz/tiaki)

Use of front companies

Over the past year, we have seen foreign states attempt to deceptively obtain sensitive technology while covering up the paper trail.

Some states will attempt to acquire sensitive technology through international front companies and supply chain intermediaries by presenting a plausible cover story designed to allay any security concerns. Brokers and resellers may also be used to conceal an end-user's identity.

Intermediaries may try to approach an organisation's leadership with an investment opportunity or aim to recruit employees to facilitate a transfer of technology or knowledge.

Foreign states hope to fly under the radar as a regular commercial operator. They assume companies will only do surface-level due diligence on the intermediary's business and not question why they are seeking the technology. False declarations will also be made. Once the goods are acquired, they might be routed through a number of overseas jurisdictions and trade hubs to further disguise the final customers which often include states such as Russia and Iran.

As explained earlier, foreign states may try to steal the technology in multiple ways. For example, while

trying to access technology through a front company, they may also be trying to breach the organisation's cyber defences at the same time.

It pays to strategise ways vulnerabilities may be exploited and understand the various ways commercially sensitive intellectual property might be used. By protecting New Zealand's technology, we also protect our economy and ensure New Zealand preserves its reputation as a safe and secure place to innovate.

CASE STUDY

Front companies can be used as a way to circumvent international sanctions and export controls. A Russian state-owned organisation sought to acquire specialised components from the offshore subsidiary of a New Zealand registered company. The technology could have been used to enhance Russia's military capability. The link to Russia's government was concealed during the approach as international sanctions and export controls meant there was no way for the organisation to legitimately access these components. Once the New Zealand company was informed of these links, they made sure additional due diligence documentation about end users was sought by their subsidiary.

Targeting operators of Ground Based Space Infrastructure

New Zealand has a flourishing space sector, but over the past 12 months New Zealand's intelligence agencies have identified foreign state actors seeking to exploit the industry's reputation for cooperation and partnership.

Our strategic location makes New Zealand an ideal place to install Ground Based Space Infrastructure (GBSI). The equipment is designed to track satellites and space debris, as well as for collecting a range of other scientific data. GBSI is also attractive for foreign states seeking to advance military capabilities and intelligence operations.

New Zealand and Pacific Island countries are well placed to track satellites passing over the Asia-Pacific in a variety of orbits, with minimal radio frequency interference and visual impediments. New Zealand can be the first or last opportunity to observe and communicate with satellites transiting regions with low GBSI coverage.

While investment in New Zealand's space industry is welcomed, some state actors and co-opted entities seek to deceptively install GBSI to advance their country's capabilities without authorisation or transparency about how it will be used, and for whose advantage.

Legitimate GBSI operators in New Zealand have been led to believe they are entering a commercial or research partnership with a foreign entity, but the company's links back to a foreign state have been deliberately obscured.

A foreign state illicitly exploiting our space industry in this way undermines New Zealand's sovereignty, and the information gathered has the potential to be used against our interests, such as covertly informing another country's military activity.



Did you know?

GBSI operators are now regulated under the Outer Space and High Altitude Activities Act to protect New Zealand's national security, foreign relations and national interests. Operators must obtain authorisation to carry out regulated activities and are required to include annual reporting verifying that protective security and due diligence arrangements remain up to date.

CASE STUDY

Purple Mountain Observatory, an organisation based in the People's Republic of China with close links to its government was found in the past year attempting to install Ground Based Space Infrastructure in New Zealand.

They worked with a local company that was likely unaware of the equipment's capability to collect intelligence of military value and would have no idea who was receiving the data.

Purple Mountain's close links to the PRC Government means they could be compelled to pass on any data collected, however, in this case we assess it would have been willingly passed on.

NZSIS, working with other agencies was able to disrupt this activity, but it was not the first time this organisation has attempted to install its own GBSI in New Zealand and is unlikely to be the last.

Legitimate GBSI operators in New Zealand and those in the Pacific are encouraged to sharpen their due diligence practices as future attempts will likely use more obfuscation.

SECURE INNOVATION

Protect your innovation from espionage and adopt the Secure Innovation principles.

The following five principles were developed alongside our Five Eyes partners as a framework for protecting an organisation's critical intellectual property.

Know the threats – understand the potential vulnerabilities that may put your innovation at risk, including the other ways it could be used.

Secure your environment – appoint a security lead at board level to strengthen oversight.

Secure your products – build security into the front end of your products by design.

Secure your relationships – make sure you can trust your collaborators with your intellectual property.

Secure your growth – manage risk around entering new markets and hiring new staff.

Protect your innovation from falling into the wrong hands. Read the guidance at:



[www.protectivesecurity.govt.nz/
secure-innovation](https://www.protectivesecurity.govt.nz/secure-innovation)

Espionage activities linked to the wider Pacific

NZSIS is increasingly coming across espionage activities that while affecting New Zealand are primarily directed towards the broader Pacific region.

Intelligence officers and co-optees are also active in the Pacific seeking to gain insights and information which is used to undermine Pacific regionalism, sovereignty and the national interests of a range of countries. When NZSIS identifies links to the Pacific while investigating threats to our national security, we share intelligence with Pacific partners and work with them to help support the Pacific country's decision making.

CASE STUDY

Through domestic security intelligence investigations, NZSIS has identified individuals carrying out espionage and foreign interference activities in the Pacific on behalf of a foreign intelligence service. These activities seek to advance the foreign state's policy objectives through deceptive and corruptive means. These actions undermine the security and sovereignty of New Zealand and Pacific countries. NZSIS shares this intelligence with relevant Pacific partners along with protective security advice on how risks can be managed.

TRAVEL SECURELY

New Zealanders have had devices compromised or have been subject to surveillance while travelling overseas for work.

Think about how to protect your most critical assets overseas. Sometimes that might mean leaving your main device at home and taking a clean and secure phone or laptop without any personal information or sensitive data.

Our guidance helps you plan to travel securely with advice for before you travel, while you are away and when you return home.

Travel safe and protect your critical data. Read the guidance at:

 www.protectivesecurity.govt.nz/overseas-travel

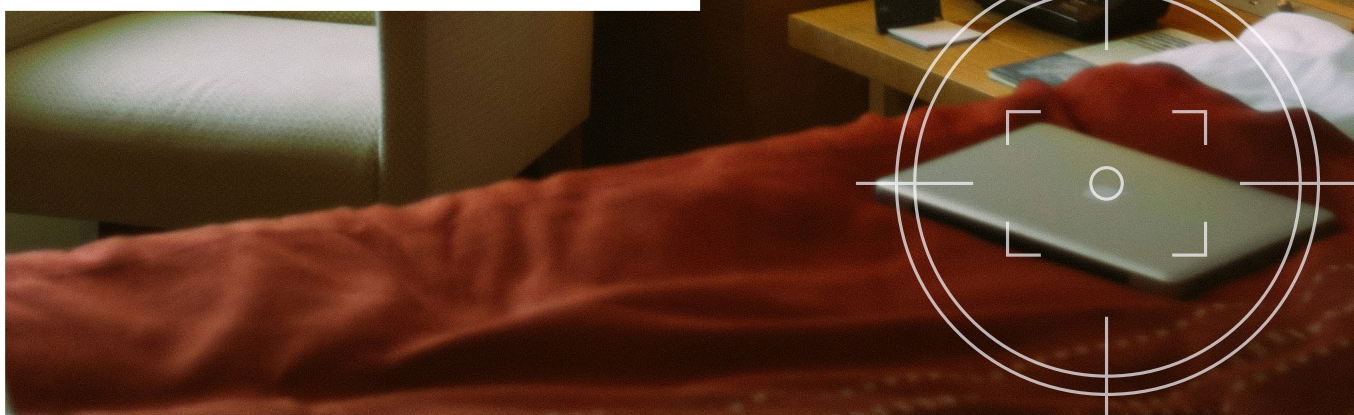
SECURE YOUR RELATIONSHIPS

Investment opportunities can be a vector for espionage.

NZSIS's Due Diligence guidance provides a list of considerations when assessing the risk of a new or existing relationship.

Read the guidance at:

 www.protectivesecurity.govt.nz/due-diligence



Recruiting New Zealanders with inside access

We have observed increased targeting of professional networking sites and online job platforms for espionage purposes by China's military intelligence services.

Specifically targeted are current and former New Zealand Government officials who have had access to classified or sensitive information. Five Eyes partners have had similar experiences.

PRC intelligence officers, or their affiliates, use an aggressive strategy where they pose as consultants or employees of think tanks, or recruitment firms. They place online job advertisements looking for analysts in foreign policy, international relations, defence or security.

Candidates are then vetted by PRC intelligence to determine what information they have had access to and whether they would divulge it. Sometimes

the assessment will involve paying a candidate to produce research papers on specific topics to understand the depth of their knowledge.

Successful candidates are pressured to provide privileged non-public information for unspecified clients who have obscured their links back to the PRC government.

The job offers are lucrative, but the intelligence officers often encourage their candidates to keep their government jobs both to keep the information tap running and to open up opportunities to recruit their colleagues.

These offers are about much more than earning some extra cash on the side. PRC's intelligence services are ultimately after privileged military, political and economic intelligence to support their state objectives.



How fake PRC recruiters target government and military officials

1. **First contact:** job ads posted on professional networking sites or gig work websites.
2. **Interview:** recruiters conceal their identities during virtual interviews and ask probing questions about government contacts.
3. **Initial testing:** candidates asked to write a trial report to test levels of knowledge.
4. **Encrypted apps:** contact moves on to secure messaging platforms where recruits are informed the client requires more privileged information.
5. **Payment:** Recruits are paid according to the quality of their reports through third-party payment platforms.

Read the Five Eyes Bulletin:
Safeguarding our Secrets

 [www.nzsis.govt.nz/
news/safeguarding-our-secrets](https://www.nzsis.govt.nz/news/safeguarding-our-secrets)

04

Insider Threat

More insiders in organisations are causing harm to their organisations and to our national security through actions that are either deliberate, influenced by others or unwitting.

Both public and private sector organisations in New Zealand are vulnerable to harm from insider threat activity such as unauthorised disclosure of sensitive information, theft of intellectual property, process corruption, compromise or misuse of assets, or sabotage.

Foreign states are increasingly targeting insiders for espionage opportunities but sometimes an insider might be motivated by personal reasons or because they have been incentivised or coerced by another third-party.

An “insider” is considered anyone who has, or previously had, access to knowledge of an organisation’s resources. Knowledge may include information about people, processes, information, technology, and facilities that is not accessible to the general public. Very few employees will become an insider threat, but it is an important risk to manage due to the harm that can be caused.

Over the previous 12 months, we have seen instances of deliberate, influenced, and unwitting insider acts.

Deliberate insiders

Deliberate insiders purposely cause harm to their organisation for a variety of reasons. They may have developed a grievance, or the job has not met their expectations.

In many cases, the insider act follows a period where they have been under pressure or have been exhibiting out-of-character behaviour.

CASE STUDY

An employee at a government agency had a change in their personal life that started to affect their judgement at work. The person never told their peers or managers what was happening out of fear it would tarnish their image as work was central to their identity.

Their job involved working closely with another agency where they held a position of trust. They did not admit they were under strain and their behaviour eventually culminated in an insider act when they misused privileged access to the other agency’s system for a personal reason.

The breach caused reputational damage to both agencies. A security investigation followed where the individual deliberately hid details of their actions. They were subsequently dismissed from their role. The person’s focus on saving face, and their reticence to ask for help has harmed them personally as well as the two government agencies.





Influenced insiders

Influenced insiders may be coerced or incentivised to cause harm. They might face external pressure from foreign states or criminal entities, or from individuals who wish to harm the New Zealand government or our national security.

NZSIS has seen examples where an insider has been incentivised with a financial reward or the promise of an increase in status.

Vulnerable people can be manipulated by skilled actors to misuse their privileged access as an employee to support a criminal group or foreign state. Such deception can have a wide spectrum of serious consequences, including compromising our national security, degrading a system or capability, eroding trust in New Zealand's institutions, economic damage, and, in some cases, physical destruction or injury.

CASE STUDY

A New Zealander put themselves at risk by advertising their security clearance on their social media profile. This captured the attention of a foreign state actor, who used a cover company to offer them a lucrative contract. The person suspected the recruiter may not be a legitimate employer, but the high salary and attractive job offer incentivised them to continue the recruitment process. The NZSIS worked with their employer to raise awareness of the security concerns it generated and to mitigate the risk.

Unwitting insiders

Unwitting insiders cause harm through negligence, poor practices or naivety. Even though there is no intent to cause harm, the consequences of their actions can be widespread and long-lasting.

CASE STUDY

NZSIS investigated an individual working for the New Zealand Government who responded to an online job offer and unknowingly agreed to work on behalf of a foreign state. The person did not tell their employer they were taking on secondary employment and neglected to carry out proper due diligence on the company they agreed to work for. A few simple checks would have identified this was not a legitimate company. Even though they did not mean to, the person shared insights and perspectives that were in part informed by their role in the New Zealand Government. Reckless sharing of such insights can still harm New Zealand's national security – even if not expressly drawn from classified documents. NZSIS worked with the employer and made sure the individual had advice on how to spot employment traps by foreign states.

Common factors in New Zealand insider threat cases

Generally, no single factor can lead an insider to undertake an insider threat act. Instead, a series of events and pressures can make an insider become more vulnerable.

Examples NZSIS has observed include financial stress, challenges at work, concern about international conflict and global instability, or mental health challenges.

Motivations for undertaking an insider threat act are complex and varied, and can include a combination of disgruntlement, grievance, ambition, financial motivation, complacency, or naivety.



Five principles for a shared approach to insider risk

The NZSIS encourages all organisations to develop an insider threat programme both to help identify potential threats early and to support staff who may be vulnerable.

Five principles underpin the advice we provide government agencies and the private sector.

1. **Adopt a shared language**
Definitions encourage consistency and help you understand the harm.
2. **Broaden your understanding of potential insider threats**
What assets need protecting and what could happen to them.
3. **Consider the 'spectrum of intent' from unintentional to intentional insider activity**
Develop systems that target all types of insider risk.
4. **Detect signs of insider threat and act to de-escalate**
Signs are often visible, so what are the opportunities to intervene?
5. **Learn the foundations for effective interventions**
Build an effective security culture with measures that shape the environment and limit the opportunities for insider events to take place.

Our guidance, *Secure Your Team: Five principles for managing insider risk* is available at:

 [www.nzsis.govt.nz/
secure-your-team](https://www.nzsis.govt.nz/secure-your-team)

If you notice any of
these behaviours or
activities, let us know at:
nzsis.govt.nz/report

New Zealand's foreign interference environment

Foreign interference actors are seeking access to New Zealand-based communities, groups, organisations, or politically significant people in order to influence, disrupt, or subvert our national interest.

There are two main forms of foreign interference: political and societal.

- **Political interference** includes acts by a foreign state intended to subvert, disrupt or influence governance, democratic institutions, and processes including elections or policy-making.
- **Societal interference** is intended to influence or disrupt New Zealand's communities and non-government sectors.

For activity to be considered foreign interference, it must be deceptive, corruptive, or coercive. Often, the people carrying out this activity are not formally employed by the foreign state. Instead, they are usually coopted to act as state proxies. People can be recruited to willingly carry out a foreign state's objectives while others may do it unwittingly.

Over the past 12 months, NZSIS has observed states deceptively and coercively engaging with community groups and attempting to suppress social and protest movements.

The PRC continues to be the most active at conducting foreign interference in New Zealand, but there are several other countries doing it as well to varying degrees and scale.

New Zealand's ethnic communities are frequently the targets of this activity. It is the state actors who are the focus of NZSIS's attention – communities are the people we are trying to protect.

The Pacific region remains an area of high interest and competition between states seeking to influence countries and communities to support their geopolitical interests.

As this period of global instability continues, we expect foreign interference activity will likely intensify as states become more openly aggressive in pursuing strategic advantage.



Did you know?

NZSIS's work to help protect elections from national security threats is undertaken in a politically neutral way and in accordance with our obligations under the Intelligence and Security Act. Like the rest of the Public Service, NZSIS staff are also subject to the Public Sector Code of Conduct and the Commissioner's General Election Guidance.

Political interference in New Zealand

NZSIS has seen foreign interference activity targeting politicians, candidates and politically influential people. Efforts to build influence are expected to continue, including throughout the upcoming election period in late 2026, but are unlikely to impact the election results.

Foreign interference actors will likely exploit the accessibility of political candidates while they are out campaigning to build relationships.

Individuals who are close to candidates, such as their community contacts, advisors and staffers, can also be targeted due to their access and perceived influence. Some foreign states will highly likely use any opportunity in front of a candidate to portray diaspora communities as politically homogenous and aligned with the state's interests. Their plan is to leverage the communities' political power to gain

influence. In some cases, candidates will think they are engaging with representatives or spokespeople for diaspora communities, when in fact it could be a foreign state actor.

Co-optees, disguising their foreign state links, might also use donations, gifts and hospitality to build a relationship with a candidate that could be later leveraged, sometimes years later. Such efforts are often ongoing and also happen outside of election periods.

NZSIS monitors national security threats associated with general and local elections along with providing protective security advice to political parties, candidates and election administrators. We remain alert to any foreign interference threats that seek to undermine New Zealand's free and fair democratic processes.



BE VIGILANT TO FOREIGN INTERFERENCE

Political candidates should not be deterred from attending events or engaging with diverse communities in New Zealand.

Candidates, party officials and advisors, or volunteers can protect themselves against foreign interference efforts by being vigilant about persistent approaches, checking any links to a foreign government and by understanding the background to any donation, gift or event they are invited to attend.

Read our advice at:

 [www.protectivesecurity.govt.nz/
elected-representatives](https://www.protectivesecurity.govt.nz/elected-representatives)

Societal interference in New Zealand

TRANSNATIONAL REPRESSION

Diaspora community groups in New Zealand are being unfairly targeted by foreign states and their proxies seeking to limit the democratic rights and freedoms they enjoy as New Zealanders.

States are increasingly using the threat of legal and administrative action, also called “lawfare”, to influence people’s behaviour. This is a type of transnational repression (TNR) and is part of a range of behaviours and activities we see affecting communities in New Zealand including foreign state-directed surveillance and harassment of their family members overseas.

Lawfare has been a consistent theme in recent months where we have seen the threat of consular services being refused, and passports and visas withheld.

People have been prevented from travelling to their country of origin and accessing bank accounts or property unless they moderate their perceived behaviour to align with the state’s preference. NZSIS is aware of several states threatening to “blacklist” people in New Zealand unless they stop advocating for a particular protest or political movement.

Such threats are unacceptable in New Zealand and all diaspora communities should be aware that they do not have to tolerate any restriction on their democratic rights and freedoms.

Why we use the term “diaspora”: We are referring to a group of people with cultural, ancestral or familial ties to another state. Being a member of a diaspora community does not take away from someone’s identity as a New Zealander, but some foreign states view this differently.

If you notice any of
these behaviours or
activities, let us know at:
nzsis.govt.nz/report



Did you know?

Changes to the Crimes Act in November 2025 created criminal offences to address foreign interference activity in New Zealand. It’s now illegal to undertake improper conduct for or on behalf of a foreign state in a way that compromises New Zealand’s interests.

GATEKEEPING

New Zealanders enjoy uncensored access to media and can read a diversity of perspectives. There are foreign states, however, that try to prevent diaspora populations from experiencing the same rights and privileges.

We continue to observe some foreign states seeking to exert control over what information communities have access to in non-English media outlets. Attempts are made to manipulate information, including by portraying the New Zealand Government as supportive of the foreign state’s narratives, even if no such statements have been made.

Community leaders are also leaned on to ensure diaspora communities in New Zealand hear the approved messages. Such behaviour is an example of gatekeeping where a co-opted group or individual places themselves as a go-between for a particular community to control the flow of information.

Foreign states facilitating these activities are trying to act as gatekeepers over the information communities are allowed to see, while at the same time trying to disguise the role they played. Such coercive and controlling behaviour is foreign interference and is designed to crowd out or silence perceived dissidents.

CASE STUDY

A foreign state official encouraged a community leader to lobby New Zealand authorities to prevent an organised protest event from occurring. The foreign state representative almost certainly intended this petitioning to appear as genuine community sentiment, and for it to support official lobbying efforts at the diplomatic level.

UNWITTING SUPPORT FOR SOCIETAL INTERFERENCE

Attending community events is part of the job for many central or local government representatives or officials in New Zealand. These engagements contribute to the richness of our society. They ensure diverse voices are heard and have the ability to inform policy decisions in their own communities. In some cases, however, these events are being exploited by foreign state actors to send a message to perceived dissidents within diaspora communities.

Foreign states routinely use events like these to choreograph photo opportunities with officials to portray some kind of ideological support with the state's objectives. A New Zealand politician or official posing for the picture would expect the photo is simply to record the occasion. But sometimes the attached narrative, or just the existence of the photo when it is published, will add legitimacy to efforts to denigrate, or further marginalise, a perceived dissident group.

The community members on the receiving end of such activity are made to feel isolated by the portrayal of familiarity with someone they see as representing their oppressor. They may lose faith in public institutions or lose their sense of belonging in New Zealand as a result.

Politicians or officials should not be deterred from participating in event photos as engagement with diverse communities is important, but it is reasonable to ask how that photo might be used and to ask for approval before its published.

CASE STUDY

NZSIS continues to see a particular foreign state's diplomatic mission pressuring local government representatives and community groups to exclude perceived dissidents from events. Such requests are happening around the country. Event organisers are persuaded that the inclusion of people who are offside with the foreign state will cause diplomatic ructions and upset the community. The foreign state representatives will hide their real intentions, which are to exert control over who they consider to be dissidents and suppress these views from reaching the wider community. Foreign states have no legal remit to exert such control over communities in New Zealand, and any such actions are inconsistent with our democratic values.

MANAGE INWARD VISITS

Organisations should not feel compelled to accept foreign delegations when there are no obvious benefits from the visit.

The Managing Inwards Visits guidance provides a framework for considering both the opportunities and security risks brought by foreign delegations.

Seek clarity about the purpose of the visit and consider any reputational costs that might arise from hosting.

Make sure hosting delegations are in your interests. Read the guidance at:

 [www.protectivesecurity.govt.nz/
inwards-visits](https://www.protectivesecurity.govt.nz/inwards-visits)

Did you know?

We see instances of pressure placed on organisations and communities about events on topics a foreign state would prefer not be discussed. These requests can become heated and result in threats of economic coercion. Foreign states do not get to dictate such matters in a democratic society. The Ministry of Foreign Affairs and Trade can provide advice to support organisations with these relationships.



ADVICE FOR COMMUNITIES

NZSIS is keen to hear when communities have experienced any of the behaviours and activities described in this section of the report.

Members of ethnic communities will likely see concerning activity before the NZSIS. Letting us know helps us to understand how common foreign interference is in New Zealand and gives us more options to work with partners across government to disrupt and call it out.

Information is treated in confidence. Community members may think their experience or information is insignificant, but it could help us to solve a wider intelligence puzzle.

Foreign interference harms New Zealand's national security and attacks our democracy. Let us know in the language of your choice by clicking on "report a national security concern" on the NZSIS website. www.nzsis.govt.nz.

COMMUNITY RESILIENCE TO FOREIGN INTERFERENCE HUB

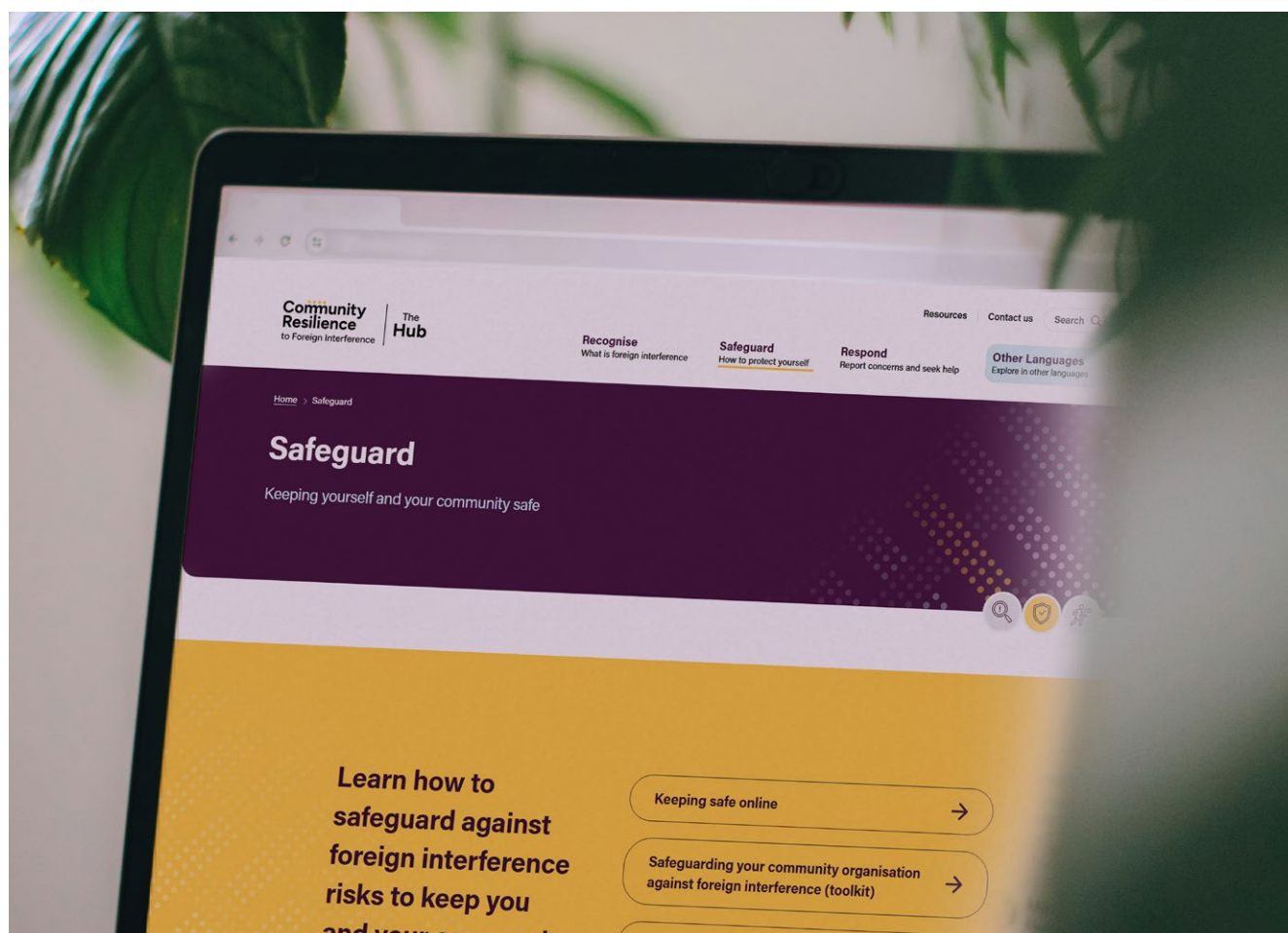
Ethnic communities in New Zealand do not have to tolerate foreign interference.

The Ministry for Ethnic Communities has launched the Community Resilience to Foreign Interference Hub, an online platform providing information, practical tools and resources for communities.

Developed with communities in mind and informed by their experiences, the Hub reflects a growing recognition that ethnic communities are not simply affected by foreign interference, they can also play a key role in strengthening New Zealand's resilience.

The Hub is designed to be an enduring platform for building community resilience. It will evolve to meet community needs and the changing nature of foreign interference.

Resources are available in 31 languages at www.crfi.govt.nz.





New Zealand's violent extremism environment

Identifying a violent extremist in New Zealand with real intent and capability to carry out an attack is increasingly difficult amid an online environment saturated with potentially radicalising content.

Violent extremists in New Zealand continue to be influenced by a broad range of ideologies, online rhetoric, domestic and global events, and personalised grievances. A disproportionate number of young people are coming to our attention after adopting increasingly extreme political, social, or religious beliefs that are motivated by violence.

NZSIS is tasked with finding violent extremists – people who justify the use of violence in order to achieve radical political, social or religious change in New Zealand.

Part of our job is to work out whether someone's vitriolic and violent online pronouncements have any link to New Zealand, and then whether they have the genuine intent and capability to take the next step and commit an act of violence underpinned by an ideological motivation.

This is a narrow focus but the pool of information and intelligence we are working with is vast.

We used to describe our work as finding a needle in a haystack. However, the internet has changed. Large volumes of toxic content, widespread anonymity, and hidden locations mean our job is now like looking for the sharpest needle in endless giant stacks of needles.

Extremist rhetoric, particularly online, has become more mainstream, a development which has made it even more challenging to differentiate between genuine support for violent extremism, hateful language designed to shock, or online content created simply to drive engagement or "likes".

The most common violent extremist ideologies seen in New Zealand remain identity and faith-motivated violent extremism. However, cases where an individual's beliefs do not fit within any distinct ideological category are now commonplace.

Read our definitions of violent extremist ideologies on page 33.

During these current times of global conflict, political and economic volatility and societal disruption, violent extremist narratives are becoming more normalised, particularly online.

New Zealanders have been exposed to groups using online channels to recruit or radicalise across all extremist ideologies.

Established faith-motivated violent extremist groups such as the Islamic State and al-Qa'ida continue to grow in some permissive regions across the Middle East, Asia and Africa. Due to the pervasive influence of the internet, these groups have been able to reach New Zealanders through spreading propaganda and other harmful ideological content.

White identity violent extremist groups tend not to be as cohesive, but their online recruitment tactics are similar, and they are finding willing consumers of their content in New Zealand.

It remains the case that New Zealanders are searching for, accessing and sharing this content, including the young and vulnerable. Exposure to such material can hasten a young person's pathway to radicalisation, especially when there is little monitoring or regulation of their online behaviours.

Likely violent extremism scenario in New Zealand

Under New Zealand's National Terrorism Threat Level framework, a terrorist attack in New Zealand is currently assessed as Possible.

The most plausible attack scenario remains someone acting alone, who has been radicalised online, takes steps to avoid detection and who mobilises to violence with little to no intelligence forewarning.

They are likely to use basic capability that is easy to access such as a firearm, bladed weapon or vehicle to target people in a crowded place or somewhere with symbolic significance.

NZSIS has also observed instances of individuals attempting, or aspiring, to access more advanced capability including Improvised Explosives Devices (IED) and 3D printed firearms.

Artificial Intelligence tools and the growing availability of technology like 3D printers can make it easier for a motivated individual to build or gain access to more advanced capabilities.

The Combined Threat Assessment Group (CTAG) is responsible for reviewing New Zealand's Terrorism Threat Level, and at the time of this report's publication, assesses a terrorist attack in New Zealand is Possible. This assessment considers the likelihood there are violent extremists with credible intent to undertake an ideologically motivated attack in New Zealand, and access to the capability to do so.

New Zealand's National Terrorism Threat Level has remained unchanged since 2022.



Terrorist attack is assessed as possible

Protecting Crowded Places

New Zealand Police has led work, alongside NZSIS and other agencies, to develop a strategy that sets out a consistent approach to promoting the safety of crowded places, including how to respond in the event of a terrorist attack.

Crowded places are locations that large numbers of people access easily and predictably. They include sporting arenas; transport hubs and public transport; buildings and offices; schools; shopping centres; restaurants, hotels, theatres and other entertainment venues; community festivals and markets; places of worship; tourist attractions; and civic spaces. Crowded places also include open spaces like busy urban streets, parks and pedestrian malls.



KNOW WHAT TO DO
www.police.govt.nz/crowdedplaces

Know what to do in an attack...



ESCAPE

Move quickly and quietly away from danger, but only if it is safe to do so



HIDE

Stay out of sight and silence your phone



TELL

Call the Police by dialling 111 when it is safe

Radicalisation in New Zealand

Individuals in New Zealand who follow a violent extremist ideology will have largely self-radicalised online.

The internet is awash with extremist content. Not all of it will be violent extremism. Extremism is considered religious, social or political ideologies that exist substantially outside of more broadly accepted belief systems and are often seen as offensive to large parts of society. Extremism becomes violent extremism when violence is encouraged or viewed as justified to realise those beliefs.

Individuals become radicalised after gradual and increasing exposure to material where violence is portrayed as a justification for radical change.

There have been cases in New Zealand where a fascination with violence has been an entry point to someone eventually adopting a violent extremist ideology. Once down a rabbit hole, platform algorithms can serve up even more extreme content and create echo-chambers in which few alternative perspectives appear.

We are increasingly seeing cases where someone's pathway to radicalisation may see them exploring and adopting a range of sometimes conflicting ideologies. We have observed people, for example, who have an interest in Islamic State propaganda and white identity extremist material at the same time.

The internet provides a place where even those with the most niche of beliefs or grievances can find likeminded communities.

Violent online communities

Algorithms on various social media platforms can link non-violent content to progressively more extreme material. The gateway subject matter can quickly expose people to violent extremist content that can support radicalisation.

New Zealanders are not just end consumers of these narratives. NZSIS has observed New Zealand violent extremists use encrypted messaging systems, social media and online gaming platforms to circulate violent material including weapon tutorials and

objectionable content. Their presence on these platforms, many of which are mainstream, also helps them to find likeminded individuals or supporters.

Male supremacist beliefs are shared within particular communities and are easy to find online. Adherents seek to preserve and advance male dominance by advocating for fixed gender roles. These views exist on a spectrum ranging from non-violent, like the 'tradwife' subculture, to violent male supremacy which encourages violence against women.

Online communities are formed around a range of violent extremist narratives. Members rarely know each other's true identity or the country where they live so these are not real-world friendships.

Violent extremist chatrooms are dark places where terrorist attacks are discussed, and attempts are made to recruit and radicalise others. Hiding behind online aliases, users feel safe to share or seek out extremist content confident that they will not face any real world consequence.

Provocative memes, dark humour and a sense of shared community draw in vulnerable or isolated individuals who find validation from others with similar grievances and ideological beliefs.

The use of youth slang and coded language within these chatrooms generates a group identity that reinforces who are the insiders and who is an outsider. Such insider slang also helps users evade moderation efforts by platforms.

We continue to notice that it is young and vulnerable people who are most likely to be susceptible to radicalisation in these environments. Young people and individuals with vulnerabilities such as mental ill health are seeking connection, especially when they struggle to maintain real life relationships.

Members of violent extremist chatrooms appeal to vulnerable newcomers by offering a false sense of connection and the freedom to be as provocative as they want.

CASE STUDY

A young person's concerning online posts were brought to the attention of the NZSIS by a member of the public. The posts appeared to indicate the individual was trying to engage with like-minded extremists, including people previously known to support violent extremism. The young person's content was provocative, suggesting a possible intent to carry out violence related to their ideology. NZSIS undertook an investigation and was able to assess that it was unlikely the young person had genuine intent to mobilise to violence, and their concerning posts were highly likely an effort to impress the extremist actors they were interacting with online. This individual is currently receiving targeted support by other agencies through the He Aranga Ake disengagement framework (see p.31).

Report your concerns

Cases involving young people are treated with extreme care and sensitivity.

nzsis.govt.nz/report

Violent extremism in the mainstream

Violent extremist content and narratives are becoming more accessible. Often such material may only be a few clicks away from more innocent content.

Unfortunately, the Christchurch terrorist attack livestream is frequently accessed and shared within New Zealand. The video is classified as Objectional Material and viewing or sharing of it is illegal in New Zealand. It is strongly encouraged to report such activity to NZSIS or Police. In much the same way as Islamic State propaganda videos, such content is known to contribute to or hasten someone's radicalisation.

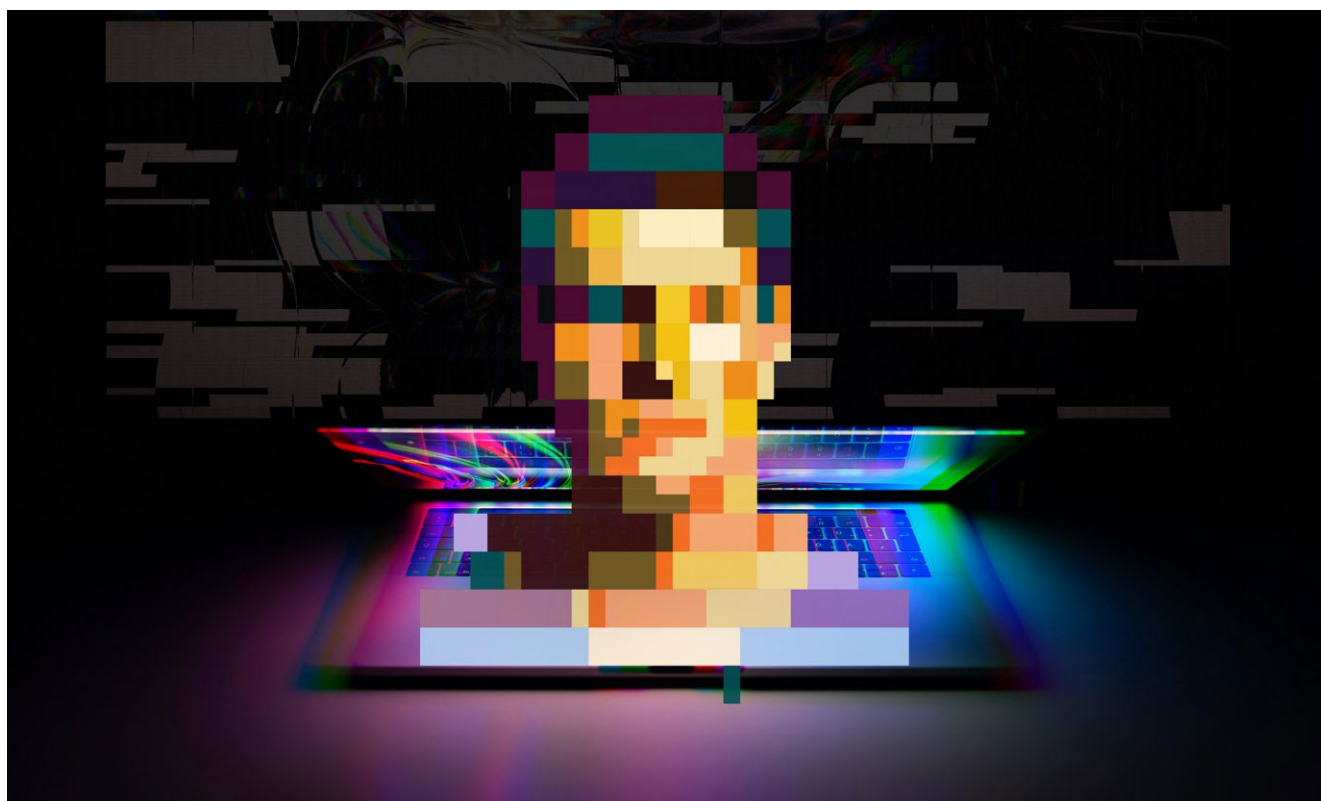
Often individuals who access this material have no violent extremist intent and capability, but our teams still need to know so an assessment can be made. Young people who have been exposed to this kind

of content may need to be referred for wellbeing support given the distressing nature of the material.

We also see beliefs and theories that were previously regarded as wholly unacceptable become more mainstream.

An example is the wide promotion of the Great Replacement Theory, a white nationalist conspiracy that falsely claims there is a plot by global elites to replace white populations in Western countries with non-white immigrants. Online influencers or well-known public figures are harnessing discontent by floating such extremist or violent extremist views.

When influential figures platform these ideas, it has the effect of reducing inhibitions about sharing this material and normalises the rhetoric. It can also contribute to an individual's radicalisation.



Emerging trend: nihilistic violent extremism

Nihilistic violent extremists advocate for violence to change society to one without moral and legal restrictions. A nihilistic society is one where any form of behaviour is permissible, including murder, sexual assault, child sexual abuse, and torture.

The phenomenon primarily develops within transnational online communities where graphic violence, violent extremist narratives, criminality and abuse are normalised, shared and rewarded.

Many of the individuals associated with these online communities are young people. NZSIS has an ongoing line of effort to understand how this movement could present in the New Zealand context and determining when support for an ideology online could translate to real-world violence.

Report your concerns

NZSIS and Police rely on members of the public to report any concerns regarding any of the behaviours and activities discussed in this section.

Let us know through the reporting function on our website. If it's an emergency dial 111.

CASE STUDY

An individual was reported to NZSIS for allegedly making online threats to carry out an act of violence in New Zealand, using an easily accessible weapon. The person was known to be a member of online groups linked to ideological nihilism, although there was no indication they understood or adhered to the ideology. It turned out the person had other criminal interests that motivated their interest in violence. Given this, NZSIS assessed in this case any act of violence would be more likely motivated by a personal grievance than a violent extremist ideology. The person is currently in prison on other charges.

Preventing and countering violent extremism in New Zealand

All New Zealanders have a role to play in preventing terrorism and violent extremism – from staying safe on the internet to helping to detect threats and prevent attacks.

NZSIS supports the following resources and programmes to help identify concerning behaviours and activities and to promote disengagement from a radicalisation pathway.

KNOW THE SIGNS

NZSIS produced Know the Signs in 2022 to help New Zealanders identify indicators of violent extremism. All 50 indicators included in the guide have been observed within New Zealand in investigations dating back to 2006.

The guidance was recently reviewed for relevance to the current threat environment and was found to be still indicative of modern trends and behaviours.

Reporting is strongly encouraged when these activities are observed so violent extremist intent and capability can be assessed. The earlier concerns are reported, the more options there are for disengagement that do not necessarily need to involve the criminal justice system. All information provided is treated in confidence.

Seven themes associated with violent extremism in New Zealand

- Mindset and ideology
- Association and relationships
- Research and planning
- Gathering knowledge and resources
- Preparation
- Security awareness
- Unusual changes in behaviour

Read more about these indicators at: <https://www.nzsis.govt.nz/knowthesigns>.

CLASSIFICATIONS OFFICE

The Classification Office has worked with young New Zealanders extensively about the kinds of harmful content they are viewing online, and surveyed adults to get their perspective too. As a result of this work, they have developed a range of insights and resources to help caregivers and educators support them to navigate the online world.

Find out more: <https://www.classificationoffice.govt.nz/resources/?subject=violent+extremism/>

Find out more about harmful and potentially illegal content at: <https://www.classificationoffice.govt.nz/classification-info/what-is-harmful-and-illegal-content/>

HEADSPACE INVADERS

Headspace Invaders is an interactive platform developed by Netsafe that helps young people aged 12 to 16 build confidence and critical thinking skills when navigating online content. It supports early action in response to manipulation, pressure, and harm online.

Try the platform, explore the modules, or access free resources for educators and families at Headspace Invaders | Critical Literacy for Young People

<https://netsafe.org.nz/headspace-invaders>

POSITIVE ONLINE INTERVENTIONS

The NZSIS and other agencies worked with Explore Hāpainga Ora to create a series of online learning modules designed to help reduce the risk of radicalisation by equipping frontline professionals with the tools to engage early, safely, and effectively.

Grounded in international best practice and tailored to New Zealand's unique cultural context, this course supports educators, youth advocates, social workers and counsellors among others to protect young people from online harm.

Sign up to the course at Preventing and Countering Violent Extremism (PCVE) – Positive Online Interventions

<https://myskill.co.nz/product/building-the-capability-of-aotearoa-to-prevent-and-counter-violent-extremism/>

HE ARANGA AKE

He Aranga Ake is a multi-agency disengagement programme intended for someone who may pose a violent extremist threat of harm to a community or themselves.

It receives referrals from participating government agencies and provides a New Zealand specific disengagement approach to each individual accepted. Support is delivered through coordinated bespoke intervention plans, which target individual and environmental protective factors.

Find out more at: He Aranga Ake

<https://www.police.govt.nz/advice-services/counter-terrorism/he-aranga-ake>

Resources

Commonly used terms

Espionage and foreign interference terms

ESPIONAGE	refers to various intelligence activities involving the clandestine collection of information or materials for the purpose of gaining advantage over a rival.
FOREIGN INTERFERENCE	is an act by a foreign state, often acting through a proxy, which is intended to influence, disrupt or subvert New Zealand's national interests by deceptive, corruptive or coercive means. Normal diplomatic activity, lobbying and other genuine, overt efforts to gain influence are not considered interference. <i>Deception:</i> Often an interference actor will claim their advocacy is for personal reasons when further digging might reveal they are being paid, encouraged or coerced by representatives of a foreign state. The true objectives or intentions behind their activity will be concealed from those they are trying to influence. <i>Corruption:</i> When state-backed actors try to gain leverage over people to get political or other favours, that is a clear case of corruption. <i>Coercion:</i> It is highly coercive when state-backed activity suppresses the freedoms of individuals in New Zealand. This might include interference in someone's freedom of expression, or their ability to freely participate in New Zealand's society or political environment.
CO-OPTEEES/ PROXIES	are individuals who are not directly employed by a foreign state but undertake activity of security concern on the foreign state's behalf. This can include New Zealand based persons or persons based offshore. Often these individuals receive tasking from a foreign state; however, some proxies understand the foreign states objectives and undertake activity in support of these objectives without being directly tasked to do so.

Insider Threat definition

INSIDER	Any person who has, or previously had, authorised access to or knowledge of the organisation's resources, including people, processes, information, technology, and facilities.
INSIDER RISK	The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.
INSIDER THREAT	An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation.
INSIDER ACT	The activity, conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

Violent extremism terms

TERRORISM	Under New Zealand law, a terrorist act is defined as an ideologically, politically, or religiously motivated act intended to intimidate a population, or to unduly compel a government to do or abstain from doing any act. A terrorist act could include acts causing death or serious bodily injury, but isn't necessarily limited to this.
VIOLENT EXTREMISM	is the use or justification of violence to achieve radical political, social, or religious change. Violent extremists often target groups they see as threatening their success or survival or undermining their worldview.
<i>Identity-Motivated:</i>	Violent extremists who promote the use of violence to advance their own perceptions of identity and/or denigrate others' perceived identities.
<i>Faith-Motivated:</i>	Violent extremists who promote the use of violence to advance their own spiritual or religious objectives.
<i>Politically-Motivated:</i>	Violent extremists who promote the use of violence to achieve change to or within an existing political system.
<i>Mixed, Unstable, and Unclear:</i>	When individuals appear to hold combinations of ideologies, which can appear to reinforce or contradict each other; who transfer between ideologies; or those with ambiguous or indeterminate ideologies.

Resources Methodology

This report is based on information gathered from a variety of sources including New Zealand Government information, academic research and media reporting.

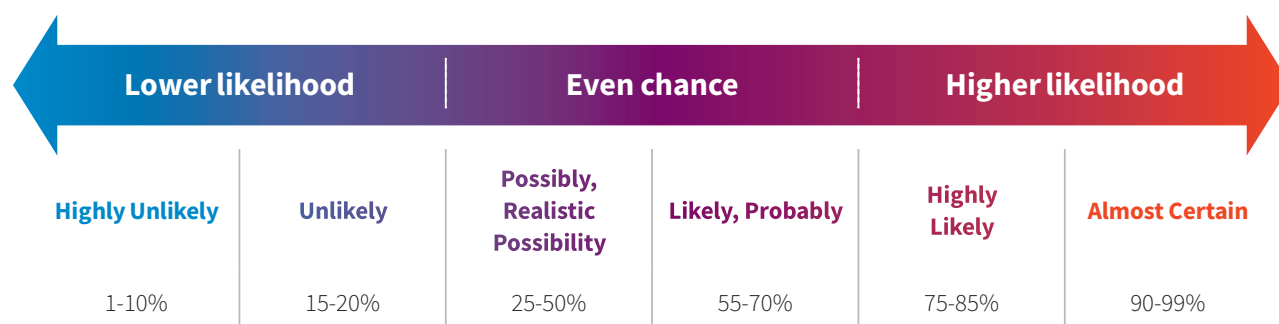
Our assessments were developed over a number of analytical sessions involving New Zealand Intelligence Community analysts and external subject matter experts.

Overall, we have medium confidence in our assessments which are based on a large body of credible and reliable sources, and our historic understanding of the New Zealand threat environment.

We acknowledge that intelligence gaps remain and alternative explanations are possible.

Probabilistic language has been used through this report. It is common practice in intelligence assessment to use probabilistic language to denote the likelihood of an assessment being true.

NZSIS's probabilistic language scale is as follows:



ACKNOWLEDGEMENTS

We would like to acknowledge the support, knowledge and feedback provided to us by our colleagues in government and external subject matter experts. It has meant we have been able to produce a much more robust assessment than would have otherwise been possible.

Resources

National security careers

You have read about the threats – help us do something about it. NZSIS is always on the lookout for Intelligence Case Officers, Analysts and Surveillance Officers to join our mission to keep New Zealand safe and secure.

Case officers

Case officers are special roles within our organisation whose job is to meet people and collect intelligence to solve some of our most complex national security challenges.

Their job involves building confidential relationships with 'human sources' from a variety of backgrounds. Case officers are responsible for assessing, recruiting, managing, and interviewing sources to gain unique insights into the intentions and activities of others. A degree of cunning is involved but our people are also highly principled and always act in line with the NZSIS's governing legislation and human rights obligations

Intelligence analysts

An analyst at the NZSIS is someone who is relentlessly curious and thinks outside the box.

Their job is to pull multiple strands of information together to solve complex intelligence puzzles and discover unknown threats.

Our analysts have a strong sense of purpose – they are driven to make a difference for New Zealand by providing leading-edge insights.

Surveillance officers

Are you a people watcher with strong attention to detail and the ability to pick up even the most subtle changes in behaviour? Being an NZSIS surveillance officer might be the job for you.

Joining our supportive surveillance teams gives you a change from the boring 9-5 office role and into a role with unpredictability, variety and travel across New Zealand.

And much more

Like any other organisation, we have a wide range of opportunities including business support, IT, policy, HR, finance and a whole lot more. Bring your skills and experience to be part of a mission that is like no other.

Secrecy is part of all our roles at the NZSIS. These are not the kind of jobs where you talk about your work day with family and friends. Your supportive team can help you learn how to manage those tricky conversations.

Check out our recruitment site at Beyond Ordinary careers to find out more about these roles and the wide range of other positions we offer.

beyondordinary.nzic.govt.nz



Te Pā Whakamarumaru New Zealand Security Intelligence Service

Our mission is to keep New Zealand and New Zealanders safe and secure. We collect and analyse intelligence in line with the Government's priorities to provide decision makers with sound national security advice. We also provide a range of protective security services to other government agencies.

Report a national security concern →
Your information could help us protect New Zealand from threats such as foreign interference, espionage and terrorism.

Ā mātau mahi Our work

We are New Zealand's domestic security intelligence agency and lead organisation for Human Intelligence (HUMINT).

FIND OUT MORE

Ngā pitopito kōrero News and speeches

We publish our media releases and speeches from our Director-General.

FIND OUT MORE

Kia mataara ki ngā tohu Know the signs

Read our guide for identifying signs of violent extremism.

FIND OUT MORE

Stay informed and report your concerns.

When it comes to protecting New Zealand's national security, everyone has a role to play.

The purpose of this report is to raise national security awareness and hopefully spark further conversations among organisations and communities on how we can work together to manage risk.

National security awareness is built on the following four principles:

1. KNOW THE THREATS

This and previous reports are all available on the NZSIS website. Our website also has a range of information about the work we do to keep New Zealand safe and secure.

Stay up-to-date by subscribing to our community newsletter at www.nzsis.govt.nz/community.

2. KNOW THE SIGNS

New Zealanders can help us by reporting behaviours and activities you find concerning.

Understand what concerns us by reading and sharing Know the Signs, the indicators of violent extremism. Common activities associated with foreign interference and espionage activities are described in this report.

3. READ THE RESOURCES

NZSIS's protective security website is full of best practice information on how to protect an organisation's people, information and assets. See www.protectivesecurity.govt.nz.

See also the Police's Crowded Places resources and the Community Resilience to Foreign Interference Hub produced by the Ministry for Ethnic Communities.

4. REPORT YOUR CONCERNS

The NZSIS relies on you as a member of the public to let us know when you notice behaviours and activities that you find concerning. Your information could help us protect New Zealand from threats of violent extremism, terrorism, foreign interference, espionage and insider threat.

There is no wrong door for reporting national security threats.

IN AN EMERGENCY CALL 1-1-1

Use either the NZSIS online form at www.nzsis.govt.nz or contact Police at www.police.govt.nz/use-105 or through their non-emergency phone number 105. Whichever channel you choose, we will make sure your information reaches the right place.



Te Pā Whakamarumarū
New Zealand Security
Intelligence Service