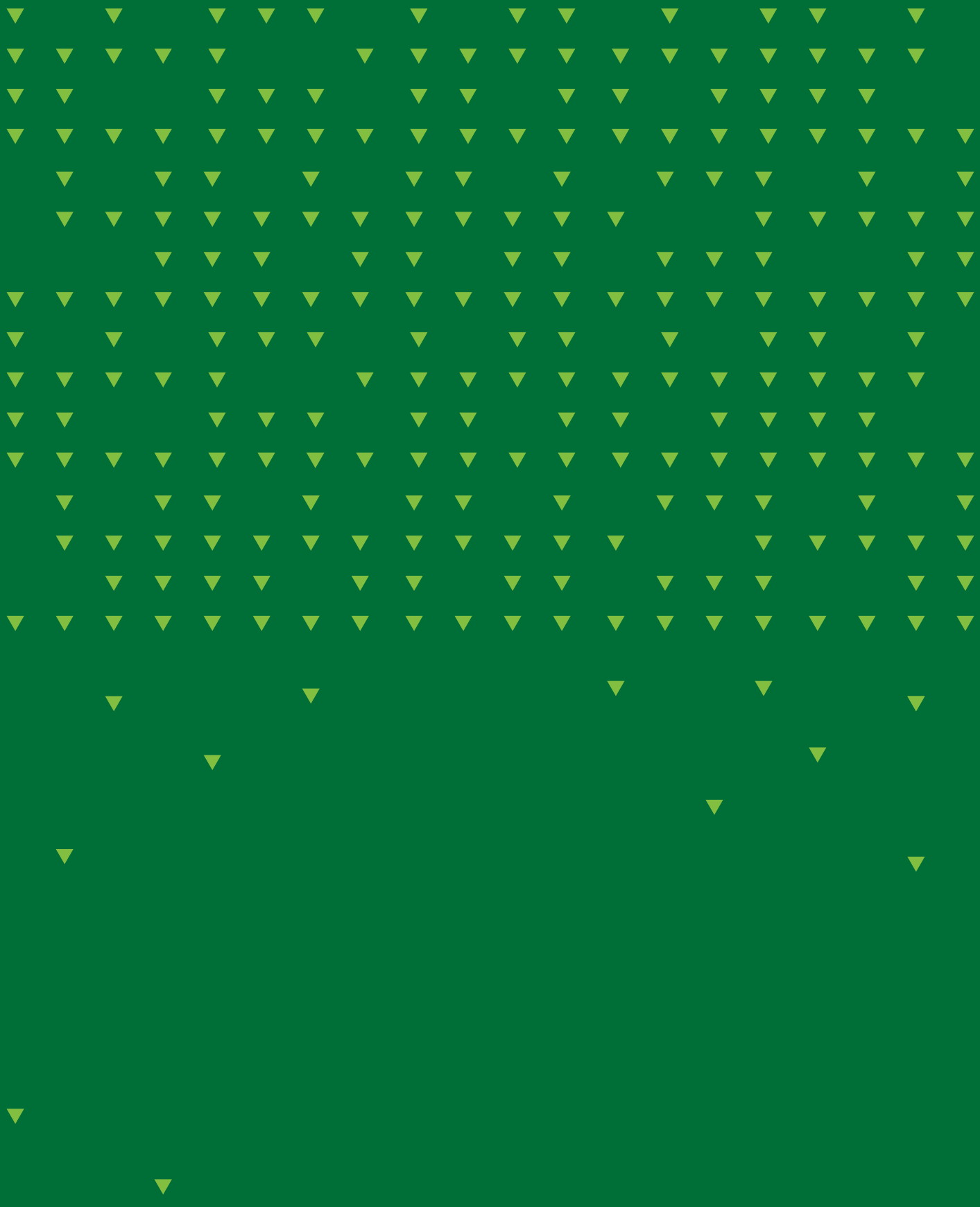
New Zealand's Security Threat Environment

2025

An assessment by the New Zealand Security Intelligence Service

Te Pā Whakamarumaru
New Zealand Security Intelligence Service



Contents

New Zealand is facing the most challenging national security environment of recent times

The New Zealand Security Intelligence Service (NZSIS) has noted further deterioration in the threat environment since last year's report, largely driven by less stable relationships between states and increasing levels of polarisation and grievance.

Tucked away in the South Pacific, New Zealand may seem like a long way from global security hotspots, but the reality is much different. The make-up of our society, our economic connectedness, our international relationships and location in an increasingly contested region means New Zealand is impacted by the competition between states for power, influence and strategic advantage.

At the same time, the murky corners of the online world can be reached in a single click. A media feed filled with polarisation and grievance awaits anyone who is vulnerable to being led astray, or who is looking for fuel for their violent ideology.

The security environment is challenging because the nature of the threats we face is so varied and complex. Understanding why someone may be motivated to target New Zealand and those who live here is difficult to untangle and the ways this country may be targeted change rapidly.

Threats cannot always be eliminated, but it is possible to manage the risk from potential harms and vulnerabilities. This third annual threat assessment is about raising awareness so that government institutions, organisations and communities can have clear-eyed conversations on how to avoid or reduce harm.

It is important to understand the nature of other national security threats too. For example, to stay on top of trends in the cyber threat environment, it's highly recommended to read the National Cyber Security Centre's annual threat report.

NCSC.GOVT.NZ

CYBER THREAT REPORT

How to read this assessment

The NZSIS is responsible for detecting, investigating, deterring and disrupting national security threats. Our current key priorities include violent extremism, terrorism, foreign interference and espionage. As such, these are the threats covered in this assessment.

This report is based on NZSIS intelligence insights gathered in New Zealand and from a local perspective. It should not be considered a Government policy document.

The job of the NZSIS is more than just reporting on the threats we face. We want to work with organisations and communities to share our knowledge about how some of these harms can be avoided or managed.

Best practice security advice can be found within the foreign interference, espionage and insider sections. This is designed to help frame your thinking about security and give you more confidence to identify and manage these risks.

Real life case studies are included to demonstrate a snapshot of how these threats manifest in New Zealand. These represent just a small proportion of the kinds of activity being observed.

Read previous NZSIS threat assessments at www.nzsis.govt.nz/threat-assessment.

You may not see yourself, your organisation or your community impacted by the threats described in this report, but it is still valuable to discuss potential harms so you can work together to manage risk.

Finally, the NZSIS's analysis is always enhanced by information received from members of the public. If you see or become aware of any concerning behaviour or activities related to violent extremism, terrorism, foreign interference or espionage then we strongly encourage you to let us know.

KEY ASSESSMENTS 2025

The NZSIS makes six key assessments about New Zealand's threat environment in 2025:

- The most plausible violent extremist attack scenario in New Zealand remains a lone actor who has radicalised online and prepares for violence without any intelligence forewarning. Any attacker is most likely to use easily accessible weapons.
- Grievances and polarising issues in the online information space are almost certainly driving support for a range of violent extremist ideologies within New Zealand. No one ideology currently stands out as presenting a greater threat.
- Young and vulnerable people in New Zealand are particularly at risk of radicalisation, especially while online.
- Foreign interference activities continue in New Zealand with several states responsible. This includes activities regarded as transnational repression that often target diaspora communities.
- It is almost certain there is undetected espionage activity that is harming New Zealand's national interests. The NZSIS has had some success disrupting this activity, but foreign states continue to target New Zealand's critical organisations, infrastructure and technology to steal sensitive information.
- Some foreign states have attempted to exploit people inside public and private sector organisations in a deceptive, corruptive, or coercive manner, to gain influence and further their interests.

Our place in the world

New Zealand's security is closely linked to our prosperity. Both depend on our international connections and the free flow of information and trade.

Last year we said that relationships between states had become less stable and less predictable than that of the previous two decades - this downward trajectory has continued into 2025.

Established relationships and agreements are being challenged as more states look to exert power in an attempt to shape key regions in line with their own priorities.

At the same time, rising authoritarianism and increasingly polarised views across societies are making some states less interested in following established international norms.

The result of these dynamics is global instability, where states, some with vastly different ideas about human rights and sovereignty, seek to wield more influence over other states.

A disregard for established norms is encouraging some states to conduct activity that infringes on New Zealand's democratic system and values. One of the most common violations we see is states engaging in foreign interference activity against diverse communities in New Zealand.

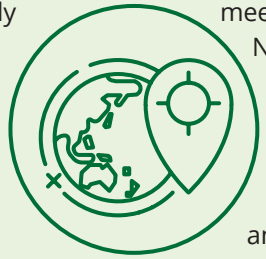
We expect foreign interference and espionage to become more frequent as global instability continues and a sense of shared values degrades.

Three global themes affecting New Zealand's security

The NZSIS has identified three security challenges happening around the world that either already have an impact in New Zealand or have potential to cause harm in the future.

1. Strategic competition

Strategic competition becomes more apparent as the global order becomes less stable. Competition between the United States, the People's Republic of China (PRC) and other countries is clearly evident and set to continue. Russia is highly likely to keep asserting its influence in Europe, both militarily and through other coercive actions, while the conflict and humanitarian crisis in the Middle East will have an enduring impact. Ongoing conflicts and tensions in Asia and Africa contribute to the instability.



Competition between powers is about economic, technological and military advantage, but it is also about disrupting policies or narratives perceived to be challenging a state's national interests. Some states, including China, Russia and Iran, are willing to engage in covert or deceptive activity in order to influence discussions and decisions, or gain access to technology and information that can help them meet these goals. As we explain in this report, New Zealand has been targeted by some of these activities.

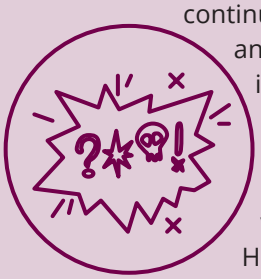
The Indo-Pacific is a focal point for geo-strategic competition between major powers. The PRC is a particularly assertive and powerful actor in the region and will look at ways it can extend and embed its influence across the region. It has demonstrated both a willingness and capability to undertake intelligence activity that targets New Zealand's national interests.

2. Polarising and violent rhetoric

Our public spaces, both online and in the physical world, are becoming increasingly polarised. At the extreme edges, well outside of what would be considered normal social and political discourse, there is a notable degree of misplaced agitation and blame for perceived societal ills. Much of this rhetoric exists solely online, and its spread is aided by algorithms that push controversial content because it generates the most engagement. Often the targets of the agitation are New Zealand's diverse communities.

There are foreign states that seek to make their own contribution with inflammatory rhetoric that can include false or misleading information. Their aim could be to distract populations or to damage social cohesion by exacerbating tensions between social, ethnic, or political groups.

NZSIS has not seen any sophisticated state-backed information operations directly targeting New Zealand. However, many New Zealanders have almost certainly consumed foreign state manipulated information when active online, even if they are not the target audience of that information.



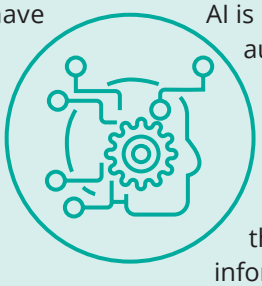
Some offshore violent extremist groups are continuing to use online spaces for recruitment and radicalisation, and are being deliberate in their targeting of young people, including in New Zealand. These groups take advantage of social divisions and offshore conflicts or crises to push violent rhetoric and justify violence. However, some individuals also self-radicalise online and the polarised nature of online spaces almost certainly increases the risks to vulnerable New Zealanders falling down radicalisation pathways.

Violent extremist propaganda has included a range of ideologies from Islamic State (IS) inspired to white-identity motivated. It is often spread without the direct involvement of violent extremist groups.

3. Technology

New Zealand has plenty to gain from advances in technology. Homegrown innovations are a force for good and should be celebrated. The NZSIS's role is not to hinder this innovation, but to raise awareness of the impact technology can have on our national security and show how it can be protected.

The rapid development and evolution of technology has played a significant role in the nature of the threats facing New Zealand over many years. From the rise of artificial intelligence (AI) to the development of emerging technologies such as quantum computing, technology has both driven the intent of threat actors to target New Zealand and shaped the kinds of threat activity we see.



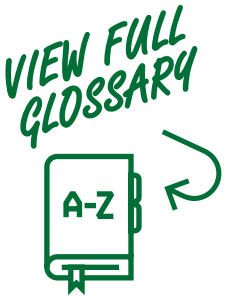
Recent advances in AI have had a particularly outsized impact on our threat environment. The use of AI to facilitate violent extremism and state-sponsored interference activities is increasing. AI is making harmful propaganda appear more authentic and allows it to be spread at scale and speed.

The ease of access to AI will be assisting violent extremists to research and plan attacks and is reducing barriers that previously made it difficult to access information about more advanced capabilities or weapons.

Some foreign intelligence actors will be using AI in their information operations, their intelligence gathering activities and to generate intelligence from open-source information or datasets.

New Zealand's violent extremism environment

Violent extremists in New Zealand are predominantly drawn to their dangerous ideology through a gateway of social, economic or political grievances.



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.

No one pathway to violence is the same, but most radicalisation is happening online. People seek to validate their grievances through their online activities. The way information is shared in New Zealand is permissible enough that it is relatively easy for someone to find violent extremist content that matches their grievance, as well as sites or forums where violence is promoted as a solution or as a way to advance their cause.

As with previous NZSIS reports, we continue to see our young and more vulnerable people as being particularly at risk of becoming radicalised to a violent extremist ideology.

NZSIS analysts look closely at how overseas events impact our threat environment.

Global events have less of a direct impact in New Zealand than elsewhere, but access to the violent extremist narratives that emerge from these situations is only a click away. One example NZSIS has observed is in how the global resurgence of the Islamic State's propaganda and attacks resonates within small pockets of New Zealand's violent extremist environment.

There remains a roughly even spread of violent extremist ideologies present among the individuals who come to our attention, including identity-motivated and faith-motivated violent extremism, as well as people who have mixed, unstable or unclear ideologies.

This section will focus less on specific ideological motivations and more on the activities we see associated with online radicalisation, as well as some of the factors that can make certain individuals vulnerable to being attracted to a violent extremist ideology.

LIKELIHOOD OF A VIOLENT EXTREMIST ATTACK

At the time of writing, a violent extremist attack is assessed as being a realistic possibility in New Zealand. Realistic possibility explains the likelihood there are violent extremists in New Zealand with the credible intent and capability to undertake an act of ideologically motivated violence. While this has been our assessment since 2022, the global violent extremism environment, which New Zealand is part of, has deteriorated in many respects over the past year.

The most likely attack scenario in New Zealand is someone who acts alone, who has radicalised online, who has prepared for violence without anyone knowing and carries out their attack using basic weapons such as a knife or vehicle.

Only a very small proportion of people expressing violent extremist views online will actually attempt to carry out an attack in the real world.

The current National Terrorism Threat Level and what that means is available on the NZSIS website.

ONLINE RADICALISATION

Ease of access to violent extremist content online is a key contributor to the radicalisation of individuals who come to the attention of the NZSIS.

Exposure to extreme rhetoric has become commonplace in some people's online experience, and they may become desensitised to what they see. Enough violent extremist content is readily available that for some people radicalisation is far too easy. This is particularly the case when a person already holds a radical or grievance-based view.

Individuals who hold mixed, unstable or unclear ideologies are especially vulnerable to being radicalised online. The NZSIS has identified a number of people who appear to explore a range of violent extremist beliefs online and adopt certain aspects to suit their grievance.

As well as being easy to find, hateful and violent content is also frequently shared in closed or anonymous online networks. These networks host groups that are contributing to the radicalisation of individuals both in New Zealand and around the world.

Inside these groups, it is not common for members to know each other's identities. This practice is encouraged among the membership. It means members can anonymously or securely share content and opinions they may otherwise keep to themselves. When there's low risk of attribution, members feel free to share even more extreme content, which can further entrench radicalisation among other young or vulnerable individuals participating in the group.

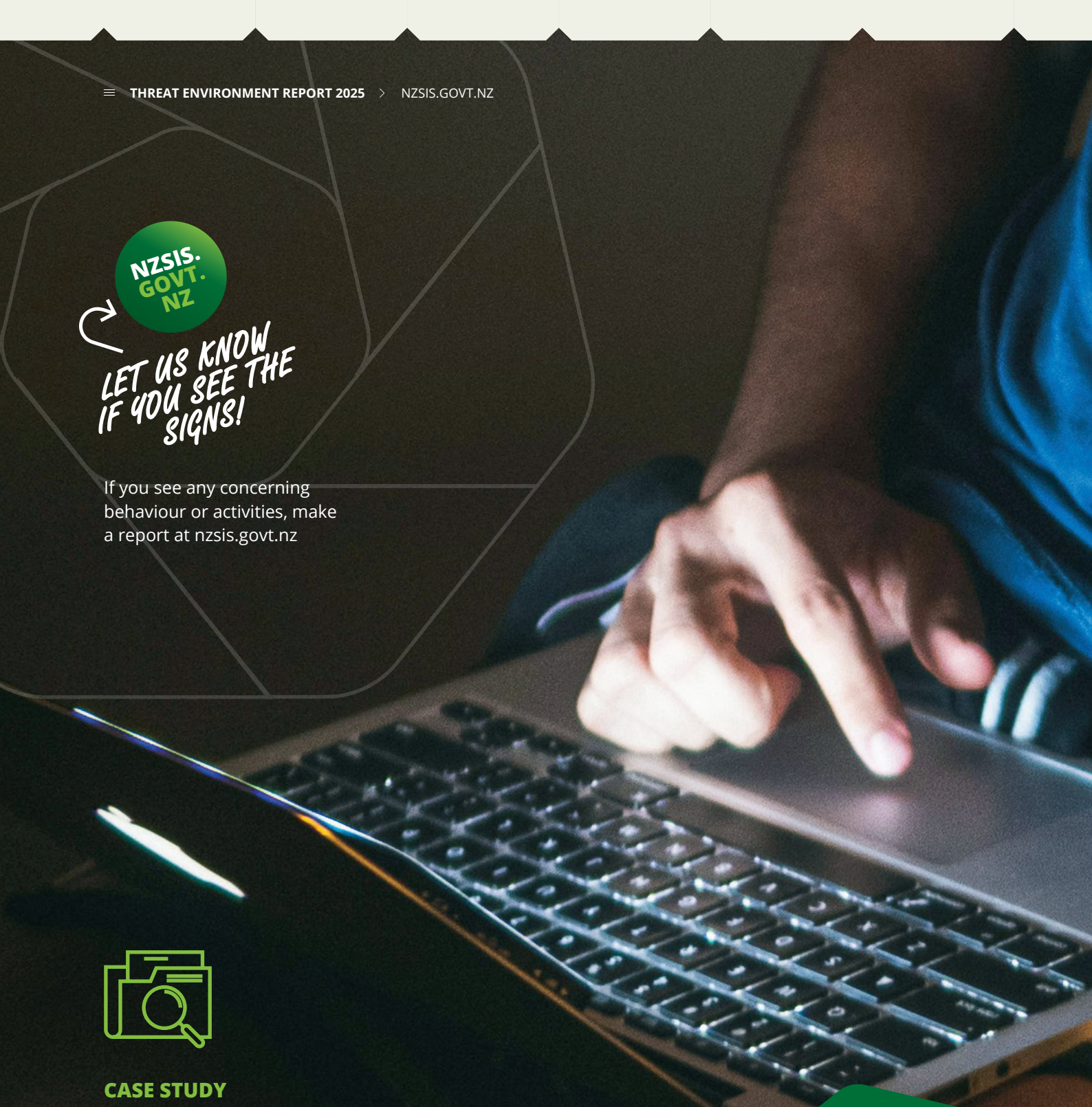
Hiding behind a cloak of anonymity is often how people separate their online and real world lives. This makes it difficult for the NZSIS to determine whether someone's anonymous comments in support of violent extremism indicate actual intent and capability to carry out an attack. People will have different motivations for being anonymous. Some may be trying to hide their true intentions, others will be protecting their privacy and have no intention of mobilising to violence, and sometimes it is simply the default setting on the online platform they are using.

Even if people confine their support for violent extremism to the online environment, it can still be harmful if the behaviour involves promoting, creating or disseminating violent extremist content.

NZSIS.GOVT.NZ

LET US KNOW IF YOU SEE THE SIGNS!

If you see any concerning behaviour or activities, make a report at nzsis.govt.nz



CASE STUDY

The NZSIS has been investigating an individual over the past year who almost certainly developed support for a faith-motivated violent extremist ideology through their consumption of online material.

The person consumed Islamic State (IS) propaganda that was designed to 'prove' the group's religious credentials. They then sought additional religious guidance that reinforced IS messaging, and which led to their support for the violent extremist ideology.

This shows behaviour often seen in violent extremists where they seek information that justifies their worldview. We continue to investigate the risk the person poses to the safety of New Zealanders.

Know the signs
Indicators

- Mindset and ideology
- Research and planning

VULNERABILITIES TO VIOLENT EXTREMISM

People with certain vulnerabilities are increasingly common in New Zealand's violent extremist environment.

Common factors seen among violent extremists in New Zealand include unstable socio-economic status, poor mental health, developmental trauma and low emotional maturity.

These are vulnerabilities which increase the likelihood of an individual taking part in anti-social behaviours, such as criminal offending, drug dependence, and violent extremism.

The vast majority of people with these vulnerabilities do not become violent extremists, but these have been common features in recent investigations, particularly those involving young people.

The challenge for security agencies is assessing the risk these people may pose to national security. Analysts work hard to understand whether someone genuinely plans to carry out real world actions based on the violent claims they make.

When a history of ill mental health is present, the challenge is more complex. Someone may express a desire to harm others, and even use extreme or ideological buzzwords, but it is not easy to determine if that is actually in support of a violent extremist ideology. Just as the presence of an ideology alone does not indicate someone will resort to violence, the presence of a mental health disorder doesn't necessarily increase someone's capacity to cause harm. Every case needs to be assessed on its merits to understand the level of risk posed.

Similarly, young people are not predisposed to violent extremism, but certain vulnerabilities that can make them more at risk can exist at a young age. Teenagers are increasingly coming to the attention of security services around the world. This trend will almost certainly continue, particularly given how exposed young people are to the online world, and the vast amounts of harmful content readily available.

The activity of young people online cannot always be supervised, and in many cases they will become exposed to violent extremist material without anyone close to them knowing. Unfettered access to the internet, along with a lack of anyone disrupting or asking questions about their activity, can make the pathways to violence incredibly short.

What might have previously been considered societal risks associated with internet safety, now have the potential to pose an ongoing risk to New Zealand's national security.

NZSIS.GOVT.NZ

LET US KNOW IF YOU SEE THE SIGNS!

If you see any concerning behaviour or activities, make a report at nzsis.govt.nz

CASE STUDY

The NZSIS has seen two recent examples of potential support for white identity-motivated violent extremism where pre-existing vulnerabilities have contributed to a radicalisation pathway.

One person had experienced mental health disorders and substance abuse issues from a young age, while the other had convictions for violent offences along with a history of depression and drug and alcohol abuse.

Their respective histories almost certainly contributed to their interest in violence, but determining whether their ideological motivations were genuine was less straightforward given their backgrounds.

Both individuals have previously demonstrated the capability to conduct an attack. The NZSIS is working with other agencies to understand whether there is intent to carry out ideologically-motivated violence, and to manage the risk posed by these individuals.

Know the signs
Indicators

- Gathering knowledge or resources
- Unusual changes in behaviour

DISCOVERING UNKNOWN VIOLENT EXTREMIST THREATS

The NZSIS has a responsibility to devote resources to detecting violent extremist threats that have not yet to come to light.

Our discovery function is about identifying actual or potential threats in the violent extremism environment. This work is driven by a strong strategic understanding about the nature of the threats New Zealand faces and exploring where there are any knowledge gaps.

An example of analytical work in this area is efforts to identify New Zealanders attempting to access violent extremist content online. Analysts use a range of methods to determine whether any of these people adhere to a violent extremist ideology and the risk they pose to New Zealand's national security.

Importance of knowing the signs

Key to NZSIS discovery efforts is information we receive from members of the public.

NZSIS's discovery and investigative efforts work to identify signs of radicalisation. However, it is a mistake to assume that intelligence and law enforcement agencies will automatically pick up on signs of radicalisation to violence. The reality is that New Zealanders are more likely to see concerning behaviour or activities before we do. This fact is reflected in our key assessment that a terrorist attack is most likely to happen in New Zealand without any intelligence warning in advance.

The 'Know the signs' guidance published in 2022 remains the most useful way for New Zealanders to help us detect early indicators of violent extremism.

The guide focuses on specific behaviours and activities that are observable in the real world. Each indicator has been seen in counter-terrorism investigations in New Zealand since 2006.

Understanding the behaviours and activities associated with violent extremism is crucial. Violent extremists in New Zealand have come from a broad cross-section of New Zealand society. That is why we ask to look for behaviours rather than a particular type of person.

Concerning behaviours associated with online radicalisation

Violent extremists will often be careful to avoid detection and maintain their online anonymity. However, from time-to-time certain behaviours will become more observable to others.

The following are specific indicators from 'Know the signs' seen in recent investigations that provide insight into how online behaviours can present themselves in the real world.

Mindset and ideology

- Identifies with a violent extremist cause
- Supports the use of violence to further their cause

Associations and relationships

- Seeks out or engages with violent extremist groups or individuals

Research and Planning

- Shows interest in terrorist activity

Gathering knowledge, skills or resources

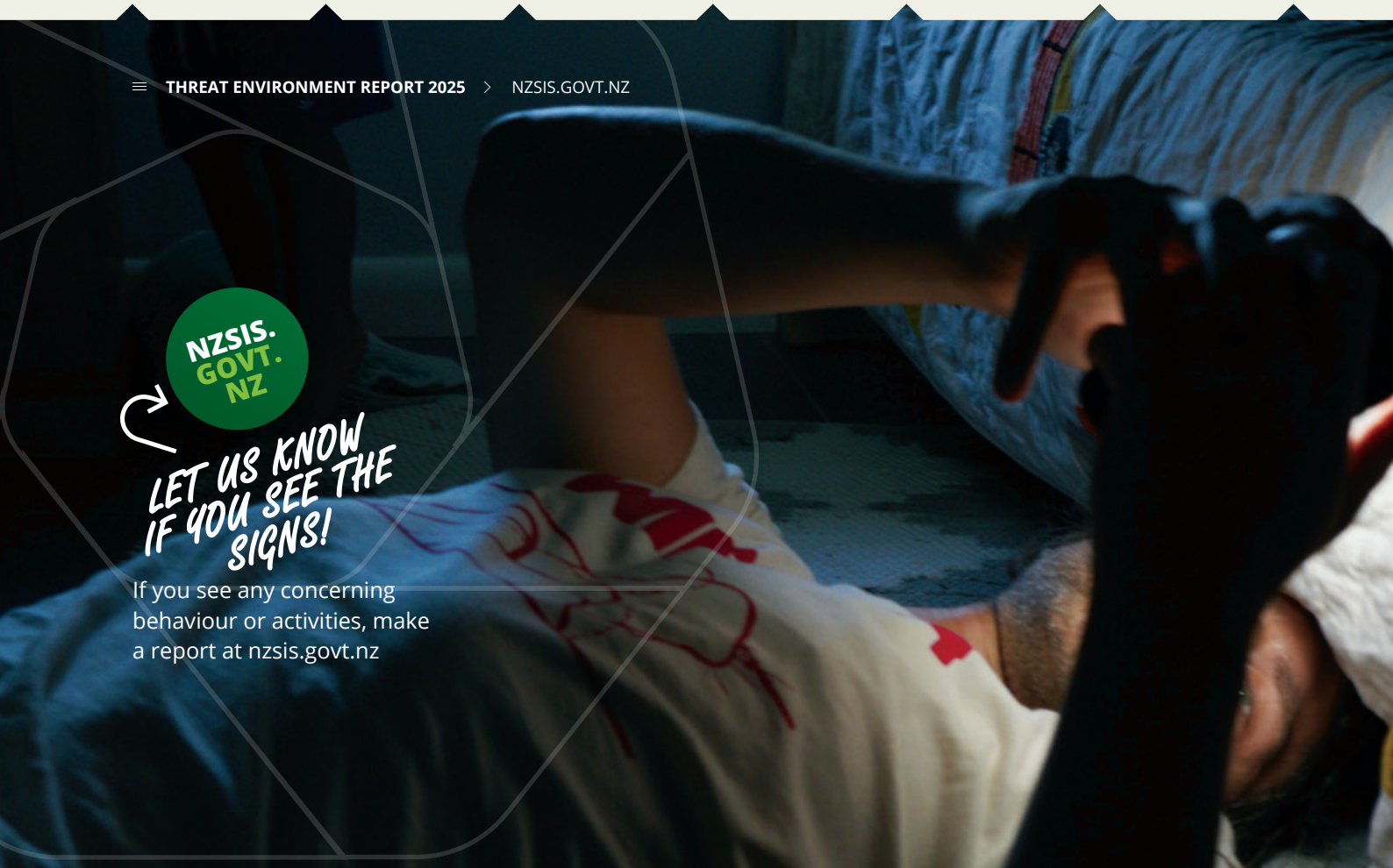
- Develops skills, experience or inside access

Security Awareness

- Displays a security awareness or concern (Note: this behaviour is concerning only when they occur alongside other activities listed in the guide.)

'Know the signs' is available digitally at *nzsis.govt.nz/know-the-signs*

NZSIS.GOVT.NZ



NZSIS.GOVT.NZ

LET US KNOW IF YOU SEE THE SIGNS!

If you see any concerning behaviour or activities, make a report at nzsis.govt.nz

CASE STUDY

NZSIS received a lead from a member of the public regarding a young person who had been displaying behaviour indicative of support for a white identity violent extremist ideology. The individual showed an interest in the Christchurch terrorist, Nazi symbols and violent content online.

NZSIS investigated to understand the extent of the individual's ideology and whether they had the intent and capability to conduct an act of violence in support of violent extremism. Working with Police, NZSIS determined the individual was unlikely to resort to violence and had significant protective factors in their life to prevent them from doing so.

The NZSIS welcomed this kind of public reporting, and was able to confidently determine the individual was unlikely to pose a risk to national security and concluded its enquiries.

Know the signs
Indicators

Mindset and ideology

New Zealand's foreign interference environment

States conduct foreign interference in New Zealand in order to achieve their strategic goals.

A range of people will be used by foreign states, either directly or implicitly, to conduct activity which aims to manipulate New Zealand's government and society to become more amenable to the foreign state's interests.

There are several states undertaking foreign interference in New Zealand. The most active remains the People's Republic of China (PRC), though it is not the only foreign state carrying out activity of concern.

The NZSIS sees two main types of foreign interference in New Zealand - political and societal. Political interference refers to acts by foreign states that are intended to influence, disrupt, or subvert New Zealand's governance, policy making, or political systems by deceptive, corruptive, or coercive means. Societal interference targets our communities and non-government sectors.

There have been numerous attempts at political interference in New Zealand in recent years. Fortunately, the vast majority have had little impact on policy making or our democratic processes, but we emphasise that the potential for significant harm through political interference activity remains. This section will focus more specifically on a form of societal interference called transnational repression, where New Zealanders may be targeted because of their ethnicity, religion, politics or sexuality.

What is Foreign Interference?

The NZSIS defines foreign interference as an act by a foreign state, often acting through a co-optee, which is intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means.

Misconceptions of foreign interference

It is important to acknowledge at the outset that these foreign states often do not consider what they are doing to be foreign interference. One reason for this is that they do not like to be called out for their behaviour. Another is that they see these activities as a continuation of their domestic policy and therefore within their sovereign authority. The NZSIS rejects any such assertions.

People living in New Zealand have the lawful right to freedom of expression and the right to participate in groups or religions without fear of reprisal. NZSIS considers it foreign interference when states seek to control, intimidate, punish or limit opportunities for people based in New Zealand. Such activity is an attack on our democratic principles and freedoms.

TRANSNATIONAL REPRESSION

The most common type of societal foreign interference that New Zealanders are likely to encounter is transnational repression (TNR).

Transnational repression is activity on behalf of a foreign state intended to suppress the rights and freedoms of groups or individuals located beyond its borders. These individuals are usually seen by the state as undermining its national security or harming its interests. TNR includes a range of methods with varying levels of severity, and is usually carried out by people co-opted to act on behalf of the foreign state.

There are several foreign states that routinely engage in TNR activity in New Zealand. They falsely believe they have the authority to extend their influence to their diaspora communities. They expect their diaspora should remain politically loyal even when they reside in another country.

Who is a target of transnational repression?

Foreign states will act against individuals, groups or communities they view as 'dissidents'. This might be any political movement or group seen as a challenge to a state's legitimacy or power.

The NZSIS has noted TNR activity in New Zealand targeting certain religions, some ethnicities, Rainbow communities and pro-democracy movements.

Though TNR is usually directed against a foreign state's diaspora community, it can also be directed against those with no ties to the foreign state. Often this is towards individuals or groups who are vocal critics of the foreign state or advocates for a targeted diaspora community.

Foreign states regularly flag legitimate violent extremist concerns with us. Such alerts are testament to our collaborative international relationships and contribute to our national security. Some states, however, have accused New Zealand-based groups or individuals of being extremists or even terrorists when they are not.

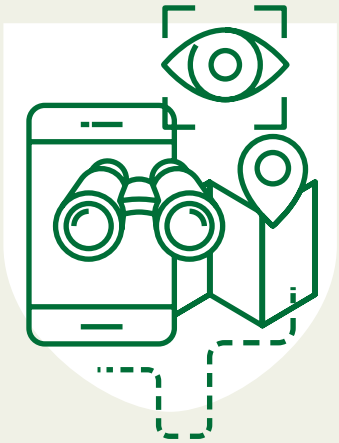
The NZSIS is extremely cautious about this deliberate labelling tactic, as it is used to stigmatise particular groups and to justify repressive activity against them.

What does transnational repression look like?

Foreign states typically use a co-optee to carry out TNR with either direct or implicit instructions. This often begins with the co-optee being asked to collect information about someone living in New Zealand and sharing this with the foreign state.

The NZSIS uses this term to refer to a group of people with cultural, ancestral or familial ties to a particular foreign state. Being a member of a diaspora community does not take away from someone's identity as a New Zealander. Some foreign states view this differently. They want diaspora members to be primarily loyal to the foreign state regardless of their legal status in New Zealand.

Activities associated with transnational repression



01

Surveillance

NZSIS is aware of co-optees undertaking both online and physical surveillance activity on behalf of foreign states here in New Zealand.

Often this includes activity such as monitoring social media, photographing individuals at events or protests, or instructing other community members to collect information. The surveillance is concerning in itself, but even more so is how that information may be used by the foreign state to undertake other coercive action if the individual ever travels to that country, or against their family members living in the foreign state.

CASE STUDY

Co-optees are often asked to collect information about New Zealanders. The co-optees are often New Zealanders themselves who have in many cases decided to support the interests of a foreign state.

As an example in 2024, a foreign state tasked a co-optee with collecting information about a New Zealand based person who had applied for refugee status in New Zealand. It is almost certain that the foreign state is interested in collecting information on this person because they are a member of a rainbow community.

02

Harassment

Foreign states use a range of tactics to intimidate and harass so-called dissidents. This can include taking pictures of them in plain sight, online harassment or blacklisting their businesses. A foreign state may also intimidate family members who live in that country.

NZSIS often receives reports of foreign officials directly approaching or using co-optees to request that certain individuals or groups be prevented from participating in public events. Sometimes donations or other financial incentives are used to influence decision-making.

CASE STUDY

In late 2024, a foreign official approached a New Zealand based co-optee and requested their assistance in preventing a 'dissident' group from participating in a community event hosted by a local council. The official instructed the co-optee to obscure the foreign state's involvement

CASE STUDY

In 2024, a co-optee of a foreign state pressured a New Zealander to provide them with the personal details of several members of a diaspora community. These community members are part of a political movement that the foreign state routinely monitors. Details about family members still living in the foreign country were also sought.

03
Administrative action

NZSIS has received reports of New Zealand-based individuals having travel documentation withheld or revoked by foreign states due to their participation in political or religious activity in New Zealand. Foreign states do this with the specific intention of deterring these individuals from participating in these activities or applying a punitive cost to the activity. It is a way that these states try to exert control over individuals outside of their borders.

States have the authority to decline or revoke official documentation, but when this is done in response to lawful activity undertaken in New Zealand it undermines the rights and freedoms that New Zealand offers.

Using administrative action to control the behaviour of diaspora populations in New Zealand can have a significant impact on the individuals affected when they have family or financial interests in the foreign country.

There is also a negative impact for New Zealand if parts of our society are afraid to participate in legitimate community or political activity due to fear of reprisals from a foreign state.

CASE STUDY

A foreign official presence is almost certainly monitoring several New Zealand-based people due to their participation in a political movement. If any of these individuals seek to travel to that foreign state, it is almost certain they will be denied travel documentation.

04
Coerced or forced repatriation

Repressive activities can become more severe if individuals are coerced or forced to travel to a foreign country. Coerced or forced repatriation often involves a foreign state laying charges against an individual and then sending undeclared officials offshore to pressure the individual to return. This pressure can involve a range of activities. Some foreign states harass or threaten individuals or their families, or they may freeze assets held in the foreign country until the individual returns. NZSIS is aware of foreign intelligence officers who have travelled here and have likely supported coercive repatriation. It is possible these efforts were directed against people living in New Zealand.

Returning to face legitimate charges where proper extradition processes have been followed is not considered TNR.

05
Physical violence

Some foreign states are known to use violence to suppress, or in extreme cases overseas, kill high-profile individuals. Foreign states will sometimes hire organised crime syndicates to conduct this activity on their behalf. This allows them to use deniability if the activity is prevented or uncovered. However, there have been states that have used intelligence officers to eliminate perceived dissidents.

This kind of activity is far less common than other forms of TNR and rarely happens in Western countries. NZSIS assesses it is highly unlikely a foreign state has ordered the killing of New Zealand-based person.

FOREIGN INTERFERENCE TARGETING NEW ZEALAND SOCIETY

Foreign states, or those acting on their behalf, routinely engage with New Zealand's communities and organisations that sit outside of central government.

Most of this engagement is harmless and provides a range of commercial and cultural benefits for New Zealand. However, NZSIS is aware of foreign interference actors seeking to manipulate certain entities in support of their objectives. Attempting to build influence is acceptable, but this activity becomes foreign interference when there is a deceptive, corruptive or coercive element involved.

Opportunities and potential relationships may not always be what they seem. This section is about raising awareness of potential risks rather than discouraging engagement.

Communities and organisations that NZSIS has observed being targeted by sophisticated foreign interference actors include local government, cultural and religious groups, academic institutions, Māori organisations and private sector businesses.

Foreign interference actors take a long-term approach to their work. Relationships and connections will usually begin in benign or seemingly legitimate ways. The dial will slowly shift over time. Skilled actors are tenacious and build pressure gradually over many years and sometimes decades. The long-term nature of these relationships can convince targets they are built on a foundation of trust or friendship while true intentions remain purposely obfuscated.

The activities described in this section can be difficult to spot, as the foreign state's involvement will often be well concealed. It can also be difficult to truly understand the harm being caused as individual interactions will appear to have little impact, but there can be effects that mount over time unless risks are managed at an early stage.

PROTECTIVE SECURITY ADVICE

There are a range of steps you can take to manage the risk of foreign interference.

If you feel someone's interest in you is suspicious, ongoing, unusual, or persistent compared to your regular interactions, attempt to remove yourself from the conversation and report it to the NZSIS.

It is also useful to try to do some online research on individuals you are unsure about and take a trusted friend with you when meeting someone new. Also consider if it is appropriate to accept any gifts you might receive.

If you notice any of the activities described in this report please let the NZSIS know by filling out our online form.

For more info, visit: *protectivesecurity.govt.nz/foreign-interference-protection*

PROTECTIVE SECURITY. GOVT.NZ

CASE STUDY

The NZSIS has seen influential New Zealanders make decisions based on misleading information provided by a co-optee they considered a trusted advisor. In one recent case, an influential decision maker had no idea that a person they trusted was a co-optee of a foreign state. The co-optee was receiving instructions from that state on what information should be provided to the decision maker.

CASE STUDY

Within the last 12 months, known foreign interference actors communicated their priorities to a range of local co-optees.

The co-optees that received these instructions were almost certainly from across New Zealand and are involved in a range of businesses, media, and civil society organisations.

It is highly likely they were encouraged to continue engaging with New Zealanders in leadership positions and that support was also offered to help the co-optees conceal the foreign state's involvement.

CASE STUDY

A New Zealand government official was looking to arrange an opportunity to share important security advice with a community but was discouraged by a community leader who has undertaken activity in support of a foreign state's objectives. This community leader, who was also a government employee, claimed that information would not be well received. Even though the intent of the security advice was to raise awareness of risks, the gatekeeper likely thought it was against the interests of a particular foreign state.

Front organisations and co-optees

Last year's threat environment report warned of deceptive front organisations conducting foreign interference and that activity continues. These groups recognise the role certain organisations and communities play in shaping New Zealand's social and political environment and seek to co-opt this influence for their own purposes.

The People's Republic of China's United Front Work Department (UFWD) is an example of an organisation that engages in foreign interference activities. The UFWD aims to build influence with key individuals and organisations outside of mainland China, including in New Zealand. The UFWD's goal is to pursue the interests of the PRC government around the world. It is important to acknowledge that not all UFWD activity is foreign interference and some engagements can have benefits for New Zealand organisations. However, its activities are regularly deceptive, coercive and corruptive and come with risks for New Zealand organisations.

The use of co-optees has been an ongoing feature of foreign interference activity for many years. There are a number of individuals in New Zealand who carry out this activity in support of the objectives of foreign states. These co-optees facilitate activity, collect information, deliver messaging, and in some cases aid in the selection of targets for other intelligence activity. Their links to the foreign state and the instructions they receive are often concealed or not disclosed to their targets.

Targeting of community leaders

NZSIS analysts see foreign interference actors taking control of community organisations by co-opting or replacing leaders. This activity often involves these actors taking control by either following normal process or through some form of manipulation. Once in charge, the co-optee sidelines those deemed to be a challenge to the foreign state's agenda.

Some foreign states have targeted their diaspora's community groups in New Zealand in this way. This has resulted in certain community voices being excluded and the co-opted leaders becoming unrepresentative spokespeople at official events or when engaging with government officials.

Gatekeeping

New Zealand government officials are sometimes restricted from meeting or talking to certain members of a foreign state's diaspora. NZSIS analysts have seen co-opted leaders place themselves as a go-between to control the flow of information to and from that community.

These people will present themselves to elected representatives or government officials as a community leader but then present opinions that are favourable to a foreign state rather than necessarily reflective of the community's views.

They may also claim they can rally the community in support or opposition to a particular policy, giving a misleading impression of the community's stance. In other cases, we have seen gatekeepers prevent information or advice from being shared with the community they claim to represent.

Exploitation of travel

Foreign interference actors have arranged travel opportunities for representatives of New Zealand organisations to build long-term influence. Often this is done to facilitate further introductions with other foreign interference actors and to build stronger relationships between them. We have seen foreign interference actors use their co-optee networks to make these travel opportunities happen while concealing the foreign interference actors' involvement.

These trips will commonly include business deals, gift giving or photo opportunities with foreign officials and are used by foreign states to promote a perception of close ties and political support from influential New Zealanders. This can have an alienating effect on repressed communities back in New Zealand experiencing transnational repression activity from the foreign state.

CASE STUDY

Local councils in New Zealand may be unaware how sister city relationships can be exploited for foreign interference activity.

Sister city relationships can generate social and cultural opportunities for local councils, however, they are also a way that foreign interference actors have gained access to New Zealand officials under the guise of legitimate engagement.

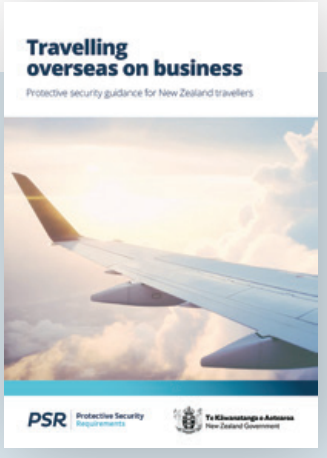
Foreign interference actors have frequently used these relationships with New Zealand councils deceptively for a range of influence building activities including travel, delegation visits and business opportunities.

PROTECTIVE SECURITY ADVICE

When travelling overseas for work:

- Be careful about how and when you use or share sensitive information.
- Be cautious about giving your personal contact details to people you meet. Consider providing your official or business contact details instead.
- Maintain physical control of documents and electronic devices at all times.
- Don't leave electronic devices, or sensitive information, unattended in hotel rooms – including in safes.
- Don't charge your electronic devices with a charger you do not own or via USB charging outlets.
- Set complex and unique passwords for each device.
- Disable wireless and Bluetooth functions when not in use.
- Avoid using public Wi-Fi – including hotels.
- Be wary of drinking alcohol and reducing your inhibitions.

For more info, visit: *protectivesecurity.govt.nz/overseas-travel*



PROTECTIVE SECURITY. GOVT.NZ

Exploitation of delegations

Over the past 18 months, there has been a noticeable increase in foreign interference actors visiting New Zealand. These foreign interference actors are highly likely to have been tasked with building relationships with specific parts of New Zealand society and are willing to engage in deceptive behaviour to meet the expectations of their organisations.

Often these foreign delegations will seek an invitation from a New Zealand organisation to host them and then use the visit as a relationship building exercise. On the surface, few organisations will sense any issue but many will not know the delegation's link to foreign interference entities. Members of these delegations will conceal these links so our communities and organisations are unable to assess the risk involved in the engagement.

NZSIS encourages strong security practices when hosting foreign delegations.

PROTECTIVE SECURITY ADVICE

When planning to host a visiting delegation:

Before the visit

- Consider the opportunities and risks associated with hosting a foreign delegation.
- Conduct due diligence on the visiting organisation and its key staff.

During the visit

- Ensure that all visitors are clearly identified and accounted for throughout the visit.
- Don't agree to anything that is not in your interests.

After the visit

- Check for anything unusual and empower your people to report concerns.

For more advice, visit: *protectivesecurity.govt.nz/inwards-visits*

PROTECTIVE SECURITY. GOVT.NZ

Exploitation of business opportunities

There are foreign states that seek to encourage business relationships that provide access to resources, intellectual property (IP) or critical infrastructure in New Zealand. Some of these relationships may begin as legitimate business relationships, but because of commercial or security laws in the other country, the foreign state can use the relationship for its own means. This can include as leverage to engage in economic coercion, to access information held by the company including IP, or as a way to further establish a relationship with a target. The New Zealand business may often be unaware of a foreign state's involvement in these opportunities.

Typically, a delegation will be sent to New Zealand or there will be an invitation to visit the foreign country, where requests are made to sign agreements or other offers are presented. Deals will often be presented to the New Zealand businesses at short notice and without the opportunity to conduct due diligence or receive legal advice.

Offers of travel, visiting delegations and business opportunities are prime examples of activities that do not pose harm in isolation, but foreign state actors are prepared to play a long-term game. They will wait to apply pressure when the time is right to take advantage of personal, political and economic leverage built over time.

PROTECTIVE SECURITY ADVICE

Before building trusted business relationships or collaborations with overseas organisations:

- Evaluate the business opportunity against any associated risks.
- Consider any legal or ethical issues with the opportunity or the partner involved.
- Review your intellectual property management systems.

PROTECTIVE SECURITY. GOVT.NZ

For more info, visit: *protectivesecurity.govt.nz/trusted-business*

New Zealand's Espionage Environment

Espionage is an ongoing threat to New Zealand's national security that is directed against organisations in both the private and public sector

Espionage refers to various intelligence activities involving the clandestine collection of information or materials for the purpose of gaining advantage over a rival.

Global competition and insecurity drive the majority of espionage activity against New Zealand. The NZSIS has seen multiple examples of states seeking covert access to information on Government policy positions, security partnerships, technological innovations and research.

Despite our size, New Zealand is seen as a strategically important location, both due to our relationships across the Pacific and as a gateway to the Antarctic. New Zealand is also home to an increasing number of innovators producing niche technology that is targeted by foreign states.

It is almost certain there has been espionage activity from foreign states in New Zealand that has gone undetected. The NZSIS has had some disruptive success, but there is continued targeting of New Zealand's critical organisations, infrastructure and technology.

The majority of intelligence collection against New Zealand likely occurs through cyber exploitation, however individuals within organisations can be a point of vulnerability. Significant damage can be caused to New Zealand's national interests if even a small number of trusted insiders are compromised.

The states carrying out espionage against us are sophisticated. It is not just intelligence officers conducting this activity. Some governments take a 'whole of state approach' to intelligence gathering, which includes utilising businesses, universities, think tanks, or cyber actors to act on their behalf.

Espionage is inherently covert and difficult to detect. Public and private sector organisations are strongly encouraged to report suspicious activity to the NZSIS. Robust security practices are important too.

INTELLIGENCE ACTIVITY TARGETING CRITICAL INFRASTRUCTURE

Infrastructure becomes critical when it is considered essential for New Zealanders' security, wellbeing and economic prosperity. This includes businesses in sectors such as telecommunication networks, water services, ports, emergency services, and financial services.

Some foreign states seek access to, or control of, critical infrastructure assets. Suppliers or service providers to these assets can also be targeted due to the amount of harm that can be caused. Access or control could be gained, for example, by creating physical or remote entry points to key assets for later exploitation, creating supply chain dependencies, or compromising significant and sensitive data sets.

The significant harm comes not only for the business who owns or operates the asset, but compromise can lead to major consequences for New Zealanders who interact with or depend on the service provided.

It pays for owners and operators of critical infrastructure to closely consider how security risks are managed around access and control over their infrastructure.

TECHNOLOGY ACQUISITION

Some foreign states attempt to advance their technology requirements through covert or deceptive activity that can come at the expense of New Zealand's economic prospects and national security.

Heightened global strategic competition and regional security threats have meant a number of foreign states are looking to improve their military and economic standing through espionage.

There are multiple states seeking to target New Zealand's innovative technology through espionage, although those with authoritarian regimes pose a particular threat.

What are they targeting?

Innovative technologies

New Zealand has a range of sectors working on innovative and important technologies that would be of interest to a foreign state. Any exploitation could prevent local companies from extracting full economic value from their innovation, but it could also undermine our national security. Often technology that is targeted by foreign states is identified for a military purpose even if that was not the creator's intention.

Foreign states also seek technology that can provide them with advantages in a range of other sectors outside of the military.

Governments rely on economic prosperity as a way to maintain their legitimacy with their own populations. Being ahead of the game on technology helps to maintain a good standard of living and economic growth.

Some foreign states are willing to engage in espionage when innovative sectors within these states struggle to develop certain technologies. They may turn to espionage to gain the capabilities that can be used in their militaries and to generate economic opportunities at the expense of the original creator.

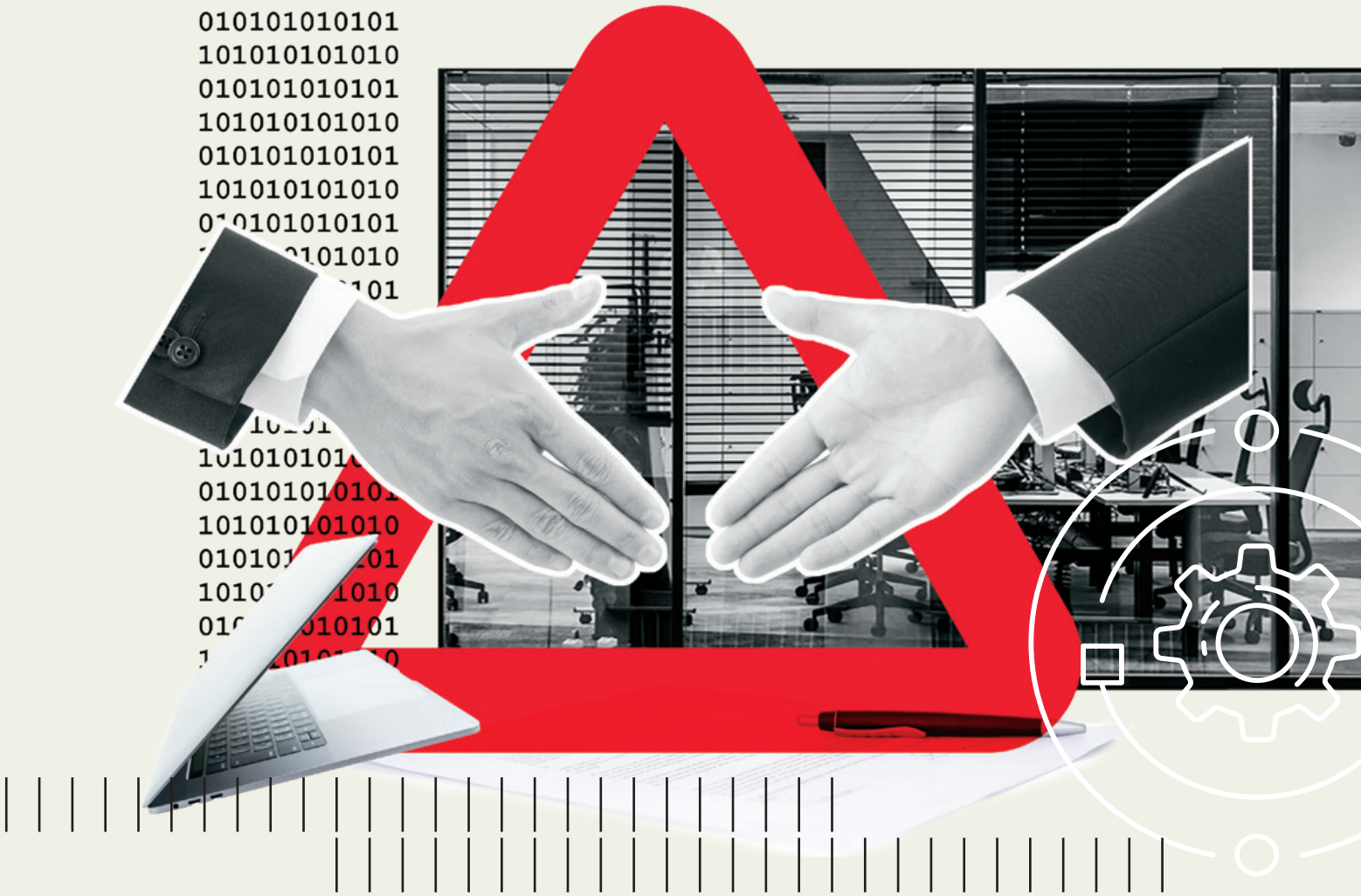
CASE STUDY

Basic due diligence prevented a New Zealand technology company being subject to activity that could have damaged New Zealand's interests.

While engaging with a potential new customer, the company did some research and found links to Iran that were concerning and had not been disclosed. The company made the decision to stop further engagement and prevented a probable attempt to obtain access to the business's technology. In this case, good security practice avoided credible risks to the business's reputation and its competitive advantage.

DUAL-USE TECHNOLOGY

Often foreign states are targeting technology with both civilian and military applications, or 'dual use'. It has become increasingly difficult to categorise technology as dual use due to the fact that technological advances mean that a much broader range of products can now be used for military purposes, even if this is not always immediately apparent to their creators.



Foreign national security laws

The PRC's national security legislation is a risk that should be managed by New Zealand businesses that have relationships with China-based entities.

The legislation creates a legal requirement for individuals and organisations in China to comply with requests from the PRC's security services. This could include providing authorities with access to data and systems, or sharing intellectual property.

New Zealand businesses should not feel as though they cannot engage with entities in China. The NZSIS recommends they should be conscious and deliberate about what information and control is at risk through that engagement.

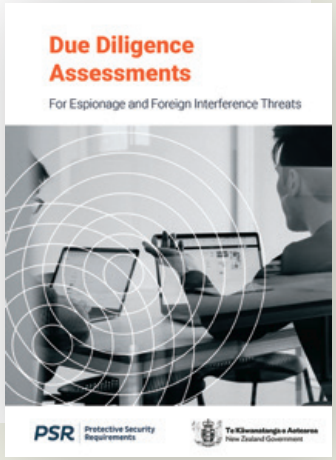
PROTECTIVE SECURITY ADVICE

PROTECTIVE SECURITY. GOVT.NZ

Conduct a due diligence assessment of the risks associated with any business, research or investment decision with a potential new partner or collaborator, to:

- Identify any foreign interference or espionage risks that may stem from your engagement
- Manage and mitigate identified risks to ensure your people, information, and organisation stay protected.

For more info, visit:
protectivesecurity.govt.nz/due-diligence



Targeting methods

Exploitation can happen under a number of guises:

Cover companies

NZSIS analysts have seen states use 'cover companies' which are designed to conceal the end-user of a piece of technology or research. These entities are often based offshore in third party countries that would not raise immediate concerns. Cover companies can provide a way for foreign states to circumvent export restrictions, trade sanctions and more generally conceal their involvement in commercial activity.

Investment

Some foreign states seek to gain access to technology by investing in a company of interest to them, or by becoming part of its supply chain. This sometimes involves the use of a cover company to obfuscate the origin of the investment. This can allow the foreign actor to gain access to the technology itself, or to individuals with experience in its development. The foreign actor may also be able to influence decisions around the technology's use or development.

Research and collaboration

Becoming involved at the research and development stage of a sensitive or emerging technology is an easier avenue for foreign states to gain access to innovation and research. Here a foreign state can exploit legitimate academic or research exchange rather than covert espionage activity to achieve their aims.

Academic spaces and research institutes are often open and collaborative in nature and also frequently experiencing funding challenges. This environment makes it easy for foreign states to access and exploit research through offers of financial support or collaboration.

Some foreign states use their domestic universities as development hubs for dual-use technology which is then implemented into their military or intelligence capabilities. New Zealand-based researchers have previously collaborated with some of these universities, perhaps without knowing the intended end use.

PROTECTIVE SECURITY ADVICE

The NZSIS and the National Cyber Security Centre worked with their Five Eyes partners to develop a set of principles to help frame thinking within organisations about how to protect innovation:

- **Know the threats** – understand the potential vulnerabilities that might put your product or innovation at risk.
- **Secure your business environment** – create clear lines of ownership around the management of security risks in a business. Appoint a security lead at board level who factors security considerations into decisions and initiatives.
- **Secure your products** – build security into the front end of your products by design. This will help protect your IP, make your products more marketable and ensure your products don't become a supply chain vulnerability.
- **Secure your partnerships** – make sure the people you collaborate with are who they say they are and can be trusted with your company's IP.
- **Secure your growth** – be aware of security risks as you expand, such as hiring new people into positions of trust and managing risk around entering new markets.

For more info, visit: *nzsis.govt.nz/secure-innovation*

NZSIS.GOVT.NZ

Insider Threat

New Zealand public and private sector organisations are vulnerable to the threats described in this report when individuals within these organisations use their access to intentionally or unintentionally cause harm.

An **insider threat** is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm its security or to harm New Zealand. This can be done either wittingly or unwittingly, through espionage, terrorism, unauthorised disclosure of information, or loss or degradation of a resource or capability.

Harm from insider threat activity could include disclosure of sensitive information; loss of sensitive technology; loss or degradation of a resource or capability; compromise of assets; or reputational damage.

Insider threat activity can sometimes be impulsive and opportunistic – at other times it can be deliberate and planned. Motivations to undertake insider threat acts are complex and usually influenced by a combination of pressures and vulnerabilities. These can include disgruntlement, grievance, ambition, feeling of unmet expectations, ego, financial motivation, divided loyalties or a combination of these factors.

Often the harm caused by insider threat is unintentional, and in these cases, can be caused by complacency, naivety, or a misunderstanding of the harmful consequences of an individual's actions.

CASE STUDY

A New Zealand government official was working on a project to procure sensitive technical equipment. The individual appeared to favour a vendor from a specific country, and their persistent support for that vendor disrupted procurement processes causing significant delays. NZSIS identified the insider risk, and supported the government agency to investigate the concerns. The agency had robust procurement policies that ensured the process remained fair, however the delays caused by this individual likely resulted in reputational damage to the New Zealand government.

INSIDER THREAT AND FOREIGN INTERFERENCE

There have been instances where insiders have engaged in behaviour that is supportive to a foreign state without receiving explicit instructions. There could be a range of motivations for this behaviour including bias, an affinity for a foreign state, or a desire to prove their worth.

Some foreign states exploit individuals who work for the New Zealand government, or who have access to government information to further their interests. They use a range of tactics to gain access to people, systems, or locations across central and local government to help the foreign state build information or influence.

Government employees routinely interact with foreign state representatives and must take care not to allow these relationships to be exploited. Foreign states approach relationships with a long-term strategic outlook, but individual employees may not be conscious of the bigger picture behind a one-off engagement.

Some foreign states will seek to use New Zealand government contacts to collect information on their targets or individuals of interest.

Roles where government employees are required to interact with both members of vulnerable communities as well as representatives of an authoritarian or repressive foreign state are at particular risk of being exploited by foreign state actors.

These states may consider using relationships with government insiders to attempt to exert influence over diaspora communities. It is possible individuals may either wittingly or unwittingly share information that could facilitate transnational repression. These employees are in a difficult position and will need more support to navigate the nuances of these communities and manage the possible involvement of foreign state actors.

PROTECTIVE SECURITY ADVICE

Security is everyone's responsibility. Developing and maintaining a strong security culture is crucial for any organisation to effectively manage its protective security.

A strong security culture is about developing a workforce that takes ownership for security issues and is more likely to think and act in a security conscious manner.

Creating a culture where employees routinely report security breaches or concerns is integral to mitigating insider threat risk. Staff members must feel confident they will be supported through their reporting and their concerns will be acted on appropriately.

For more advice, visit: *protectivesecurity.govt.nz/it-happens-here*

PROTECTIVE SECURITY. GOVT.NZ

Commonly used terms

CO-OPTEES/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.

DISINFORMATION is information that is intentionally false or misleading, spread with the intent to cause harm or achieve a broader aim.

ESPIONAGE refers to various intelligence activities involving the clandestine collection of information or materials for the purpose of gaining advantage over a rival.

FAITH-MOTIVATED VIOLENT EXTREMISM (FMVE) refers to violent extremists motivated by any interpretation of faith.

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.

IDENTITY-MOTIVATED VIOLENT EXTREMISM (IMVE) refers to violent extremists who seek to advance their own identity through violence or seek to denigrate the perceived identity of others.

INSIDER THREAT is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm its security, or to harm New Zealand. This can be done either wittingly or unwittingly, through espionage, terrorism, unauthorised disclosure of information, or loss or degradation of a resource or capability.

INTELLIGENCE is information that has been deliberately organised to give someone an advantage when making decisions under conditions of uncertainty. Intelligence may be derived from secret or open sources, but is usually classified to protect the advantage it confers.

MISINFORMATION is information that is unintentionally false or misleading, usually spread out of ignorance.

MIXED, UNSTABLE, AND UNCLEAR (MUU) is 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.

POLITICALLY-MOTIVATED VIOLENT EXTREMISM (PMVE) refers to violent extremists who oppose existing political systems, the Government, and are anti-authority.

STRATEGIC COMPETITION is where states seek to advance competing visions for regional and global order.

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.

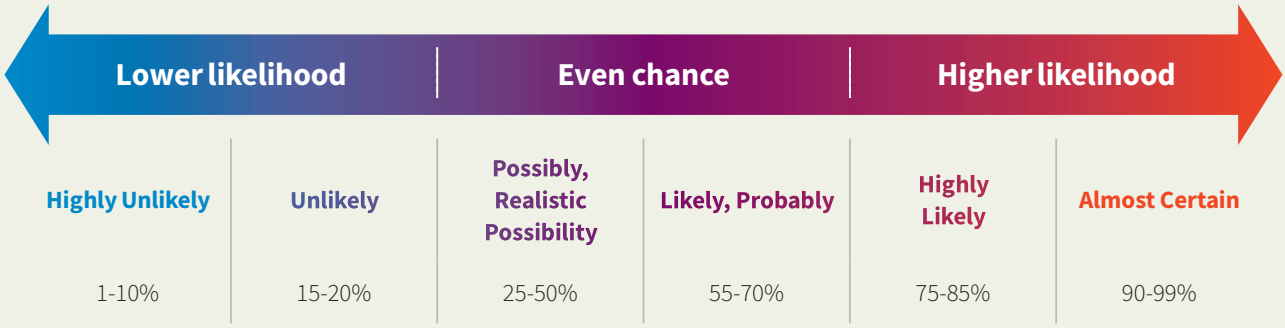
VIOLENT EXTREMISM is the use or justification of violence to achieve radical political, social, or religious change. Violent extremists often target groups they see as threatening their success or survival, or undermining their worldview.

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.

How to report a national security concern

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.

IN AN EMERGENCY CALL 1-1-1 IMMEDIATELY

There is no wrong door for reporting threats to New Zealand's national security.

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 number 105.

Whichever channel you choose, we will make sure your information reaches the right place.

ADVICE FOR PROVIDING INFORMATION

Please provide as much specific information as you can including, where possible, names, addresses, online usernames and anything else you think is relevant.

The NZSIS online form allows you to upload documents in addition to the information you provide. Every piece of information could potentially make a difference.

The form is available in nine languages and information can be provided in any language you prefer.

Your information will be treated in confidence. Submitters will only rarely receive a call back but you can be assured you have done the right thing by sharing your concerns.

NZSIS.GOVT.NZ

Sign up to our community newsletter at *www.nzsis.govt.nz/community*

Image disclaimer: A number of stock images used within this report were Generated with AI (Adobe Stock).

Te Pā Whakamarumaru
New Zealand Security
Intelligence Service