Te Pā Whakamarumaru
New Zealand Security Intelligence Service

New Zealand's Security Threat Environment 2023

An assessment by the New Zealand Security Intelligence Service

Contents

01. Scene Setting

i. Foreword from the Director-General of Security 4
ii. Executive Summary 6
iii. Glossary of key terms 13
iv. Who poses a threat to New Zealand 14

02. The security and intelligence threat environment in New Zealand

v. New Zealand's violent extremist environment 18
vi. New Zealand's foreign espionage and interference environment 24

03. The factors shaping New Zealand's security and intelligence threat environment in 2023

vii. Increased strategic competition 33
viii. Declining social trust 37
ix. Technological innovation 41
x. Global economic instability 45

04. Afterword

xi. The methodology behind our assessment 48
xii. Countering threats to our national security 49
xiii. Providing information 52

Foreword

Tēnā koutou

I am pleased to have the opportunity to publish an unclassified report outlining the nature of the security and intelligence threats we face.

This marks the first time the public will have access to NZSIS's consolidated analysis on New Zealand's threat environment.

This follows the release in October 2022 of *Kia mataara ki ngā tohu – Know the Signs*, our guide to identifying signs of violent extremism.

The NZSIS sees enormous value in sharing more of our insights with the wider public.

Typically, assessments like this are read by key decision makers across Government and mostly by people who hold a national security clearance. In this instance, we think our analysis will be useful to a much wider audience. There are people inside New Zealand businesses, institutions and communities who can use this document to help them make informed decisions about risk and mitigation.

The more we can help inform New Zealanders about the nature of the threats we face, the better security outcomes we achieve together. Heightened awareness allows us all to approach threats to our national security with a sense of confidence and inclusion.

We can make a greater impact if we, as a country, can learn to foster a sense of confidence that we can face up to national security threats of our time. Together, we can make great strides if we know more about the nature of these threats, where they come from and how they can be countered.

Being inclusive is an important part of the equation too. It helps us realise we all have a role to play to protect our national security and each other's wellbeing. When we get the mix right, we make ourselves a harder target for those who wish to cause us harm.

Our analysis is not about predicting what individuals or foreign states will do. No intelligence agency has access to that kind of crystal ball. Instead it is about understanding the factors that motivate or drive particular choices so we can better prepare ourselves for security threats, present and future.

I would like to think this assessment contributes to the vision outlined in the Royal Commission of Inquiry into the Terrorist attack on Christchurch masjidain on 15 March 2019. The report called for a more mature conversation about our national security. Being open and transparent with one another about the threats we face is one way we can have this important discussion.

In order to protect New Zealand, we must understand New Zealand's unique environment. Our goal for this report is for it to be a starting point for a greater level of awareness and a healthy conversation.

Ngā mihi

Andrew Hampton
Director-General of Security

Executive Summary

Within the national security community, the New Zealand Security Intelligence Service has a responsibility to detect, investigate, collect and analyse intelligence on matters of national security.

We work alongside other agencies such as the Department of the Prime Minister and Cabinet and the Government Communications Security Bureau.

Our mission is to keep New Zealand and New Zealanders safe and secure. To fulfil this, our current areas of focus are countering violent extremism and terrorism as well as espionage and foreign interference. These are also the focus areas for this report.

Other documents, such as the Cyber Threat Report produced by the Government Communications Security Bureau's National Cyber Security Centre, contribute to a broader picture of national security threats to New Zealand.

Our assessment is presented in two parts.

01. The security and intelligence threat environment

02. The factors shaping the threat environment

The first section examines the security and intelligence threat environment in New Zealand. The analysis then identifies four factors that we consider have the greatest impact and will shape our threat environment in 2023.

Executive Summary

The Security and Intelligence Threat Environment in New Zealand

Violent extremism

There are a diverse range of ideologies and influences that motivate violent extremists in New Zealand. The last year has seen the emergence, both here and around the world, of individuals who explore a range of extremist beliefs without aligning with any one in particular. We have adopted the phrase 'mixed, unstable and unclear ideologies' to help us understand their unique characteristics.

The traditional identity, faith and political motivations are still identified in violent extremists we detect and monitor in New Zealand but this new trend has emerged around the edges.

The National Terrorism Threat Level was revised to LOW in November 2022, meaning that a terrorist attack in New Zealand is considered a realistic possibility. Online spaces remain a haven for inflammatory language and violent abuse but the vast majority of those making threats are unlikely to follow through by committing a violent act in the real world.

Foreign interference

Both political and societal interference have been detected in New Zealand but the latter is probably more common. The main targets of interference activities in New Zealand are our migrant and well-established communities who may be viewed as dissidents by a foreign state. These communities can receive unwanted and unjustified attention from foreign states who conduct malicious activities designed to threaten and disrupt their peaceful life in New Zealand.

There are a small number of states who conduct foreign interference in New Zealand but their ability to cause harm is significant.

This report highlights the activities of three states in particular: the People's Republic of China (PRC), the Islamic Republic of Iran and Russia.

Espionage

There are foreign intelligence agencies who persistently and opportunistically conduct espionage operations against New Zealand both at home and abroad. The primary target remains the Government but now there are broader objectives that can see corporates, research institutions and government contractors in focus.

The information foreign agents aim to steal is increasingly broad too. Anything from military capabilities to sensitive intellectual property, or even personal information is being sought in order to gain strategic advantage.

Executive Summary

Factors shaping our threat environment

Our analysis identifies four factors we consider have the greatest impact and will shape our threat environment in 2023. They are:

strategic competition

declining social trust

technological innovation

global economic instability

All of these factors are seen as interconnected and each affects the four main threats the NZSIS is charged with monitoring. They are not presented in any particular order.

We seek to understand how individuals and foreign states interpret these factors and twist them to their advantage. Developing that understanding helps to shed light on some key questions such as: How do violent extremists exploit social distrust and grievances to achieve their goals? Are technological innovations making it easier for authoritarian states to meddle in the lives of their citizens at home and abroad? Will strategic competition drive foreign efforts to influence our politics?

Such questions are not straight forward to answer. New Zealand and our Pacific neighbours exist in a security environment that is becoming increasingly challenging for governments to navigate.

Over the last two decades, our national security conversation has been dominated by the threat of domestic and transnational terrorism, but now a threat that has been on the backburner has re-emerged.

Strategic competition is where states seek to advance competing visions for regional and global orders. We have seen this return to the forefront between the major powers, which is making the global and regional security environment more complex and unpredictable.

There are clear implications for New Zealand and our home region when geopolitical tensions become more intense. It is during times like these that foreign states will more frequently turn to the tools of espionage and interference to gain an advantage against us and our international partners.

Some states will seek to gain an advantage in any way they can. Technological developments are a common feature of strategic competition but attempts to drive social changes are becoming equally commonplace. The race to gain an upper hand is also helping to fuel a hyper-active information environment in which disinformation can spread rapidly.

Strategic competition and general disruption are the common themes behind most of the changes seen in New Zealand's threat environment over the past year. Our analysts have noticed these themes cutting across the social, political, economic, security, and technological factors they considered.

Disruptive changes in our online and information environment will continue to shape the threats we face. The anti-authority narratives, which gathered momentum online during the peak of the pandemic and in the months since, have created new pathways for violent extremism and have provided new opportunities for foreign states to interfere in New Zealand society.

On the technology side, foreign states and violent extremists alike will seek to find an advantage through the use of innovations such as data processing, encryption and tracking. The challenge for security agencies like NZSIS is to find ways to manage these threats while also upholding the values of a democratic society, such as human rights and privacy – considerations that will not be made by those who do not share the same principles.

The state of the global economy may be another wedge for some states to exploit. The current period of instability and weakness may encourage the further use of coercive and strong-arm approaches by some states to interfere and disrupt. At home and internationally, growing social and economic inequalities are among the many factors that we expect to contribute to the radicalisation of violent extremists in New Zealand.

Our threat environment is evolving at pace and already appears noticeably different, as well as more complex, to what was seen at the same time last year. We would expect that next year's threat assessment will look different to this one and have added layers of complexity.

A rapidly evolving threat environment will require a rapidly evolving response. Thinking about how we can make ourselves harder targets for acts of violent extremism, foreign interference and espionage has developed considerably in recent years and will need to continue on a similar trajectory in order to stay ahead of those who wish to cause us harm.

Glossary of key terms

The following is a list of terms NZSIS uses in its analysis.

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

SECURITY INTELLIGENCE is intelligence that helps Government agencies identify, understand and mitigate security threats.

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.

TERRORISM. Under New Zealand law, a terrorist act is defined as an ideologically, politically, or religiously-motivated act intended to induce terror in a civilian 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.

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.

ECONOMIC COERCION is any act by a state intended to influence the behaviour of another state by disrupting existing commercial relationships.

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

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

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

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

Who poses a threat to New Zealand?

NZSIS is focused on threats to New Zealand's national security that are caused deliberately by people. As indicated, these include threats from terrorism, violent extremism, espionage and foreign interference.

Only a small number of people are involved in causing these threats, all of whom are either agents of foreign states or individuals intent on using violence to achieve political or social objectives.

Agents of foreign states are directed by foreign governments to undertake espionage or interference activities against New Zealand. While only a few states direct such activity against New Zealand, some do so persistently and with the potential to cause significant harm to our governance structures, democracy, and social cohesion. In particular, states that engage in foreign interference are usually autocratic, repressive, or highly nationalistic.

NZSIS is very clear that those responsible for the foreign interference threat are the states themselves and the agents who act on their behalf. The vast majority of people in New Zealand who have ethnic connections to those states are not a threat. This is an important distinction. The report does not single out any community as a threat to our country, and to do so would be a misinterpretation of the analysis.

Very few people in New Zealand support using violence to achieve political or social change. Those who do can potentially cause great harm to the cohesion and safety of our communities. Acts of terrorism are rare in New Zealand, although we have suffered two attacks in the last five years.

It is important to note that the use or threat of violence is integral to the concepts of violent extremism and terrorism. NZSIS has no interest in the activities of persons with radical, unconventional, dissenting or alternative beliefs who do not intend to use violence. All our intelligence collection and analysis activities occur within a strict legal framework and are subject to several levels of approval and oversight, including by the independent Inspector-General of Intelligence and Security.

02.

The security and intelligence threat environment in New Zealand

Violent extremism

New Zealand's violent extremism environment continues to be influenced by a diverse range of ideologies, grievances and domestic and international events.

The spectrum of violent extremist activity in New Zealand mostly consists of expressing support for violent extremist ideologies. We assess there is a realistic possibility there are individuals in New Zealand who have the intent, and almost certainly have or could easily acquire the capability, to conduct a domestic terrorist attack. However, we are currently not aware of any specific or credible domestic attack planning – this includes by individuals or groups based outside of New Zealand. That assessment could change rapidly, and at any time.

We continue to see inflammatory language and violent abuse online targeting a wide variety of people from already marginalised communities.

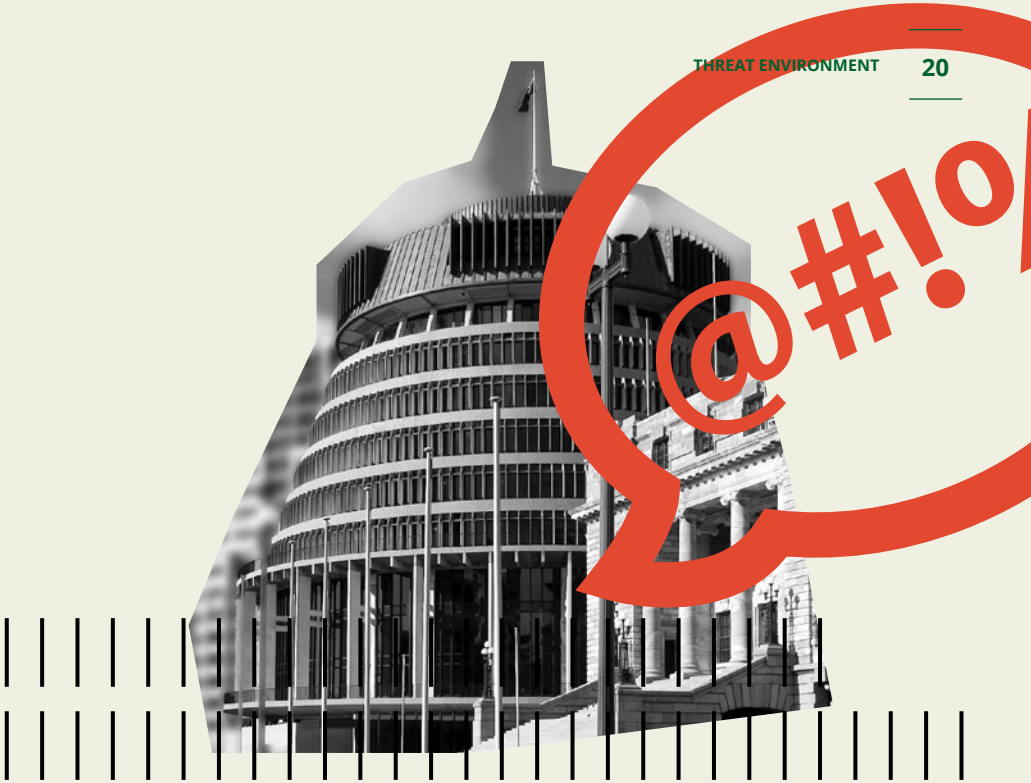
Despite the difficulty in assessing the true intent behind such threats, the vast majority making threats online are unlikely to engage in real-world violence.

A spectrum of ideologies continues to influence New Zealand's violent extremism environment, including Politically-Motivated Violent Extremism (PMVE), Identity-Motivated Violent Extremism (IMVE) and Faith-Motivated Violent Extremism (FMVE). While most violent extremists hold easily identified violent extremist ideologies, we have observed an increase in individuals holding mixed, unstable and unclear ideologies.

Politically-Motivated Violent Extremism (PMVE)

There are a small number of individuals who adhere to PMVE ideologies in New Zealand, largely focussed on anti-authority narratives, driven by conspiracy theories and misinformation and disinformation – in some cases produced by foreign states, though not targeted specifically at New Zealand. Even though PMVE adherents in New Zealand are typically united in their opposition to the existing political system, their narratives are often highly personalised and lack an overarching ideology or central ideologue.

Since the start of the COVID-19 pandemic, PMVE individuals have integrated a broad range of grievances into existing anti-authority beliefs. For example, United States (US)-specific ideas and events are often incorporated into New Zealand narratives, such as references to 'First Amendment' rights, despite having no applicability to New Zealand's political system. Following the lifting of most COVID-19 mandates, PMVE adherents have shifted focus to other domestic political issues and will highly likely look to exploit other polarising issues to further spread their beliefs.



CASE STUDY

NZSIS received credible public reporting concerning the behaviour of an individual displaying indicators of mobilisation to violence, including an 'us vs. them' ideology, justification of violence underpinned by their ideology, acquisition of weapons, and stated preparation to conduct an attack. The individual made threats to shoot specific politicians and supporters of COVID-19 mandates using legal and illegal firearms they possessed.

Based on the reported threats and other intelligence collected by NZSIS, we assessed the violent threats were motivated by the individual's ideological opposition to COVID-19 mandates and a desire for those deemed responsible for them to be punished. While NZSIS assessed that the individual lacked specific plans, there were signs the person had the intent and capability to conduct an attack. As a result, NZSIS used its legal authority to share this information with New Zealand Police, who then worked to mitigate the threat the individual posed.

Identity-Motivated Violent Extremism (IMVE)

White Identity-Motivated Violent Extremism (W-IMVE) continues to be the dominant IMVE ideology in New Zealand. Young people becoming involved in W-IMVE is a growing trend. W-IMVE adherents in New Zealand express views, which include but are not limited to, rhetoric relating to anti-Semitism, anti-Rainbow Communities and various white supremacy narratives, such as anti-Māori and anti-Islam. W-IMVE narratives in New Zealand can use local social, political and economic issues as justification for their ideologies, though they are generally secondary to transnational issues. Attack-related propaganda, including the Christchurch terrorist's manifesto and livestream footage are regularly shared among W-IMVEs in New Zealand.

Faith-Motivated Violent Extremism (FMVE)

A very small number of known individuals continue to adhere to FMVE ideologies in New Zealand. New Zealand-based individuals continue to express support for Islamic State of Iraq and the Levant (ISIL) and similar groups, though this has significantly decreased in recent years. Current ISIL support in New Zealand is largely from individuals who consume online propaganda and promote supportive rhetoric. This decrease in support is likely due to a number of factors including: the fragmented and leaderless nature of ISIL support in New Zealand; ISIL's current focus on an insurgency in Iraq and Syria lacks attractiveness and relevance to a potential New Zealand audience; and a general decline of support for ISIL in Western countries since the collapse of the physical so-called "Caliphate."

CASE STUDY

NZSIS received information from a partner agency about a New Zealand-based individual espousing support for what we assessed to be White Identity-Motivated Violent Extremism, in ideologically focussed online discussion groups. The user expressed support for ideologically-motivated violence against specific minority groups and women, and made threats of violence against representatives of government. The user posted material indicating they had radicalised a peer and was considering applying for a firearms license.

NZSIS conducted an investigation into the individual and worked closely with domestic agencies to understand the extent to which the individual posed a threat to national security. NZSIS assessments concluded the individual expressed support for ideological violence and their online threats and violent extremist rhetoric may have encouraged others to support violence, but the individual did not have the intent to carry out such an act themselves. The individual was also assessed to be facing challenges in their life not related to their ideology. NZSIS passed relevant information to other government agencies best placed to intervene and support the individual.

Mixed, Unstable and Unclear ideologies (MUU)

We have observed an increase in violent extremists in New Zealand and internationally who appear to hold highly personalised ideologies with no strong allegiance to a specific violent extremist or terrorist group. Often individuals exhibit behaviour which can be interpreted as 'ideology shopping' or exploring a broad range of extremist beliefs and adopting aspects that suit them personally.

To help with understanding the distinct characteristics of this phenomenon we have adopted the phrase 'mixed, unstable and unclear ideologies'.

Mixed ideologies refers to an adherence to multiple violent extremist beliefs at once, which may reinforce or appear to contradict one another. Unstable ideologies are when an individual's primary violent extremist ideology changes over time. Any shift might depend on external events or their own personal interest at a point in time and the range of beliefs they shift between may not be consistent. Finally, unclear ideologies are those where an individual has expressed violent extremist views or intentions with no explicit or obvious ideology underpinning it. There are new violent extremist ideologies emerging which we label as unclear until further investigative and assessment activity can be undertaken.

Although each individual is different, we assess the ease of access to a wide variety of violent extremist material online highly likely facilitates the development of MUU ideologies. These ideologies tend to evolve over time and allow an individual to make sense of and express their grievances. The threat and risk posed by individuals assessed to hold MUU ideologies varies based on the unique circumstances and mind-set of the individual.

Foreign espionage and interference

Some foreign states target New Zealand for political, economic and military advantage through the use of espionage and interference.

Espionage is by its nature intended to be secret and may go undetected for extended periods. Tactics include obtaining information, which may be used to support foreign interference activities. Foreign interference is distinct in its specific intention to have a disruptive, corruptive, or subversive effect on the targeted country, organisation, or individual. States carry out intelligence activity using both human and technical means.

Espionage

A number of foreign intelligence services persistently and opportunistically undertake espionage against New Zealand and New Zealanders, domestically and abroad. Espionage includes a range of activities carried out in secret to collect information, materials or capabilities for the purpose of obtaining an advantage over another state. Given the secret nature of espionage, it can be difficult to understand and identify the significant harm to our sovereignty, communities, economy, and national security.

While historically espionage was used to target government and classified information, today espionage activity also targets New Zealand organisations or individuals who may have knowledge or access to a broader range of information of interest to a foreign state. Many foreign intelligence services seek out individuals or information on the margins of government work. Such organisations might include businesses, academic and research institutions, government contractors, and others. Espionage may also be used to facilitate foreign interference, including the surveillance and harassment of migrant and ethnic communities.

Political espionage can help a foreign state gain insight into New Zealand's political decision-making or secure an advantage in trade or diplomatic negotiations. Foreign intelligence services routinely seek classified, sensitive and open source information in support of their strategic military and defence objectives. This can include information on existing military capabilities, planned acquisitions, current and future operational plans, strategic intentions, and research and technology developments relevant to the defence sector. States also use espionage to support their economic development and prosperity. This involves the theft of trade secrets, intellectual property, and new and sensitive technologies. We call this economic espionage (occasionally referred to as industrial espionage). It targets private sector commercial and industrial entities, alongside public and private research institutions. These entities are often more vulnerable to espionage than government agencies protected by national security systems.

International COVID-19 travel restrictions have prompted foreign states to consider different ways to target countries and to gain access to intelligence. The traditional methods of having foreign intelligence officers on the ground have been difficult so states have taken to trying to access and influence New Zealanders living and working offshore. Cyber-espionage is another common tactic and will continue to impact New Zealand networks

CASE STUDY

Espionage is not always targeted directly against classified materials or individuals with security clearances. A recent NZSIS investigation involved an undeclared foreign intelligence officer, who targeted and sought to cultivate a New Zealander with access to information and people networks of interest to the foreign state. The intelligence officer almost certainly sought to obtain political, economic and national security intelligence through the relationship, and in exchange offered financial and intangible incentives. The targeted New Zealander was in a position of having access to information and individuals with knowledge of New Zealand policy matters, but also had a public profile. Those individuals are often identifiable to foreign intelligence services through online networking and social media platforms, which allow them to engage significantly more prospective sources than if they were using solely in-person methods. In this case, NZSIS was able to intervene at an early stage. The relationship did not result in any information being exchanged that posed a significant security risk.

Foreign Interference

Only a small number of states engage in interference against New Zealand, but some do so persistently and with the potential for significant harm. Foreign interference is an act by a foreign state that is intended to influence, disrupt or subvert New Zealand's national interests by deceptive, corruptive or coercive means. Such a definition is an important distinction from the normal diplomatic activity in which most states engage, which include efforts to lobby and influence as part of normal and open diplomatic relations. There are other activities, including normal advocacy, dissent, and protest, which are carried out by individuals or organisations that may align with the interests of a foreign state, but are not deceptive, corruptive, coercive, or credibly linked to a foreign state. We do not consider such activities to be interference.

NZSIS has detected interference activity from a number of foreign states. Most notable is the continued targeting of New Zealand's diverse ethnic Chinese communities. We see these activities carried out by groups and individuals linked to the intelligence arm of the People's Republic of China (PRC).

We have also observed that public and official awareness of foreign interference matters and strong policy responses, make it more difficult for states to conduct interference activities in New Zealand. Deliberate protective efforts to guard against the threat since 2016 have probably helped make interference more difficult, but will also be driving changes to how states carry out political and societal interference.

NZSIS categorises interference into two categories, political and societal, in order to describe the objectives and victims of interference.

Political Interference

Political interference is an act by a state intended to influence, disrupt or subvert another state's governance or political systems by deceptive, corruptive or coercive means. In New Zealand this has largely taken the form of efforts to deceptively influence New Zealand policy-making. However, as the experience of other nations has shown, political interference has the potential to have wider impacts on the perceived integrity of elections and other democratic processes.

CASE STUDY

In 2022, a representative of a foreign state secretly worked with New Zealand-based community figures with the intent to persuade a New Zealander with political influence to change their position on a subject of sensitivity to that foreign state. The foreign state representative probably conveyed instructions to a number of New Zealand-based community figures, likely in an inauthentic attempt to portray a united grassroots movement against the political figure's position. The responsible foreign state is known to seek to suppress dissenting views on issues of sensitivity, and assert its own view of the issue as the views of all people with links to that state. In addition to providing the instructions, the foreign state also required individuals to report back and provide evidence that they had undertaken the required actions. NZSIS is aware that many of the individuals are committed and responsive to the instructions of the foreign state, and would be responsive to future direction to advance the position of the foreign state. NZSIS provided protective security briefings to the individuals who were targeted.

Societal Interference

Societal interference is probably the most common form of foreign interference in New Zealand.

Societal interference refers to acts by foreign states that are intended to influence, disrupt or subvert New Zealand's communities and non-government sectors by deceptive, corruptive or coercive means. This includes New Zealand's academic sector – encompassing institutions, employees and students. Increased public awareness of societal interference since 2016 has probably prompted some states to rethink how they engage with local communities in New Zealand.

Given the ongoing interests of autocratic and repressive states in monitoring migrant and well-established communities, such groups in New Zealand will remain at risk of societal interference. Most foreign efforts will likely remain focused on monitoring individuals perceived as dissidents by the foreign state, promoting nationalistic sentiment, and preventing expatriate communities from developing views deemed subversive by the foreign state. Social media monitoring, media manipulation, deploying networks of motivated community contacts and covert intelligence operations are some of the tactics used to achieve their goals. Communities that are reliant on information sources from foreign states are also likely to be vulnerable to misinformation and disinformation.

A subset of interference is transnational repression, which refers to any effort of a foreign state intended to prevent acts of political dissent in migrant or expatriate populations. Transnational repression can include a range of acts, some of which have been seen in New Zealand. These include:

- Community surveillance, including the monitoring and infiltration of community groups, and the co-option of community figures;
- Harassment, threats and assault intended to intimidate individuals into curtailing activities considered threatening by the foreign state;
- Proxy punishment, including the harassment, confinement, or harm

CASE STUDY

NZSIS has observed intelligence activity from a range of foreign states, including espionage to enable foreign interference. In one case, NZSIS detected a likely undeclared foreign intelligence officer undertaking activity in New Zealand to meet the intelligence priorities of a foreign state, which in this case likely focused on monitoring individuals of concern to that state. The likely intelligence officer gained access to sensitive and private information about a number of New Zealand-based people. The information may have exposed vulnerabilities of these peoples, and been used to collect further intelligence against them, and prompted surveillance and intimidation. This foreign state regularly monitors migrants, students, and dissidents internationally, and engages in interference and transnational repression activities, including forcible detention and assassinations. NZSIS provided protective security advice to ensure that the activity was mitigated.

to relatives in the country of origin as retribution or coercion of an individual abroad; and

- Involuntary repatriation, in which individuals are coerced or compelled to return to their country of origin.

Internationally, we are aware that a number of foreign states undertake assassinations of dissidents and defectors deemed threats to those foreign governments. Some foreign states target individuals in their resident countries, as well as third party countries when those individuals travel.

NZSIS has identified the Islamic Republic of Iran undertaking societal interference, including monitoring and providing reporting on Iranian communities and dissident groups. Globally, Iran has sought to silence dissenting Iranian voices in response to perceived threats to the Islamic Republic. Such activity has historically been unlikely in New Zealand, although the NZSIS continues to assess the threat in light of Iran's increasingly aggressive behaviour internationally.

03.

The factors shaping New Zealand's security and intelligence threat environment in 2023

Increased strategic competition contributes to foreign intelligence activity and the development of violent extremism

STRATEGIC COMPETITION

The international security environment in which New Zealand operates is now more challenging and less predictable than has been the case in recent decades.

Strategic competition is contributing to this unpredictability, evident in both a growing assertiveness from the People's Republic of China (PRC) and in international reactions to that assertiveness, as well as through large-scale conflicts such as Russia's illegal military invasion of Ukraine.

What is foreseeable is that an increasing competition between states creates fewer opportunities for more collaborative approaches to statecraft. As a result, we see greater incentives for states to reach for covert tools such as espionage and interference. This situation is especially evident in an environment where some states are moving away from, and attempting to rewrite, accepted international rules and norms of state behaviour. In a complex strategic environment, more states are likely to turn to intelligence to avoid surprise and gain an advantage.

PRC's efforts to advance its political, economic, military and security involvement in the Pacific is a major factor driving strategic competition in our home region. PRC has significant and growing intelligence and security capabilities, and its efforts are increasing New Zealand's exposure to the consequences of strategic competition.

The ongoing impacts of Russia's invasion of Ukraine are also being felt internationally through disruptions to supply chains and challenges to international norms. In addition to Russia's illegal war in Ukraine, Russia is also seeking to interfere in international support for Ukraine through coercive measures and leveraging its dominance in energy markets.

Strategic competition also manifests in conflict zones and under-governed spaces around the world. States look for opportunities to exert influence through support of governments and armed groups that align with their values or objectives. The movements and ideologies that ferment in these areas are often focused on local issues first but can adopt more global worldviews to garner support to further their cause.

Impact of strategic competition on **foreign interference and espionage**

NZSIS is aware of ongoing activity in and against New Zealand and our home region that is linked to the PRC's intelligence services. This is a complex intelligence concern for New Zealand.

New Zealand's geographic position in the Indo-Pacific, our links with other Pacific countries, and our shared interests in a stable, peaceful, prosperous, and resilient home region will draw the attention of foreign intelligence services who want to inform foreign governments on New Zealand's government policy and strategy in the region, and find ways to create conditions more favourable to those states.

In the context of strategic competition internationally, and as demonstrated prior to and during the Russian invasion of Ukraine, states will seek to further their advantage through intelligence activities. These activities include human and cyber-enabled foreign interference and espionage, seeding disinformation, and the use of economic coercion, among other methods. Due to the interconnected nature of our digital world, together with the comprehensive nature of global supply chains and interoperability of technology, many of the above activities targeting specific states will be felt by New Zealand and our international partners. Domestic and global networks are increasingly vulnerable to a range of potential cyber-related collateral impacts.

Impact of strategic competition **on violent extremism**

While not always targeted towards New Zealand or New Zealand-based people specifically, state-generated misinformation and disinformation is still consumed by New Zealanders. This information often references political and security-related events overseas to exploit pre-existing differences in society and is generated and disseminated to discredit competing world views and values. While not the only cause of an individual's radicalisation towards violent extremism, there is a realistic possibility it contributes to the process by further entrenching mistrust and grievances.

Historically, reduced state-to-state cooperation has at times allowed violent extremist and terrorist organisations the opportunity to advance their cause, or in times of strategic competition to receive outright support from a state to achieve a mutual advantage. While in most cases this has little impact on violent extremism in New Zealand, there are occasions when this does happen, for example ISIL had global impact, including generating support in New Zealand.

Declining social trust is shaping pathways and opportunities for violent extremism and societal interference in New Zealand

DECLINING SOCIAL TRUST

In part due to the COVID-19 pandemic, social fragmentation, disconnection, and polarisation have featured as an international phenomenon in recent years.

New Zealanders' trust in government, politicians, and fellow citizens remains high, especially when compared to global levels. There are signs, however, that trust levels are possibly diminishing and by some measures trust in the media is now below the global average[1]. Because of New Zealand's traditionally high levels of trust, a decline is more noticeable.

A study conducted by The Treasury into social cohesion in New Zealand found the reasons for diminishing levels of trust relate to perceptions that people are being deliberately lied to and misled; that those with power don't have New Zealand's best interests at heart; and that politicians are incapable of solving the problems facing the country. These factors are often the result of an individual or group's real or perceived concerns about their place in society, changes in societal and cultural norms, as well as life experiences. In some cases, these concerns are amplified by misinformation and disinformation. This is especially true online, where reliable information sources must compete for attention in a high-volume and quickly changing information space in which false or misleading information can spread rapidly.

The majority of people will use legal and non-violent avenues to address their concerns. Voting, standing as a candidate in elections, organising and attending protests or lobbying politicians are all normal and valid examples of ways to get across an opinion.

However, as a result of grievances and distrust in 'traditional' institutions, people can feel they have no other option than to work outside legal and non-violent channels. From this group, a small number of people can adopt beliefs and ideas, influenced by the information they consume and people they interact with, which support or advocate the use of violence. Such an environment may also support and

[1] The Treasury – Social Cohesion in New Zealand: Analytical Paper 22/01 and Trust in New Zealand Acumen Edelman Trust Barometer 2022

encourage activity that is detrimental to a free and open society.

Social discontent provides unique opportunities for foreign states to conduct interference activity. States may try to leverage significant social tensions or disagreements in society to their advantage. There could be attempts to cultivate political and social movements, which motivate interference and intelligence activity against expatriates, migrants, and others perceived to threaten the stability of foreign regimes. Foreign interference in New Zealand can also be driven by social discontent or upheaval within a foreign state's own country, as it may prompt them to target migrants in New Zealand or have an impact on a New Zealand policy decision.

Misinformation and disinformation spread in times of social upheaval because they tend to offer simple explanations for complex issues. They also reinforce existing biases or grievances. Misinformation and disinformation is often pitched in a way that makes the consumer feel they have special knowledge, or know the "real truth." It can even foster a sense of community or common purpose, as was evidenced over the past two years by those who seized on various conspiracy theories to unify their opposition to government COVID-19 responses. Misinformation and disinformation are unwelcome forces in our information environment, but are not considered threats in and of themselves. In most instances the information will fail to gain traction beyond niche and often insular audiences. Nonetheless, its presence can foster grievances over time that, left unchecked, can make our communities more vulnerable to violent extremism and foreign interference.

There are a range of sources of misinformation and disinformation including individuals, groups and states that each use it for their own purposes. For those producing and sharing violent extremist-related material, the information they peddle has the purpose of radicalising others to their cause and aims to build acceptance that violence is a means to achieve it. States produce and disseminate misinformation and disinformation to take advantage of already existing divisions within rival states and to attempt to control the narrative about how they are viewed abroad.

Impact of declining social trust **on foreign interference**

Foreign states may leverage significant social tensions to further their interests and shape narratives on a topic of interest or to sow disruption.

State-backed disinformation doesn't need to be targeted specifically at the New Zealand context to have an effect. New Zealanders will still come across it. Russia's international disinformation campaigns have not targeted New Zealand specifically, but have had an impact on the views of some New Zealanders.

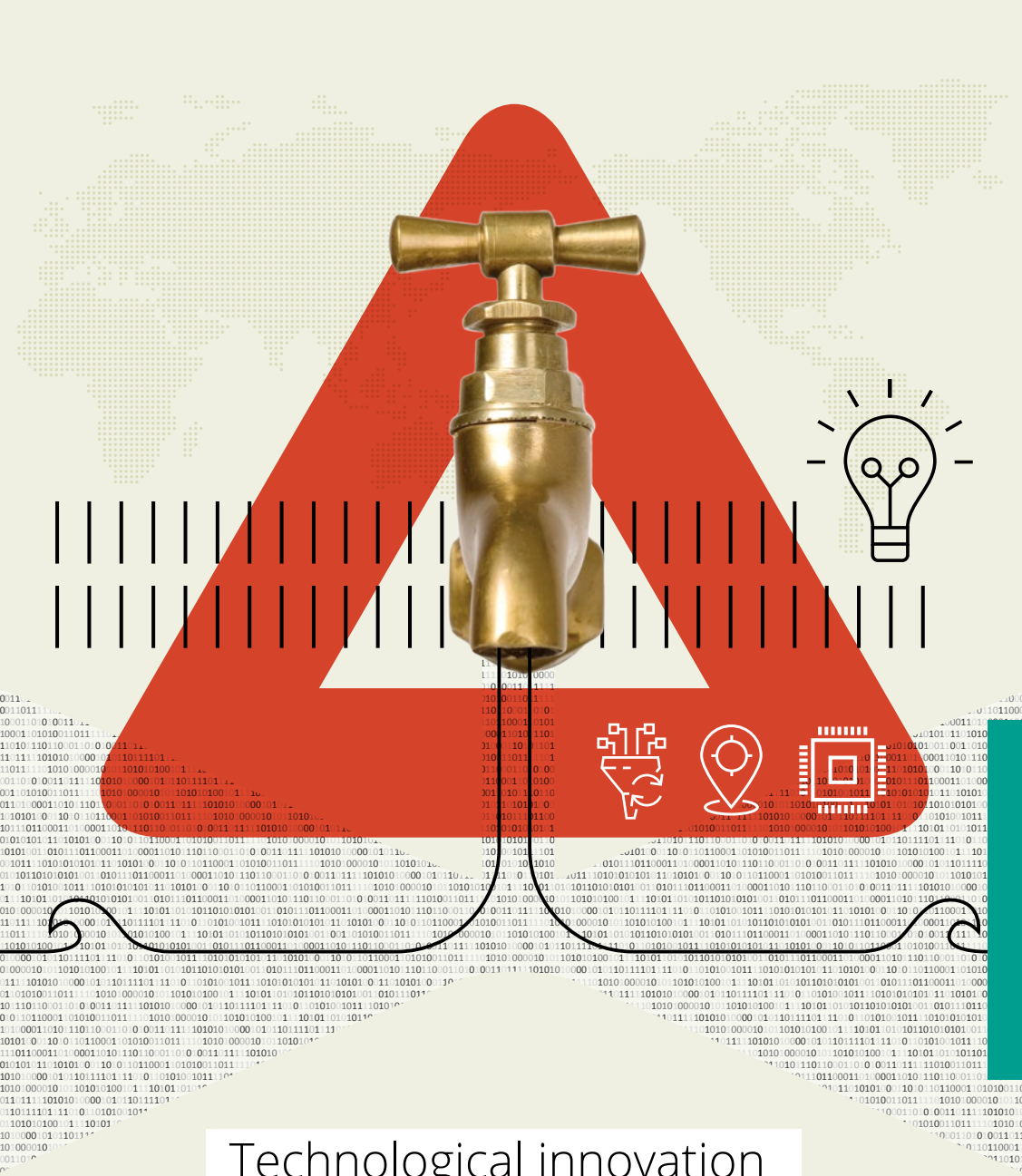
New Zealanders that rely heavily on discredited foreign information sources, such as the official or state-backed media of autocratic countries, are likely to be more vulnerable to the effects of disinformation. Often for those for whom English is a second language, there are few or no alternatives.

Impact of declining social trust **on violent extremism**

The consumption of misinformation and disinformation entrenches grievances by exploiting existing uncertainty and anxiety about what is happening in society. For a small number of people it acts as a gateway to increasingly more concerning information and can radicalise them towards the belief that violence is the only way to achieve their ideological goals.

Radicalisation often occurs in online echo chambers that become a person's main source of information.

In these online communities, which often cut across national borders, like-minded people share material and ideas that justify their support for violence. Members encourage people towards uncritical thinking, which disregards alternate solutions or explanations. The nature of these communities build a sense of belonging that strengthen one's loyalty to the ideology. This, in turn, enhances radicalisation and in exceptional cases, the path leads to mobilisation to violence.



Technological innovation is challenging security dynamics

TECHNOLOGICAL INNOVATION

Technology is part of our daily lives and its pace of advancement brings new challenges for New Zealand's security and wellbeing. Technology is ever more closely linked with other factors in our threat environment such as social disruption and strategic competition.

Increasing inter-connectivity between people and the delivery of services online is generating an exponential growth in the volume and complexity of data. Individuals and their activities leave a digital wake over the course of their lives, which is of significant interest to the commercial world but also to states. The ability to process large swathes of data means that data leaks and cyber security compromises become particularly valuable to both governments and the criminal world.

Acquiring and processing large datasets, including hacked and leaked information, highly likely allows foreign states to develop a comprehensive picture of large groups of people. Some of this activity has been brought to light by investigative journalists and civil society groups who have used open-source analysis to expose and report on foreign state activity.

Digital technologies also have the ability to bring people from across the world together through online communities. This has been demonstrated by the proliferation of social media and encrypted communication technologies. While these technologies have many benefits, they have also contributed to radicalisation by making access to extremist content easier and more secure. Social media algorithms can create feedback loops of violent and extreme content, while encryption and the proliferation of new communication and information-sharing services make detecting and countering such content very difficult.

Foreign states can also use sophisticated digital tools and tactics to identify, locate and monitor citizens or individuals they perceive as threatening offshore. Online communities are being used by states as channels for disinformation campaigns, as well as sources of intelligence on communities of interest to them.

The value of technological innovation for intelligence collection and disruption has driven states to invest significantly in research and development. This desire for cutting edge technology is so great that if states cannot develop it themselves they seek to steal it using cyber-espionage and other tactics. Intellectual property on technological innovation is equally useful, so states will deploy their own researchers abroad, often undercover, to study defence-related technologies in particular.

Sanctions and export controls also drive some of the illicit activity to acquire advanced technology. Access to some key technologies, such as semiconductors, is often strictly controlled. Semiconductors are a common feature in US-PRC competition. Meanwhile, sanctions placed on Russia since its invasion of Ukraine in February 2022 have likely hindered its development of new technologies and encouraged it to use more covert methods of acquiring essential components.

Technological innovation provides opportunity for those who wish to cause harm to do so in ways not originally intended by the manufacturer. For example, violent extremists have used 3D printing to manufacture firearms in terrorist attacks.

Impact of technological innovation on **foreign interference and espionage**

Technology has made covert activity cheaper and easier. It allows foreign states to conduct foreign interference and cyber espionage and deny any involvement by using cyber-criminal groups or other actors not directly linked to the state.

The ubiquitous nature of modern information technology provides opportunities for states to conduct societal interference, and using their global reach to locate, monitor, and target individuals and communities.

Cyber-enabled espionage poses a significant threat to New Zealand's national security and economic prosperity. Foreign states highly likely target New Zealand individuals, industry and government to gather information for their own economic, military or political advantage. The threat to critical national infrastructure is a particular area of concern. The impact of malicious cyber activity targeting NZ's critical national infrastructure (such as electricity grids or telecommunication networks) would likely be significant. There is also the potential for malicious cyber actors to opportunistically or inadvertently compromise critical national infrastructure through network vulnerabilities that leave the sector exposed. The National Cyber Security Centre's (NCSC) annual Cyber Threat Report provides more insights about the cyber threat landscape.

Impact of technological innovation on **violent extremism**

The online environment has contributed to the radicalisation of New Zealand-based violent extremists. Violent extremist material is predominantly consumed in isolation with little or no real-world contact with those who share the same beliefs. It is not difficult to access extremist information and concepts online, which are then interpreted by New Zealand-based people according to their grievances and often adapted to their New Zealand context.

The Internet offers violent extremists high levels of anonymity, which can make it difficult for intelligence agencies to detect and identify such individuals. The challenge is made even harder by the widespread public use of encryption technologies.

Detecting the true intent and ideology behind violent threats online is often difficult to establish unless additional information is available. Threats can sometimes be made in the context of ironic and deliberately provocative content designed to promote extreme messages.

Global economic instability is contributing to polarisation and disenfranchisement

GLOBAL ECONOMIC INSTABILITY

Global economic instability has become a feature of our security environment and is being driven by three main factors.

Firstly, global financial conditions tightened as major central banks raised interest rates to tame inflation. Secondly, Russia's war in Ukraine is dragging out and provoking a slowdown in the European economy that is curbing demand for exports from the rest of the world. Thirdly, the economy in the PRC is undergoing a sharp correction with the country's GDP growing 3% in 2022, the second lowest since 1977.

Economic risks certainly existed before COVID-19, but the pandemic and the subsequent global economic downturn have highlighted how much states rely on imports as well as the fragility of supply chains. Uncertainty over supply chains in particular is causing states to rethink how they mitigate future risks by bringing some manufacturing industries back closer to home and placing greater export restrictions on critical natural resources. It has highlighted the significance of key transport routes, including sea lanes, to ensure continued access to global supply chains and is leading some states to exert their geographic influence. The impacts of climate change, both current and anticipated, are exacerbating these trends.

High costs, tight labour markets and the hangover of COVID-19 related illnesses are also a feature of global economic uncertainty and have become another factor pressuring global supply chains under stress.

Higher prices of everyday consumer products and the increasing cost of debt are straining budgets in lower-income households in both advanced and developing economies. Meanwhile small-and-medium-sized-businesses are trying to keep afloat at a time of weakening consumption. At the same time, the real and perceived impacts of social and economic inequalities are contributing to global feelings of dissatisfaction and anxiety.

Impact of global economic instability on **foreign interference and espionage**

Foreign states may seek to exploit difficult economic times and the associated fear it creates in a similar way that some look to take advantage of societal divisions.

Economic difficulties at the national level could also reduce the resilience of New Zealand and our international partners to forms of foreign interference such as economic coercion. Russia has sought to leverage this advantage in Europe to weaken support against its invasion of Ukraine.

Economic uncertainty and the rising cost of living can make some people more vulnerable to states that seek to exploit them. For example, individuals with access to sensitive information who find themselves in a difficult financial situation would highly likely be considered a vulnerable espionage target by foreign states.

Impact of global economic instability on **violent extremism**

Economic instability can exacerbate the radicalisation of some violent extremists. An environment where there is public disillusionment with existing government policies and potential feelings of disenfranchisement can contribute to the development of a grievance. This is especially true where worsening economic conditions lead to job insecurity and make life less affordable. While most people will express economic frustrations peacefully, there are others to whom this justifies the use of violence.

04.

Afterword

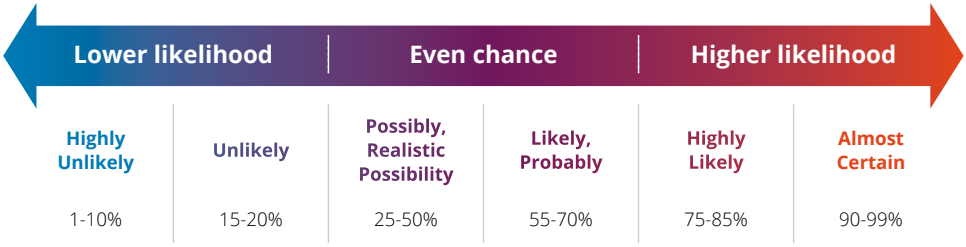
The methodology behind our assessment

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.

We have high confidence in our assessment of the current threat environment in the first part of this assessment. Our enduring focus on these threats domestically provides a large body of highly reliable and credible intelligence reporting, which is well corroborated. This is supplemented by our long-standing deep understanding of terrorism, violent extremism, espionage and foreign interference matters.

We have medium confidence in our assessments in the second part of the report on the factors shaping New Zealand's security and intelligence threat environment and future impacts. While we have developed our assessments based on a large body of credible and reliable sources, and our well-developed understanding of the current New Zealand threat environment, we acknowledge that intelligence gaps remain and alternative explanations are possible.

Probabilistic language has been used in parts of 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:

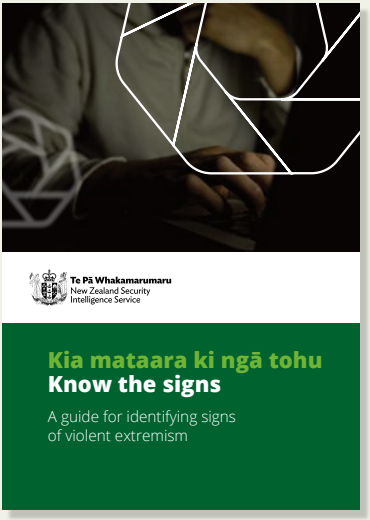


Acknowledgements

We would like to acknowledge the support, knowledge and feedback provided to us by our colleagues in government and external subject matter experts, which makes for a much more robust assessment than would have otherwise been possible.

Countering threats to our national security

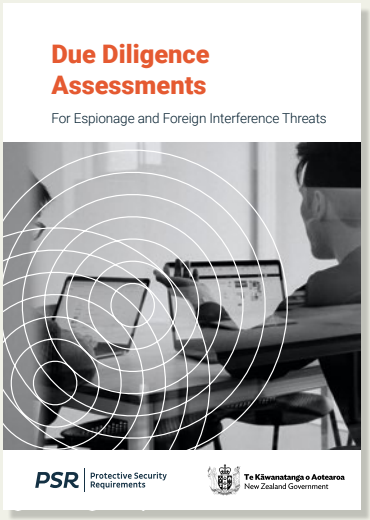
NZSIS produces a range of resources to help identify potential threats and advise on how they can be countered.



Kia mataara ki ngā tohu – Know the signs

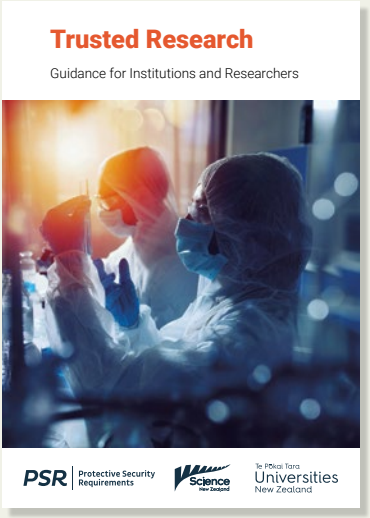
A guide for identifying signs of violent extremism.

This resource draws on the expertise and experience of NZSIS's intelligence professionals to identify the most common behaviours and activities they have observed during their work to counter violent extremism in Aotearoa.



Due Diligence Assessments for Espionage and Foreign Interference Threats

This guide is produced by NZSIS's Protective Security Requirements team to help organisations identify and mitigate the risks associated with foreign interference when working with others.



Trusted Research: Guidance for Institutions and Researchers

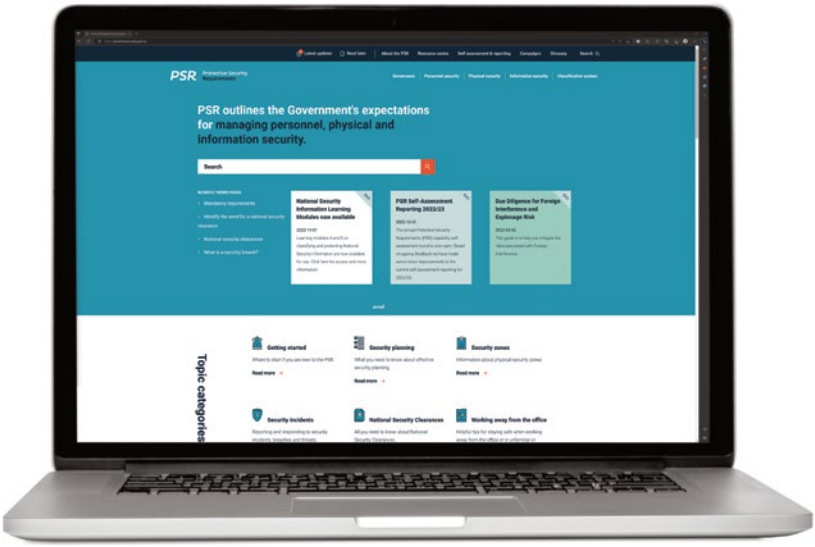
Trusted Research aims to help New Zealand's research and innovation sector get the most out of international scientific collaboration while protecting their intellectual property, sensitive research and personal information.

Espionage and Foreign Interference Threats: security advice for members of the New Zealand Parliament and Locally Elected Representatives.

This advice was produced to help elected representatives understand why they might be targeted by foreign states and the nature of the threats to which they may be exposed.

Protective Security Requirements website

Protective Security Requirements is New Zealand's best practice security policy framework. The website outlines the Government's expectations for how its agencies should manage security governance and personnel, physical and information security. There are a range of self-service resources available for any organisation wanting to improve its security arrangements. Find the framework at protectivesecurity.govt.nz.



Providing information

Your information could help NZSIS protect New Zealand from threats such as foreign interference, espionage and terrorism.

We all have a role to keep New Zealand safe. You can help by telling us if you notice concerning behaviour or activity.

You might be the person best placed to notice a threat to our communities, our economy, or our country.

Every year NZSIS receives hundreds of reports from New Zealanders who share information about potential threats to our national security. Even the smallest piece of information can be vital in helping us to detect and prevent foreign interference or terrorist attacks.

Trust your instincts. If something doesn't look or feel right, it's better to let us know.

Contact

In an emergency, phone 111 immediately. Also phone 111 immediately if the information is time-critical, such as if an attack is likely to happen very soon.

If the information is not time critical, you can report suspicious behaviour in one of the following ways.

TELL NZSIS

Complete an online form confidentially on our website: **www.nzsis.govt.nz**

TELL THE POLICE

You can either:

- Complete an online report at 105.police.govt.nz, or
- Call their non-emergency number 105.

Te Pā Whakamarumaru
New Zealand Security
Intelligence Service