



**Te Kāwanatanga o Aotearoa**  
New Zealand Government

# Let's talk about our national security: National Security Long-term Insights Briefing

Engaging an increasingly diverse Aotearoa New Zealand on national security risks, challenges and opportunities

October 2022

## Foreword

Tēnā koutou katoa

**Waiho i te toipoto, kaua i te toiroa** (Let us keep close together, not wide apart)

This National Security Long-term Insights Briefing is the first of its kind.

Work on this briefing has been led by the Department of the Prime Minister and Cabinet and the Ministry of Foreign Affairs and Trade on behalf of the Security and Intelligence Board<sup>1</sup>. Developed independent of ministers and the Government of the day, it looks at our changing national security landscape and presents some opportunities for the future.

National security affects us all. Our communities have experienced significant harm from violent extremism; the damaging impact of cyber attacks on our business, banking and health sectors; the ongoing danger from organised criminals; and the breakdown of international order, and the stability it provides, as some countries seek to assert their interests.

As we continue to experience the impacts of the COVID-19 pandemic, the accelerating rate of climate change and the rapid spread of mis- and dis- information, our collective understanding of national security threats and our ability to respond is constantly being tested.

Through this briefing, which focuses on engaging an increasingly diverse Aotearoa New Zealand on national security – we seek to share information on some of our most pressing national security risks and challenges. As a nation, we have choices about how we approach these. By increasing public conversations on national security, we can prepare and grow our resilience to meet these challenges together with a shared understanding of possible ways forward.

We are publishing the draft briefing now for public consultation, prior to finalising it later in the year.

Thank you to all those who have engaged with us and contributed to this briefing so far. We have heard that conversations about national security matter, and that regular sharing of information is important. This briefing is one step toward this.

When developing this briefing we have considered public feedback, information on future national security issues, international research and Statistics New Zealand data. We are now seeking your feedback on our ideas for what a bright future for national security could look like, and how we can engage an increasingly diverse New Zealand to turn those ideas into action.

Thank you for taking the time to provide feedback on this draft briefing.

We look forward to hearing your views and continuing this conversation with you.

Ngā mihi



Tony Lynch  
Chair, Security and Intelligence Board

# Welcome

This Long-term Insights Briefing is about protecting and advancing Aotearoa New Zealand's national security – our people, our nation and our interests – considering how we can thrive now and in the future.

The topic of this briefing is ***Engaging an increasingly diverse Aotearoa New Zealand on national security risks, challenges and opportunities.***

In particular, it looks at a number of risks and challenges to our national security – such as cyber attacks, terrorism, violent extremism, disinformation, and organised crime. It also presents some ideas to support a bright future for our national security, including why engaging with New Zealanders is central to this.

Conversations about national security can be difficult, but they are key to ensuring New Zealand's future as a safe and secure place for those who live, work and visit here. We believe open, inclusive, and accessible engagement by government will help build trust and confidence, and strengthen our national security. Through this briefing we aim to increase awareness and understanding about national security. We hope this will lead to greater engagement and debate in the future.

We are keen to know what you think of our ideas and welcome all feedback and suggestions.

## The story behind this briefing

Long-term Insights Briefings are a new way for government agencies, acting independently of their Ministers, to explore and report back on issues that matter for the future wellbeing of the people of New Zealand.

The [Royal Commission of Inquiry](#) into the terrorist attack on Christchurch masjidain recommended that government rethink the way we involve the communities we serve – to create a society where all New Zealanders feel safe and included. We want to use this briefing to help us move toward this over the long term, to hear your views and explore what our future national security could look like.

This briefing was produced by a group of nine government agencies that are responsible for protecting New Zealand from national security threats. It follows a public survey, research and public consultation. We learned that New Zealanders care a lot about national security, want to be kept informed and updated on developments, and want to be part of conversations about New Zealand's national security plans for the future.

This is encouraging, because the increasingly complex risks to our national security mean we need to involve all New Zealanders in our efforts to protect our country from harm.

This briefing uses the research and information we have heard from communities, businesses, and government agencies to look at:

- key global trends that will influence New Zealand’s national security over the next 10 to 15 years
- some national security risks and challenges of concern and how they might change over the next 10 to 15 years
- what key features could support a bright future for national security into the future.

*Please note that, while this briefing has been produced independently of ministers and is not Government policy, it has been written at a time when a broader set of Government policy initiatives are being developed that aim to create change in the national security sector – namely New Zealand’s first National Security Strategy and a review of the national security system functions and form (as recommended by the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain).*

*This briefing also explores similar themes to other government Long-term Insights Briefings– particularly the Public Service Commission’s briefing on “[How can we better support public participation in government in the future?](#)” and the briefing led by the Department of Internal Affairs which considers “[How can community participation and decision-making be better enabled by technology?](#)”*

## Where we started – research and engagement

As part of the development of this briefing, we have sought information on Aotearoa New Zealand's national security from a range of sources.

Our research included:

- a [National Security Public Survey](#)<sup>2</sup> – an independent survey of more than 1,000 people living in Aotearoa New Zealand, which we hope to repeat each year. The survey focused on New Zealanders' perceptions, attitudes to, and awareness of, a broad range of Aotearoa New Zealand's national security risks, challenges and opportunities.
- feedback from our initial round of consultation on the briefing topic – where we received 105 submissions from members of the public, organisations and businesses expressing their views. The submissions were supportive of the topic, with those who took part commenting on the need to consider a range of national security risks and challenges and take a more open and collaborative approach to conversations on national security. You can read a summary of their views at <https://dpmc.govt.nz/our-programmes/national-security/national-security-long-term-insights-briefing/ltib-topic>
- information from government agencies involved in New Zealand's national security system<sup>3</sup>
- publicly available data and research from New Zealand and overseas.

The survey findings and initial public consultation provided us with a deeper understanding of how New Zealanders perceive national security risks, challenges and opportunities. We have used these information sources to inform this briefing – enabling us to identify areas where we can provide more open and accessible information.

## What we learned – some findings of note

The information we gathered through the National Security Public Survey, submissions, research and other public sources revealed three key areas of concern for the future of our national security:

- New Zealanders perceive threats to our national security are increasing
- global events and trends are increasingly and intensely affecting New Zealand’s national security, and
- confidence in the government’s ability to respond varies.

### New Zealanders are more concerned on average than people in other countries about a wide range of threats

The National Security Public survey included a wide range of threats, risks and challenges to our national security. This broad coverage helps us to better understand public perceptions across a range of issues, which we can compare with international survey results.

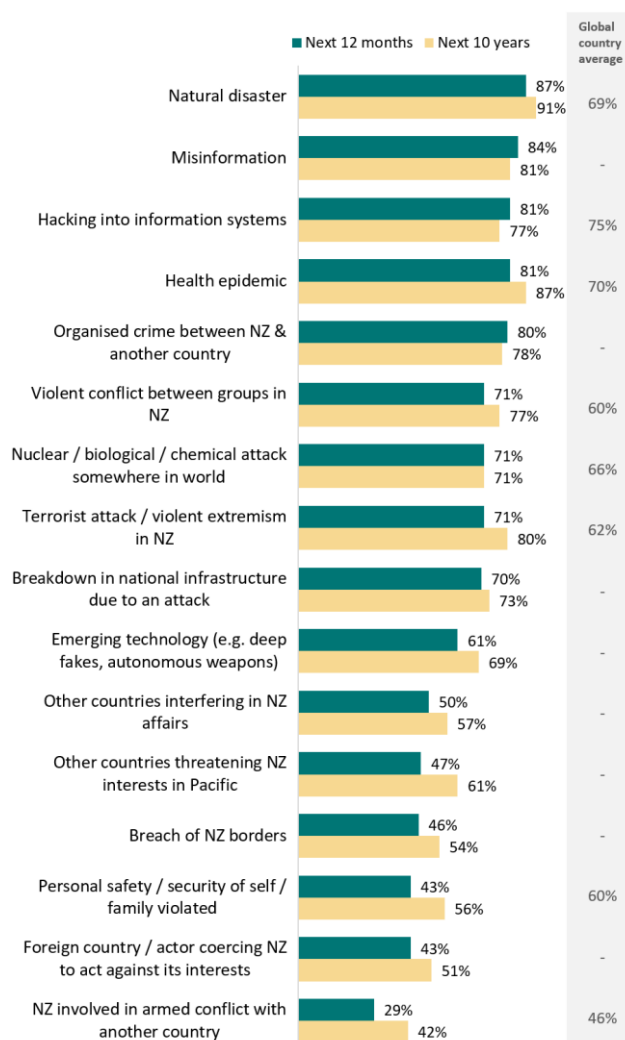
On average, we heard through the survey that New Zealanders are more concerned than other people around the world about a range of threats.

It is not surprising that New Zealanders feel concerned about natural disasters occurring, given our vulnerability to events like earthquakes, floods, droughts and volcanic activity. We are one of the most natural disaster-prone countries in the world. The New Zealand government takes an integrated approach to natural disasters, focusing on: reduction, readiness, response and recovery. More information on the approach is available at [www.civildefence.govt.nz/cdem-sector/the-4rs/](http://www.civildefence.govt.nz/cdem-sector/the-4rs/).

Health epidemics will also be top of mind for people, as we continue to respond to the ongoing impacts of COVID-19. More information on the approach being taking is available at [www.health.govt.nz](http://www.health.govt.nz) and <https://covid19.govt.nz/>.

### National Security Public Survey

Q. How real do you feel the threat is of any of the following happening in the next 12 months / 10 years?



Source: 2022 IPSOS National Security Public Survey (published October 2022).

Note, misinformation here covers both mis- and dis-information

What is particularly interesting in the context of this briefing is the level of concern about threats caused by people or countries wishing to do us harm (often referred to as “malicious actors”), such as hacking (attacks by cyber criminals and country-backed malicious actors who steal, expose, alter, disable or destroy information through unauthorised access to computer systems), or organised crime (illegal activity across national borders). The second-highest threat of concern in the next 12 months was the spread of misinformation (misinformation here covers both mis- and dis-information).

The survey shows that there is increasing concern over the long term for some of these types of threats too, including a foreign country or actor coercing New Zealand, a country threatening New Zealand’s interests in the Pacific and the potential for New Zealand becoming involved in an armed conflict.

We also heard, through the survey and through public consultation on the briefing topic, that people want us to share more information and talk more about these types of national security threats.

## The focus of this briefing

Reflecting the perspectives of the agencies participating in the development of this briefing alongside what we have learned through the survey and public consultation, we will focus on trends and issues of particular concern, including the following specific national security threats:

- Disinformation
- Hacking and cyber attacks
- Transnational organised crime
- Foreign interference and espionage
- Terrorism and violent extremism
- Pacific resilience challenges.

By sharing this information, we seek to support greater public understanding and conversation about national security.

## Global trends are affecting New Zealand's national security

Threats to our national security do not occur in a vacuum. What people told us reinforced our view that in a world that is more connected and competitive than ever before, international events and trends are having an increasingly detrimental effect on New Zealand's national security. We expect that in the next 10 to 15 years, the most significant risks to our national security will be influenced by, and in some cases originate from, four key global trends:

- **Increasing competition** between countries, and a continued deterioration in the 'rules-based international order' (this worldwide system is made up of rules, principles and organisations that support countries to work together, which encourages peaceful, predictable and cooperative behaviour).

New Zealand's support for the rules-based international order enables us to benefit from peaceful cooperation with other countries. However, we believe that threats to the international order will increase as countries with views and goals that are at odds with this system seek to undermine it and act in disregard of it. This was demonstrated most recently and acutely by Russia's ongoing invasion of Ukraine. While Europe and other countries have been and will continue to be affected most, the invasion is a grave breach of international rules, putting pressure on the international order and will affect people around the world.

For New Zealand, further deterioration in the international order will increase threats to our national security while also making it more challenging for us to respond and protect our interests.

- **Technology change** will impact all aspects of life, creating transformational benefits and improving standards of living but also presenting new risks and challenges. While predicting this change accurately is difficult, we anticipate an increasingly connected global population owing to the continued rapid development of technology.
- **Climate change** impacting the availability of water, food, and habitable land – creating competition for scarce resources and changing migration patterns. More frequent and severe weather events and natural disasters will place increasing pressure on countries' abilities to recover.
- The ongoing, shared and disruptive economic, social and political effects of COVID-19 and future **pandemics**.

Alongside these evolving trends and risks, New Zealand's demography is changing – we are getting older and more diverse and increasingly living in cities. We believe we need to respond to this development by changing the way we engage with New Zealanders to encourage more inclusive and representative participation. This will help government to build trust and respond to their needs, and ensure that we collectively understand the risks, challenges and opportunities before us. It has been forecast that by 2038:<sup>4</sup>

- New Zealand's population will have increased from 5.08 million to 5.88 million, with most living in cities (71 per cent)
- our ethnic makeup will be more diverse, with projected increases for Pacific, Māori and Asian ethnicities
- we are an ageing population, with the average age increasing from 37.4 years (2018) to 42.2 (2038) and the number of over 65's doubling to 1.3 million (2038).



## What could these trends mean for our national security in the future?

To help us consider the future, we present **three hypothetical outlooks**. They summarise how global trends could impact the context in which national security threats occur, and the conditions under which we may need to respond. Trends and events can develop in unpredictable or unexpected ways. The ways threats interact is constantly changing and can lead to unanticipated outcomes. *In the next 15 years, perhaps we could see...*

### A continued decline

More countries, including powerful ones, increasingly and more rapidly try to promote their interests, at the expense of our own values and interests. The prospect of armed conflict between countries becomes greater as the rise of nationalism pervades the international landscape. Cooperation through multilateral institutions diminishes, making it harder to meet global challenges such as climate change. Competition for resources (energy, food, and water), and changing migration patterns, increases the chance of direct conflict. A deteriorating global order means transnational organised crime thrives, including online, and some states are more brazen in their willingness to interfere and disrupt our way of life – including through cyber-attacks and espionage. Efforts by malicious actors to interfere in our democratic processes remains a growing concern. Greater divisions in our society threaten to erode trust in public institutions. There is little shared public understanding of the challenges we face in New Zealand, and in the context of an ageing population, cycles of inequality and automation in the workforce, some will be particularly susceptible to extremist ideologies spread online and shaped by mis- and dis-information.

### A dramatic decline

Conflict in Europe continues, with Ukraine remaining an active frontline, and with other countries becoming directly involved and more severely impacted for the longer-term. There is an ever-present threat that a nuclear weapon could be used. There is open conflict in the Indo-Pacific region, for example, through a potential miscalculation in the Taiwan Strait, and/or increased militarisation in the Pacific. This is against a backdrop of accelerating and unmitigated climate events. As a result, some countries actively prioritise their interests at the expense of others, and there is direct competition for resources (energy, food, and water). At home, threats to our national security accelerate and our communities are harmed. A catastrophic cyber event, either globally released or directly targeting New Zealand degrades digital services that we rely on in our everyday lives impacting businesses, health services, and transport infrastructure. A lack of resourcing, information sharing and the spread of sophisticated technology-enabled mis- and dis- information makes it difficult for people to tell fiction from fact. New Zealand is more polarised than ever, trust in the institutions of state is diminished, threatening the foundations of our liberal democracy.

### An optimistic and improving outlook

While pressure on the international rules-based order remains, there is still strong impetus for countries to meet global challenges such as climate change collectively, and to work together to mitigate national security threats, while holding malicious actors to account. International collaboration, technological innovation, and investment in climate adaptation, encourages the sharing of resources, helping to avoid direct and armed conflict. Greater transparency, open and accessible information-sharing, engagement and partnership between government and the public increases trust, confidence, and social licence to respond to national security challenges. New Zealand's national security sector is future-focused and adaptable, and we band together as a country to protect and promote our national security interests and support our people to thrive.

## National security risks and challenges of concern

In this section we take a closer look at some specific national security risks, threats and challenges that we are concerned about, and which were raised consistently throughout our research and engagement.

- Disinformation
- Hacking and cyber attacks
- Transnational organised crime
- Foreign interference and espionage
- Terrorism and violent extremism
- Pacific resilience challenges.

For each risk or challenge we include:

- a description
- what we heard through our research and survey
- how we see this might change over the next 10 to 15 years
- some work we are doing to prepare for the future.

Later in this briefing we present some ideas to support our future national security over the long term, including why engaging more with New Zealanders is important.

### The challenge of disinformation (and misinformation)

**Disinformation** is false or modified information knowingly and deliberately shared to cause harm or achieve a broader aim.

We are particularly concerned about disinformation as we see this exacerbating a number of national security issues. It is impacting liberal democracies worldwide, eroding trust in institutions, and our ability to respond to it as a society is being tested.

Disinformation takes different forms and creates a range of harms, for example by promoting extreme beliefs; fuelling disagreement and division in society; and, spreading harmful narratives which threaten minority groups. Ultimately, the spread of disinformation can lead to radicalisation and violence when people chose to act upon these beliefs.

Country-sponsored disinformation poses a particular challenge. When this activity is backed by other countries, they can create sophisticated and sustained disinformation campaigns, using vast and specialist resources to push false or deceptive information online about ideas or topics that matter to New Zealanders.

For example, recent analysis by Microsoft reports that New Zealanders were subject to a spike in exposure to Russian disinformation or propaganda online after December 2021, much of this related to COVID-19.<sup>5</sup> This spike preceded an increase in protests against COVID-19 measures and other issues in New Zealand.

When compared to other countries, New Zealand overall has relatively high levels of trust in mainstream media and public institutions. We are concerned that disinformation will damage that trust and undermine our national security. Disinformation can also affect social cohesion (where everyone feels safe, valued and heard, has a strong sense of belonging and can participate fully in society).

The open nature and reach of the internet allows for the rapid sharing of information and connection between people globally. However, as much as this is a positive and important aspect of the internet, it is also a highly effective means for spreading information that may appear to be legitimate and credible but is not. When this false information is shared by someone believing it to be true, this is **misinformation** – information that is false or misleading, though not created or shared with the direct intention of causing harm. In this way, false and misleading information continues to spread at speed, particularly on social media – and while some social media platforms have implemented some measures to combat this, the challenge remains, and the need to balance credibility against freedom of expression makes responding to this complex.

***“This has been a real problem for the past few years. Due to ever-increasing internet and social media sites, people are more likely to come across information that, while false, resonates with their ideology.” Survey respondent***

The spread of disinformation and misinformation affects our ability to meet challenges such as COVID-19 as a whole country, based on a shared understanding of evidence. We are worried that this challenge will continue and accelerate into the future.

In the National Security Public Survey, we heard:

- misinformation topped the list of perceived national security threats (‘misinformation’ here covers both mis- and disinformation)
- 84 per cent of respondents felt there was a real threat that misinformation on topics of public importance would spread in New Zealand in the next 12 months
- 25 per cent considered misinformation to be the greatest threat to them and their families/whānau
- misinformation was seen as a threat both now and in 10 years’ time.

Most disinformation is legal and fits within definitions of protected speech – making it difficult or inappropriate to address using traditional law enforcement and intelligence tools before the harms become apparent. Government, communities and academia need to work together, alongside technology and media companies, to prevent harmful messages being spread online, while also protecting freedom of expression and an open internet.

For some people in New Zealand, experiences of inequality, neglect or discrimination (including racism) and a distrust of government and news media have extended through generations. In turn, these views can enable the spread of disinformation, especially by malicious actors and other countries who seek to divide our society and encourage disagreements between groups.

#### **In the next 10 to 15 years, we expect to see:**

- an increase in the prevalence and sophistication of disinformation. Other countries may purposely seek to encourage tension, distrust and divide New Zealanders. This will pose an ongoing threat to our democracy and national security
- new and emerging technology is likely to increase the problems caused by disinformation, including the emergence of synthetic media such as ‘deepfakes’ as well as machine learning and artificial intelligence

- increasing harm and consequences caused by disinformation narratives driving disagreement between our communities and impacting people (for example, potential threats, abuse, intimidation and harassment towards lawmakers, the media, academics, authorities, officials, and the general public)
- disinformation narratives influencing and exacerbating a range of other national security risks and challenges.

### **Preparing for the future now:**

- **Collaboration** – greater efforts are needed to detect disinformation campaigns and networks, and disrupt them in a coordinated way internationally, while calling out those that sponsor this activity. This must include working with a diverse range of communities, media, academia, civil society and the private sector – especially social media platforms – to understand the impact of the algorithms they use to steer people towards online content. Sharing intelligence and information with other countries will remain an important part of the response.
- New Zealand’s approach to building resilience in our society and preventing the spread of disinformation needs to be comprehensive and long term. It should bring together those who can draw on a wide range of tools and expertise, while protecting human rights and freedoms, and a free, open and secure internet.

## Hacking and cyber attacks

Hacking and cyber attacks can be motivated by financial gain, as an act of aggression or espionage, or a desire to promote ideas or beliefs. They can cause financial losses, damage reputations, steal intellectual property and disrupt critical services such as banking and health systems.

Cyber attacks are a global issue affecting all nations, as they can cause nationally significant services to be disrupted and individuals to suffer personal harm. Our ability to address cyber attacks requires cooperation with other countries in identifying solutions and agreeing on ‘responsible’ behaviour.

### **Cyber attacks in New Zealand are common**

Recent high-profile cyber attacks have included:

- an attack on the NZX (New Zealand’s stock exchange) in which the organisation’s systems was flooded with internet traffic to prevent users accessing connected online services
- a data breach at the Reserve Bank of New Zealand caused by IT supplier’s systems being compromised
- a \$30 million cyber hack on the Christchurch-based cryptocurrency exchange Cryptopia, and
- a ransomware attack on the Waikato District Health Board.

In the next 10 to 15 years, we expect cyber attacks to become more frequent, severe and sophisticated worldwide. Cyber attacks overseas will also negatively impact New Zealand. Here in New Zealand, 81 per cent of respondents to the National Security Public Survey said cyber attacks were a concern – a result that was higher than the global average (75 per cent). The view was also echoed by submitters on the briefing topic, who noted that individuals were not often equipped to maintain their safety online.

***“This is already happening all the time. In my job we have to follow A LOT of procedures to try and prevent these attacks, with only some success.” Survey respondent***

Many people said to us that we need to put the same effort into online security as we do into offline (physical) safety, especially for groups with little understanding of the online world and those who are vulnerable for other reasons.

Over 2020/21, the [National Cyber Security Centre](#) (NCSC), part of the Government Communications Security Bureau, recorded 404 attacks against nationally significant organisations – an increase of 15 per cent on the previous year. Of these incidents, 27 per cent showed indications of suspected criminal or financially motivated actors (in comparison to 14 per cent the previous year). NCSC estimated their defence capabilities had prevented around \$199 million of harm.<sup>6</sup> Reporting from [CERT NZ](#) shows that for individuals and other businesses it is estimated that incidents rose by 13 per cent in 2021 with a direct cost of \$16.8 million.<sup>7</sup>

Industry submissions on the topic for this briefing pointed to a mismatch between the rising threat of cyber attack and organisations’ investments in cyber security, and conflicting expectations of who should be responsible for cyber security. Government does not have all the tools to keep New Zealand secure. Businesses and individuals will need to become more security aware and take an active role in their own protection against cyber attacks.

### **In the next 10 to 15 years, we expect to see:**

- a growth in more complex and frequent cyber crime challenging our collective ability to respond
- more cyber attacks targeting technology critical for businesses, including supply chains
- emerging technologies and the evolving use of these continuing to lead to new ways of undertaking cyber attacks and cyber-enabled crime
- more country-backed cyber activity, and a blurring between country and independent malicious actors and their capabilities
- increased dark market platforms that buy and sell malicious software and information, bringing cyber attacks into the domain of non-technical people
- increased use of cryptocurrencies through weakly regulated financial systems in the money laundering aspect of cyber attacks, and
- an increase in the use of cyber attacks to support other activities that will affect national security such as disinformation and misinformation, foreign interference and trans-national organised crime.

## Preparing for the future now:

- **Collaboration** – [New Zealand's Cyber Security Strategy 2019](#) provides a framework for government-led action, in partnership with the private sector. The NCSC supports nationally significant organisations to protect their networks, and works to provide preventative advice on, and to deter, detect, and disrupt, the tuples of malicious cyber activity that could affect the country's national security or economic wellbeing. With cyber attacks being a form of organised crime and primarily profit-motivated, the Transnational Organised Crime Strategy deals with the organisation of illicit groups and the money laundering behaviours that sit beneath illicit profits, including those of cyber attackers.
- **Public information and engagement** – the NCSC, CERT NZ, NZ Police, and Netsafe receive and publish reporting and advisories.
- **International engagement** – this includes accession to the '[Budapest Convention](#)' on Cybercrime, which aims to strengthen international cooperation to address cybercrime, and engagement with close partners in the UN and in other fora to deter and disrupt malicious cyber activity. This recognises that cyber threats often relate to cross-border issues that require international solutions. The NCSC also works closely with international partners to build a cohesive line of cyber defence.
- **Law enforcement and intelligence** – agencies work with international partners, including by sharing information and intelligence to prevent cyber attacks at source in other countries. Police also seeks to take transnational asset recovery cases against cybercriminals in partnership with overseas law enforcement.

## Transnational organised crime

Transnational organised crime is a worldwide problem that undermines community wellbeing, governance, economic development and national security. Globally, the turnover of transnational organised crime groups is estimated to be USD\$3 trillion (or the equivalent to 4% of world GDP).<sup>8</sup>

Through their illegal activities, transnational organised crime groups often seek to gain power, influence and money through activities such as drug trafficking, migrant exploitation and human trafficking, fraud and corruption, and cybercrime. They operate in and through New Zealand, causing harm to people and businesses, and impacting trust in our institutions and reputation globally.

***“Reliable news sources over the past several years have reported a number of large-scale drugs busts, illegal weapons crimes etc. This is a sure sign that organised crime involving international players is alive and well in New Zealand at present, and there is every likelihood of further events of this type being detected in the next 12 months.”***  
**Survey respondent**

We think the increasing sophistication and pervasive global transnational connections enable organised crime. The connections work through border and trade systems, financial, shell company and trust and professional facilitator money laundering systems, and transnational demand and supply for illicit goods and services means the risks for our society from transnational organised crime are growing.

These impacts have the potential to affect the trust and confidence New Zealanders have in our public institutions and systems to respond. Eighty per cent of respondents to the National Security Public Survey felt there was a real threat of organised crime in the next 12 months, and 78 per cent felt the threat would continue for the next 10 years.

Transnational organised crime groups are governed by leaders that use bribes and intimidation and threats to control the groups' criminal activities and to protect illicit markets. Violence is seen as a necessary end point for control. Violence-as-a-service can be a paid service provided by illicit specialists and/or with illegal drugs we see physical violence, weapons and firearms as a means to support control of criminal activities. A number of those who made public submissions on the briefing topic highlighted the broader social implications of transnational organised crime, and cited gang-related violence and local drug distribution networks as key concerns.

### **In the next 10 to 15 years, we expect to see:**

- increasing exploitation of illicit markets wherever there are profits – in illegal drugs, illegal weapons and firearms, cybercrime and emerging technology tools, wildlife and natural resources, illicit migration and labour, unlawful importation of regulated goods, organised fraud and corruption. We expect transnational organised crime groups to continue adapting and evolving their methods of making financial gains from others' harm
- increasing Illicit drugs crime particularly affecting communities in New Zealand that are socially and financially disadvantaged, because they're targeted by criminal organisations as victims of crime but also as communities where transnational crime groups can recruit from<sup>9</sup>
- increasing sophistication in money laundering, including through shell companies and trusts worldwide, and through cash and cryptocurrencies. Unregulated cash markets in New Zealand help to fuel money laundering. They'll be quick to take advantage of gaps in regulation. Proceeds of crime find its way into business ventures, housing and luxury goods, causing significant harm to people who are buying houses and running businesses
- organised crime placing stress on New Zealand's border controls
- increasing efforts by transnational organised crime groups to influence, infiltrate, corrupt or bribe individuals and professionals and the public service to help further criminal activity and national security threat efforts. This threatens public trust and confidence in our institutions and New Zealand's reputation as a relatively corruption-free society and low risk trading partner.

### **Some things we're doing now**

- **Anti-money laundering and asset recovery** – intelligence sharing, working with transnational partners to prevent, detect, and deter organised crime.
- **Partnership across agencies, and with other countries to prevent threats offshore** – working overseas, including by sharing information and intelligence, to stop the threats, especially drugs and criminals from arriving in New Zealand.
- **Law enforcement** – cross-agency efforts to respond to organised crime, including the Cabinet mandated Resilience to Organised Crime in Communities work programme and Transnational Organised Crime Strategy.

## Foreign interference and espionage

New Zealand has been, and will continue to be, a target of foreign interference and espionage. This includes efforts by countries to, for example:

- gain access to our sensitive information, technology or intellectual property (such as from our businesses, universities and research institutions)
- use cyber attacks to steal information or to target infrastructure
- monitor, control or intimidate our communities, especially those with links to foreign countries, impacting on their rights and freedoms in New Zealand
- suppress or spread information (including via social media) that reflects their interests, including spreading disinformation
- influence democratically elected government representatives, political parties, and elections, and
- threaten or seek to coerce New Zealand's sovereignty or freedom to make certain decisions (for example, the threat to ban the import or export of certain goods between countries if a particular course of action is taken).

Globally, foreign interference is increasing, and New Zealand is not immune – we are seeing more examples of this.

Of those who made public submissions on the briefing topic:

- several saw foreign interference as a threat at both personal and national levels
- some were concerned that foreign countries could seek to divide ethnic communities in New Zealand (in the context of a weakening international order)
- just over a third referred to China, with concerns relating to interference in communities living in New Zealand and possible influence over New Zealand's political institutions, media and businesses, and
- some raised concerns about the need for New Zealand to diversify its trade markets further to avoid economic coercion in the future.

### **In the next 10 to 15 years, we expect to see:**

- emerging digital technologies changing the way that foreign countries seek to influence New Zealand (and neighbouring countries) and making it increasingly difficult for us to prevent it happening
- competition between countries increasingly featuring in the 'grey zone' between conflict and peace (including acts of foreign interference). There will be a greater risk of adversarial and coercive statecraft. Some countries will pursue their objectives secretly, while maintaining a degree of separation to avoid or minimise any negative reactions or responses internationally.



### Preparing for the future now:

- **Public Engagement** – boosting awareness and capability in entities that face foreign interference risks. The [government](#) is working with research organisations to help them manage the risks associated with sensitive technology, and providing guidance for elected officials and other sectors facing particular risks.
- **Sharing information and tools** – we are promoting greater transparency of foreign country activity and using [New Zealand’s Protective Security Requirements](#) to provide a framework that organisations can use to assess and strengthen their security arrangements.
- **Legislation** – we are ensuring that New Zealand has fit-for-purpose policies and laws to combat foreign interference and espionage. These include the Overseas Investment Act 2005, the Telecommunications (Interception Capability and Security) Act 2013, the export controls framework and our electoral financing laws.

## Terrorism and violent extremism

Responses to the National Security Public Survey highlighted that people are concerned that terrorism and violent extremism are evolving in New Zealand and will be more difficult to prevent in the future. Eighty per cent of survey respondents believed there was a real threat of a terrorist attack or act of violent extremism in New Zealand in the next 10 years, and 23 per cent considered terrorism the greatest threat to their communities.

Around the world, violent extremism is an evolving threat, driven by increasingly complex ideologies (ways of thinking) and terrorism continues to threaten the individuals’ safety and the communities’ sense of cohesion. The common drivers of violent extremism include polarisation within a society (deep divisions in opinions or beliefs), divisions between and within political, religious and identity groups, and real and perceived threats to group identities, values, power and status.

The internet continues to be abused by violent extremists – and their actions are increasingly enabled by online anonymity, accessibility, the privacy provided by encryption, and the challenges for governments, companies and civil society to keep ahead of technology. Violent extremists are using the internet to recruit, share knowledge, and plan and live-stream attacks, and their radicalising messages are enabling a range of ideologies to emerge with little or no warning.

[Ko tō tātou kāinga tēnei](#) – the report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain – highlighted the challenges of monitoring and countering extremism online, and reaffirmed the need for intelligence and security agencies to have the expertise, tools and capacity to support counter-terrorism efforts. These efforts are hugely assisted through access to the right information at the right time.

### In the next 10 to 15 years, we expect to see:

- increasing spread of hate and intolerant views online, especially violent hate speech and the use of violent extremist material, which will contribute to increasing threats of terrorism and violent extremism
- increasingly diverse extremist ideologies around the world, with new subsets and overlapping ideologies emerging.

## Preparing for the future now:

The aim of [New Zealand’s Countering Terrorism and Violent Extremism Strategy](#) is bringing our nation together to protect all New Zealanders from terrorism and violent extremism of all kinds. This strategy has four pillars, with work that includes:

- **Mōhio, understand** – establishing [He Whenua Taurikura](#), the National Centre of Research Excellence for Preventing and Countering Violent Extremism. The centre will provide independent, New Zealand-specific research on the causes of, and measures to prevent, terrorism and violent extremism.
- **Mahi tahi, work together** – the annual He Whenua Taurikura hui on preventing and countering violent extremism provides a focal point for working collectively as a nation to reduce the risk. Internationally New Zealand, alongside France, leads the global implementation of the Christchurch Call to Action to eliminate terrorist and violent extremist content online. Agencies also work with their international counterparts to contribute to global counter terrorism efforts.
- **Whakahōtaetae, prevent** – work is underway to develop a [Strategic Framework for preventing and countering violent extremism and radicalisation in Aotearoa New Zealand](#). Prevention work already underway includes He Aranga Ake, a multi-agency early intervention programme that is working with and supporting individuals displaying concerning behaviour.
- **Takatū, ready to respond and recover** – we are working in partnership to support the victims of attacks, as well as ensuring that we have fit-for-purpose laws on counter-terrorism, firearms, anti-money laundering and countering financing of terrorism.

## Pacific resilience challenges

Our geography, the close connectivity between our peoples, and the integration of our systems (for example in healthcare), means what happens in the Pacific region profoundly impacts New Zealand. A peaceful, stable, prosperous and resilient Pacific is critical for New Zealand’s national security. But our home region faces a range of interrelated and compounding security challenges.

Climate change will remain the single greatest threat to the livelihoods, security and wellbeing of the peoples of the Pacific, with increasingly severe impacts including sea-level rise, more extreme weather events, freshwater shortages and pressure on food stocks. An existential issue for some Pacific countries, climate change also risks exacerbating existing social, economic and security challenges.

Transboundary threats will continue to stress Pacific resilience including but not limited to: transnational organised crime; environmental crimes such as illegal logging, maritime pollution and illegal, unreported and unregulated fishing; biological threats including communicable diseases and invasive species; and more recent phenomena such as cybercrime, foreign interference and mis- and dis-information.

Respondents to the National Security Public Survey felt that New Zealand's influence in the Pacific is now under pressure, and believed the challenge will only increase in the next 10 to 15 years:

- 57 per cent said there is a real threat of other countries (from outside of the Pacific) endangering New Zealand's interests in the Pacific in the next 12 months
- 61 per cent saw the threat from other countries in the Pacific as being of concern in the next 10 years. This view was more common among Asian and Pasifika respondents.

We see strategic competition increasing in the Pacific, driven primarily by a rising China. In the future this competition will increasingly affect the security and sovereignty of our region and of Pacific nations. While New Zealand's national security has benefitted from a peaceful and stable region for much of the past seventy years, the signalled intent from actors outside the region to enhance their security footprints is resulting in greater security competition. This puts long-standing practices that have benefitted our region for so long at risk.

For example, in 2019, China publicly announced its intention to increase its military cooperation in the Pacific, aligning with its geopolitical, strategic and economic goals.<sup>10</sup> A range of other countries are also seeking to increase their Pacific engagement and presence for a variety of reasons and this expanded interest means increased complexity and competition.

#### **In the next 10 to 15 years, we expect to see:**

- intensifying strategic competition that poses challenges to the current foundations of regional security in the Pacific
- increasingly complex and advanced trans-boundary and non-state security challenges, such as transnational organised crime
- pressures on human security, including food and water security
- events and crises arising from climate change affecting multiple countries at the same time and will therefore require us to invest more in Pacific resilience and ability to respond.

#### **Preparing for the future now:**

- Our ongoing engagement within the Pacific reflects our deep connection with the region and its people and is driven by our desire for a peaceful, stable, prosperous and resilient neighbourhood.
- Aotearoa New Zealand's Pacific Resilience Policy reinforces the centrality of the Pacific in our identity and worldview, and acknowledges that the most enduring way we can address these complex challenges is through a holistic approach, in close partnership with other Pacific countries, to bolster long-term resilience.
- Recognising that national security risks always have a range of underlying social, political, economic and environmental drivers, we have committed to providing over \$1.8 billion in development assistance to Pacific countries between 2021 and 2024, in areas ranging from Pacific education, health systems, economic self-reliance, human rights and inclusive development, governance and democracy, infrastructure development, and much more.

- We have long provided support to bolster Pacific countries' own security capacity, for example in policing, customs, immigration and cyber security. Working with our close partners, particularly Australia, Aotearoa New Zealand also provides direct defence and security contributions into the region, including preventative activities such as fisheries patrols, and emergency responses – for example following natural disasters.
- We are also strong supporters of the regional architecture that enables Pacific responses to Pacific problems, we contribute to a wide range of regional bodies such as the Forum Fisheries Agency, the Pacific Transnational Crime Coordination Centre, the Pacific Islands Chiefs of Police, and more.
- *How* Aotearoa New Zealand works with Pacific partners will continue to be as important as *what* we do. Demonstrating the values of whanaungatanga, kotahitanga and kaitiakitanga and acknowledging the inherent mana of Pacific countries will strengthen our partnerships.

# National Security in Aotearoa New Zealand in 10 – 15 years

The risks to New Zealand's national security are increasing, complex and interrelated. To ensure we are in the best possible position to respond we need to engage with all New Zealanders.

We recognise that government agencies alone cannot deliver the range of responses required to address national security risks on the horizon and are seeking your views on what national security could look like in 10 to 15 years' time.

In this section we:

- look at some of the key competing demands and choices we face
- consider what we have heard we should be doing (through the topic consultation, National Security Public Survey and views from the wider national security sector) to engage better, and then
- present some ideas on what a bright future for national security could look like, and how we can evolve the ways we engage with an increasingly diverse New Zealand to turn those ideas into reality over the longer term.

We are interested in hearing your views, including your ideas on what happens next.

## The competing demands and choices we face

The competing demands and choices we face are those that will affect our ability to deliver a bright future for New Zealand's national security. New Zealanders over time will increasingly need to balance and prioritise these demands and choices, while recognising that people's needs, and expectations will change over time.

For example, we will need to balance and prioritise between:

- privacy, security and trust
- individual and collective needs and wants
- freedom of expression and countering hate speech, violent extremism and disinformation
- investing in response to current crises and building our capacity and capability to respond to future challenges, including preparing for high impact but rare events, and
- the different demands for public funding, including the likely differing public expectations of investments in national security. Public expectation and levels of support might not necessarily reflect the increasing risks and challenges to New Zealand's national security.

## We need to talk about national security

Events in recent years, such as war in Europe, a global pandemic, malicious actors targeting New Zealand, and a shifting world order, leaves us increasingly concerned about our national security.

We know New Zealanders are concerned too and want to know more, and some want to be more involved in how we respond – they believe we should act quickly given our own experiences and the changing threats on a global scale.

### In the National Security Public Survey:

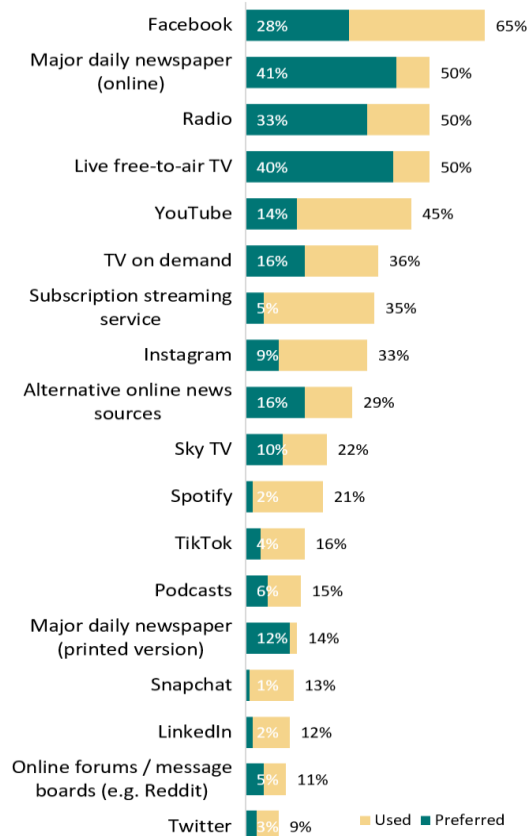
- most respondents (58 per cent) were interested in learning more about New Zealand's national security threats, challenges and opportunities
- 39 per cent were interested in having their say or being more involved in public discussions on national security, and
- 25 per cent knew where to find out more about New Zealand's national security issues but, only one in five thought our national security agencies shared enough information.

*"We should make an effort to engage everyday Kiwis in conversations about national security threats in New Zealand, and in particular reach out to communities that are most at risk from national security threats." Survey respondent*

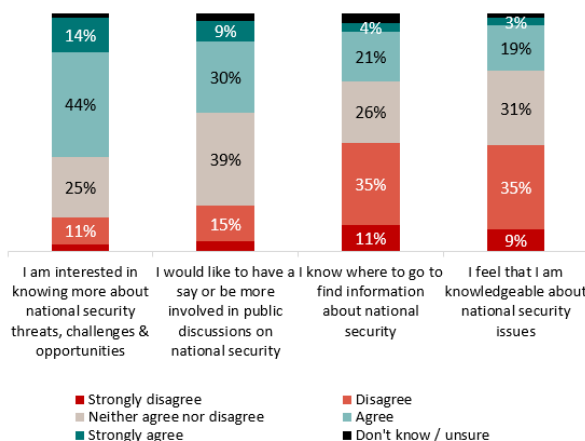
### New Zealand's national security agencies currently share enough information about national security with New Zealanders



### National Security Public Survey: Information Channels used and Preferred Channel for Information on threats



### Thinking again about all the threats we have covered so far, do you agree or disagree with each of the following statements?



Source: National Security Public Survey 2022

Many submitters on the briefing topic commented on what they see as an overall lack of transparency and accessibility in New Zealand's national security agencies. They wanted to know more about the threats most concerning to them. Survey respondents said they preferred to receive information on national security threats via online newspapers and free-to-air TV.

Submitters and survey respondents also:

- identified practices that were making information hard to get. These included limited explanations of the national security threats, why the threats were relevant and how New Zealand should respond
- commented on the complexities of having many agencies involved in national security, and
- said that some people and communities are afraid of engaging with national security agencies because of their past experiences.

There were suggestions that national security agencies could improve their accessibility by:

- organising meaningful outreach programmes (which would help and encourage members of the community to get involved in protecting New Zealand's national security)
- creating and publishing an engagement strategy, and
- developing a roadmap to guide the development of a partnership with the public on national security.

## Confidence in the government agencies' ability to respond varies

The National Security Public Survey revealed that New Zealanders' confidence in government agencies' ability to provide security and protection varies according to the type of threat.

When asked how government agencies could build public confidence, survey respondents highlighted the need for agencies to:

- respond quickly
- be prepared, and
- keep the public educated and informed.

## What could a bright future for national security could look like?

We have identified ten features we think would support a brighter future for New Zealand's national security over the next 10 to 15 years. They would help us better prepare and respond to the risks and challenges presented in this briefing. Described briefly and at a high level, these features are options for potential further exploration.

These features are founded on trust, confidence, and social cohesion – they would enhance our domestic resilience and support us to act early and protect our national security interests.

These features overlap and interrelate, supporting us to respond quickly and collectively, drawing on shared knowledge of the risks we have identified through conversations with politicians, Māori, government officials, academics, businesses, media, community leaders and members of the public.

We are already making progress, for example, through the development of New Zealand's first National Security Strategy and a review of our national security system in response to the findings and recommendations of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain. However, we think additional opportunities exist and are worthy of exploration.

### The key features of a bright future include:

- **Transparent and accessible public information** – sharing information and making it easy for people to access and read it will build the public's knowledge of our national security risks, what we are doing about them and how they can help to reduce and respond to them. This in turn will help to correct information imbalance and support people's participation.
- **National security sector stewardship** – National security agency Chief Executives are supported to collectively take a stronger stewardship role, to proactively look ahead and provide advice and take action on future challenges and opportunities, to help current and successive governments.
- **Strengthened political leadership on national security** – consistent with the recommendations of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, government ministers are well informed and there is "more debate on, and cross-party support for, national security issues."<sup>11</sup>
- **International partnerships that grow and strengthen our national security** – recognising that current and future national security threats may have global origins requiring international engagement and cooperation to address; proactively sharing intelligence, insights and experiences and working together with those who share our values, will be important to support global and regional security, and protect our country's interests.
- **A national security sector that reflects the diversity of our nation and is adaptable and capable of responding to future challenges** – in the future, a well-resourced national security sector with a range of capabilities and sufficient capacity will be able to respond to complex national security issues happening at the same time. The diversity of the sector will change as New Zealand changes, and strategies to promote diversity and inclusion are embedded. We acknowledge the Royal Commission of Inquiry specified the need for a well-resourced national intelligence and security agency, mandated through legislation, to be responsible for security and intelligence leadership.



- **Open debate among, and advice from, experts outside government** – academic institutions and think tanks on national security receive the sustainable funding they need to provide independent advice and grow our understanding of the threats we might face in the future, and how we can meet them.
- **Active and engaging media coverage** – media coverage of national security issues supports open debate on national security threats, potential trade-offs and the strengths and weaknesses in approaches. Coverage reflects a diversity of views from all parts of New Zealand society and while articulating threats and challenges, also recognises the resilience of our communities and celebrates where challenges have been met collectively as a whole country.
- **Recognising and working with partners outside of government** – we will have a clear understanding of the experts and expertise available in our communities to help mitigate and respond to national security challenges (we have heard that our business sector and communities have a vast range of knowledge and skills and are ready and willing to support responses to national security threats).
- **Communities that feel enabled and empowered to engage with the national security sector** – we recognise the importance of building New Zealanders’ trust and confidence in each other and our institutions. Communities are encouraged, supported and funded to engage in national security matters through information sharing and capability building as a ‘business as usual’ feature in our national security sector.
- **Trusted and accountable institutions** – a national security system that has the trust and confidence of the people it serves (that is, it has a ‘social licence to operate’) can operate more effectively than a system that does not.

## What happens next?

This briefing is intended to support ongoing conversations about our national security and the ways we can engage an increasingly diverse Aotearoa New Zealand on national security risks, challenges and opportunities. We welcome and encourage your ideas and feedback on the draft briefing – particularly on:

- The **ten features outlined in the briefing** that could support Aotearoa New Zealand's national security, and
- **Ideas you have** to support Aotearoa New Zealand's national security.

## How you can share your feedback

You can share your thoughts through the online feedback form:

<https://consultation.dPMC.govt.nz/long-term-insights-briefing/draft-ltib-consultation>

We will consider all the feedback before finalising the briefing. The final briefing will be shared with relevant Ministers and tabled in Parliament.

## Publishing your feedback

A summary of public feedback will be published on the DPMC website. While we do collect submitters' names and contact information, please note that personal contact details will *not* be shared or published.

All responses provided may be released under the Official Information Act 1982. If you do not want your response to be published, please note this in your submission together with a reason why your submission should be withheld.

*Thank you for your time, and for sharing your thoughts and ideas.*

## Annex A – Glossary

**Cyber attack** – a deliberate exploitation of information systems to cause harm.

**Cybercrime** – Crimes that are committed through the use of computer systems, and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing

**Disinformation** – Information that is false or modified information knowingly shared to cause harm or achieve a broader aim

**Espionage** -refers to a range of clandestine activities undertaken to collect information, materials or capabilities for the purpose of obtaining an advantage over a rival.

**Foreign interference** – An act by a foreign country, or its proxy, intended to influence, disrupt or subvert a country's national interests by covert, deceptive or threatening means. The goal is to avoid or subvert ordinary approaches to international engagement and gain advantage. While countries including New Zealand often take economic or diplomatic actions to further their interests, it is the use of deception and coercion that poses risks to national security.

**Malicious actor** – A person or organisation that deliberately causes harm.

**Misinformation** – information that is false or misleading, but not created or shared with the intention of causing harm

**National security** – [under review] A condition that permits New Zealanders to go about their daily lives confidently, free from fear and able to make the most of opportunities to advance our way of life. New Zealand currently adopts a broad definition of national security. This reflects our exposure to a variety of hazards and threat-based security risks, ranging from earthquakes, wildfire and tsunamis to terrorism, foreign interference and espionage, and corruption. These risks are an inherent part of the world in which we live and managing them is complex.

**Ransomware** – Software that prevents people accessing their files or computer systems unless they pay ransoms.

**Rules-based international order** – A worldwide system of 'fair play', made up of rules, principles and organisations that support countries to work together, and in turn encourages peaceful, predictable and cooperative behaviour.

**Social cohesion** – Where everyone feels safe, valued and heard, has a strong sense of belonging and can participate fully in society. A socially cohesive society is one in which all individuals and groups have a sense of belonging, social inclusion, participation, recognition and legitimacy.

**Terrorism** – Acts that include (but are not limited to) acts that cause death or serious bodily injury and are intended to intimidate a population or compel the government to do (or not do) certain things.

**Transnational organised crime** – is crime that operates across national borders, or crime that is carried out in one country, but which has strong links to other countries.

**Violent extremism** – the justification of violence with the aim of radically changing the nature of government, religion, or society. This violence is often targeted against groups seen as threatening violent extremists' success or survival or undermining their world view.

## Annex B – Endnotes

- <sup>1</sup> These agencies are the Department of the Prime Minister and Cabinet, Ministry of Foreign Affairs and Trade, New Zealand Security Intelligence Service, Ministry of Defence, Government Communications Security Bureau, New Zealand Customs Service, New Zealand Defence Force, New Zealand Police, and Ministry of Business, Innovation and Employment.
- <sup>2</sup> The survey report is available on the DPMC website <https://dpmc.govt.nz/our-programmes/national-security/national-security-long-term-insights-briefing/2022-ipsos-national>. This online survey was conducted by IPSOS New Zealand between 11 February – 2 March 2022. Fieldwork overlapped with the Russian invasion of Ukraine and Parliament Protest Activity. It is possible these events impacted people’s responses.
- <sup>3</sup> For more detailed information about New Zealand’s National Security System. See <https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security/new-zealands-national-security>
- <sup>4</sup> Stats NZ (2021) National ethnic population projections: 2018(base)-2043. See <https://www.stats.govt.nz/information-releases/national-ethnic-population-projections-2018base-2043>
- <sup>5</sup> Microsoft (June 2022). Defending Ukraine: Early Lessons from the Cyber War. See <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>
- <sup>6</sup> National Cyber Security Centre, Cyber Threat Report 2022/21. See <https://www.ncsc.govt.nz/newsroom/ncsc-cyber-threat-report-shows-rise-in-malicious-attacks-on-new-zealand/>
- <sup>7</sup> CERT NZ. 2021 Report Summary. See <https://www.cert.govt.nz/about/quarterly-report/2021-report-summary/>
- <sup>8</sup> Transnational Organised Crime in New Zealand: Our Strategy 2020 – 2025. See <https://www.police.govt.nz/sites/default/files/publications/transnational-organised-crime-in-new-zealand-our-strategy-2020-to-2025.pdf>
- <sup>9</sup> Stats NZ (2012). Vulnerable children and families: Some findings from the New Zealand General Social Survey. See <https://www.stats.govt.nz/assets/Uploads/Retirement-of-archive-website-project-files/Reports/Vulnerable-children-and-families-Some-findings-from-the-New-Zealand-General-Social-Survey/vulnerable-children-and-families.pdf>
- <sup>10</sup> New Zealand Ministry of Defence (2021) Defence Assessment, He Moana Pukepuke E Ekengia E Te Waka, A Rough Sea Can Still be Navigated. See <https://www.defence.govt.nz/assets/publication/file/Defence-Assessment-2021.pdf>
- <sup>11</sup> Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019. Section 2.3 Paragraph 24, 2. Recommendations to improve New Zealand's counter-terrorism effort. See <https://christchurchattack.royalcommission.nz/the-report/findings-and-recommendations/chapter-2-recommendations-to-improve-new-zealands-counter-terrorism-effort/>