Ko tō tātou kāinga tēnei

Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019

Volume 3: Part 8

ROYAL COMMISSION OF INQUIRY INTO THE TERRORIST ATTACK ON CHRISTCHURCH MOSQUES ON 15 MARCH 2019

TE KŌMIHANA UIUI A TE WHAKAEKE KAIWHAKATUMA I NGĀ WHARE KŌRANA O ŌTAUTAHI I TE 15 O POUTŪ-TE-RANGI 2019

26 November 2020

Ko tō tātou kāinga tēnei

Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019

Published 26 November 2020

978-0-473-55326-5 (PDF)
978-0-473-55325-8 (Soft cover)

This document is available online at:
www.christchurchattack.royalcommission.nz

Printed using ECF and FSC certified paper that is also Acid free and biodegradable.

Part 8

Assessing the counter-terrorism effort

Chapter 1: Introduction

1 Earlier in our report we explored what relevant Public sector agencies knew about the individual (see *Part 6: What Public sector agencies knew about the terrorist*). We concluded that the relevant Public sector agencies involved in the counter-terrorism effort did not hold information on the threat posed by the individual and of his planning and preparation for the terrorist attack on 15 March 2019. In *Part 7: Detecting a potential terrorist*, we explored the ways in which the individual could have come to the attention of the relevant Public sector agencies, but did not.

2 In this Part we focus on what we call the counter-terrorism effort – that is how Public sector agencies detect terrorists and disrupt their organisation, planning, preparation and attacks. This Part looks at the continuum of counter-terrorism roles and activity (including countering violent extremism). The promotion of social cohesion and social inclusion, which supports any broad comprehensive counter-terrorism strategy, is discussed in *Part 9: Social cohesion and embracing diversity*.

3 Our Terms of Reference required us to make findings on:

> 4(c) whether relevant [Public] sector agencies failed to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats;
>
> (d) whether any relevant [Public] sector agency failed to meet required standards or was otherwise at fault, whether in whole or in part; and
>
> (e) any other matters relevant to the purpose of the inquiry, to the extent necessary to provide a complete report.

4 We also had to consider whether to make recommendations about the counter-terrorism effort.

5 In the following chapters of this Part we discuss:

a) the setting in which the counter-terrorism effort has operated over the past two decades (chapter 2);

b) leadership and oversight of the counter-terrorism effort (chapter 3) and assessment of the terrorism threatscape (chapter 4);

c) the counter-terrorism efforts of the New Zealand Security Intelligence Service (chapter 5), New Zealand Police (chapter 6), the Government Communications Security Bureau (chapter 7) and the border agencies (chapter 8);

d) interagency activities – information sharing (chapter 9), target discovery (chapter 10), online capacity and capability (chapter 11) and the relationship between New Zealand Police and the New Zealand Security Intelligence Service (chapter 12);

e) two statutes central to the counter-terrorism effort – the Terrorism Suppression Act 2002 (chapter 13) and the Intelligence and Security Act 2017 (chapter 14);

f) our evaluation of the counter-terrorism effort (chapter 15);

g) our findings (chapter 16); and

h) questions asked by the community (chapter 17).

6 As we will explain, the intelligence and security agencies were at a low ebb in 2013–2014. A 2014 *Performance Improvement Framework* review of the New Zealand Intelligence Community was considered one of the worst reviews of its kind amongst New Zealand Public sector agencies. Recognition of significant capability and organisational weaknesses across the agencies resulted in the Strategic Capability and Resourcing Review. In 2016 Cabinet agreed to add considerable additional funding ($178.7 million over four years) into the intelligence and security agencies (including a small amount of additional funds for the Department of the Prime Minister and Cabinet). This additional money started to become available in the 2016–2017 financial year.

7 Our primary – although not exclusive – focus in the chapters that follow is on the period between 2014 and 2019, with particular emphasis on the last three years. The 2014 *Performance Improvement Framework* review provides a useful snapshot of the state of the New Zealand Intelligence Community. And, beginning in the 2016–2017 financial year, the additional funding from the Strategic Capability and Resourcing Review was approved to enable the intelligence and security agencies to rebuild capacity and capability.

8 There are three additional themes that emerged as the result of our inquiries:

a) New Zealand had not been the subject of recent terrorist attacks. The apparently low threat of terrorism, controversies associated with the intelligence and security agencies and associated public suspicions as to their activities and utility, meant that the agencies had limited social licence, political support and funding.

b) Leadership and coordination of the counter-terrorism effort was limited with the relevant Public sector agencies operating largely independently and in parallel. In the chapters that follow, we discuss the efforts that were made to address this and what these efforts did and did not achieve.

c) There was a focus on Islamist extremist terrorism as the presenting threat and only very limited resources were dedicated to understanding other terrorist threats. We explain why this was so and make findings about it.

9 As we described in *Part 4: The terrorist*, the individual attempted to maintain operational security for a sustained period and was able to fund his activities with his own resources. He was a lone actor, who did not need to involve or rely upon others in order to carry out his plans. So, even if substantial additional resource had been dedicated to non-Islamist extremist threats, and to extreme right-wing threats, it is very unlikely that the individual's activities, including his plans and preparation, would have been discovered by the relevant Public sector agencies.

2.1 Overview

1 In this chapter we provide background to the counter-terrorism effort as it has evolved over the last two decades.

2 In what follows, we:

a) describe the changing threatscape since 2001 and the impact of these changes on New Zealand;

b) discuss how the nature of terrorist attacks, and terrorists themselves, have changed and adapted over time;

c) outline the controversies and other events that have affected Public sector agencies involved in the counter-terrorism effort;

d) list the reviews of components of the national security system over the last twenty years; and

e) describe the Strategic Capability and Resourcing Review, which resulted in significant investment to improve the capability and capacity of the New Zealand Intelligence Community over the last four years.

2.2 The changing threatscape

11 September 2001 and the global terrorist threat

3 The Al Qaeda terrorist attacks against the United States of America on 11 September 2001 transformed the perception of terrorism throughout the world. But terrorism is not a new phenomenon. While there is no universally agreed definition of terrorism,[1] it has been part of history since ancient times. Some of the terrorism trends discussed in this and other chapters started well before 2001.[2]

4 There is no easy way to track terrorism globally. What is defined and reported as terrorism can vary significantly across countries. In states where there is some form of armed civil conflict it can be difficult to distinguish between terrorism and insurgency (civil wars in Syria and South Sudan are recent examples).[3] Even so, there are several credible open-source databases that measure terrorism globally.[4] Their data reveals a gradual increase in the frequency of terrorist attacks from 1970–1992, then decline until 2004. From 2014 there has been a dramatic rise in the number of terrorist attacks worldwide. The regions most affected by this sharp increase are South Asia, the Middle East, and North Africa. They collectively account for around 70 percent of terrorist attacks in the past ten years.

[1] One researcher found at least 212 definitions of terrorism in use throughout the world. See Jeffery D Simon *The Terrorist Trap* (Indiana University Press, Bloomington, 1994) at page 29.

[2] Khusrav Gaibulloev, Todd Sandler and Charlinda Sanifort "Assessing the Evolving Threat of Terrorism" (May 2012) 3(2) *Global Policy* at page 16.

[3] Anthony H Cordesman *Global Trends in Terrorism 1970-2016* (Center for Strategic and International Studies, 2017) at pages 4–6.

[4] The most comprehensive of which is the University of Maryland's Global Terrorism Database.

5 Terrorism in Western countries is much less common. In comparatively recent times it has included left-wing terrorism (for example, the Red Brigades in Italy in the 1970s), nationalist or separatist terrorism (for example, Northern Ireland in the 1970s and 1980s) and extreme right-wing terrorism (for example, the Oklahoma City bombing in 1995). And before 11 September 2001 there were examples of Islamist extremist terrorism against Western targets, such as the 1993 bombing of the World Trade Center.

6 The attacks on 11 September 2001 were a "watershed" terrorist event. The response to the terrorist attacks of that day significantly affected the global security environment.[5] Considerable international attention and effort was focused on Islamist extremism and states that were thought to finance and harbour terrorists. Shortly after the attacks, the United States of America commenced its twenty year "War on Terror", fought predominantly in Afghanistan and Iraq.

7 After 11 September 2001, countries around the world reallocated significant resources to counter-terrorism, both international and domestic. Terrorism became a conspicuous feature of the international security environment. The United Nations, which had previously engaged with terrorism only tentatively, acted swiftly. The United Nations Security Council adopted Resolution 1373, which imposed a number of binding obligations on states, including tighter border controls and called for enhanced international cooperation against terrorism. This Resolution underpins the global legal framework for the prevention and suppression of terrorism.[6]

8 The events of 11 September 2001 were followed by other terrorist attacks, some of which were not undertaken by Islamist extremists. The list below is not exhaustive, and focuses on terrorist attacks that would have been of particular interest to intelligence and security agencies in the West. We recognise that terrorist attacks have been far more numerous in Africa, the Middle East and South Asia. Relevant for our purposes, the terrorist attacks listed below were formative in shaping the security arrangements of Five Eyes countries, including New Zealand.

[5] Khusrav Gaibulloev and Todd Sandler "What We Have Learned about Terrorism since 9/11" (June 2019) 57(2) *Journal of Economic Literature*.

[6] Walter Gehr "The Counter-Terrorism Committee and Security Council Resolution 1373" (December 2004) 4(1 and 2) *United Nations Office on Drugs and Crime: Forum on Crime and Society*.

Table 9: Terrorist attacks since 11 September 2001 that shaped Five Eyes countries' security arrangements

Date	Event	Fatalities[7]
12 October 2002	Bombings in Bali, Indonesia	202 people killed, including 2 New Zealanders
11 March 2004	Bombings in Madrid, Spain	193 people killed
7 July 2005	Bombings on the London underground and bus transport network in London, United Kingdom	52 people killed, including 1 New Zealander
11 July 2006	Bombings of trains in Mumbai, India	209 people killed
27 July 2008	Bombing in Istanbul, Turkey	17 people killed
5 November 2009	Mass shooting at Fort Hood, Texas, United States of America	13 people killed
22 July 2011	Bombing in Oslo and mass shooting on Utøya Island, Norway	77 people killed
11 March 2012	Mass shooting in Montauban and Toulouse, France	7 people killed
5 August 2012	Mass shooting at the Sikh Temple in Oak Creek, Wisconsin, United States of America	6 people killed
15 April 2013	Bombings at the Boston marathon, Massachusetts, United States of America	3 people killed
24 May 2014	Mass shooting at the Jewish Museum in Brussels, Belgium	4 people killed
15 December 2014	Hostage taking and shooting at the Lindt Café in Sydney, Australia	2 people killed
7–9 January 2015	Mass shootings in Île-de-France, Paris (including at the Charlie Hebdo office), France	17 people killed
14–15 February 2015	Mass shooting in Copenhagen, Denmark	3 people killed

[7] Fatalities do not include perpetrators.

Date	Event	Fatalities
26 June 2015	Mass shooting at a tourist resort in Sousse, Tunisia	38 people killed
17 July 2015	Mass shooting at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, United States of America	9 people killed
13–14 November 2015	Bombings and mass shooting in Paris, France	130 people killed
2 December 2015	Mass shooting in San Bernadino, California, United States of America	14 people killed
22 March 2016	Bombing at Brussels airport and subway, Belgium	32 people killed
16 June 2016	Knife attack in Birstall, United Kingdom	1 person killed, Jo Cox – British Member of Parliament
14 July 2016	Vehicle attack in Nice, France	86 people killed
19 December 2016	Vehicle attack at Berlin Christmas market, Germany	12 people killed
29 January 2017	Mass shooting at Quebec City Mosque, Canada	6 people killed
5 March 2017	Vehicle attack at Westminster Bridge, London, United Kingdom	5 people killed
7 April 2017	Vehicle attack in Stockholm, Sweden	4 people killed
3 June 2017	Vehicle and knife attacks at London Bridge and Borough Markets, London, United Kingdom	7 people killed
19 June 2017	Vehicle attack at Finsbury Park Mosque, United Kingdom	1 person killed
17 August 2017	Vehicle and knife attacks in Barcelona and Cambrils, Spain	16 people killed

Date	Event	Fatalities
22 May 2017	Bombing at the Manchester Arena, United Kingdom	22 people killed
23 April 2018	Vehicle attack in Toronto, Canada	10 people killed
27 October 2018	Mass shooting at the Pittsburgh Tree of Life Synagogue, Pennsylvania, United States of America	11 people killed
9 November 2018	Knife attack in Melbourne, Australia	1 person killed

9 Some of the terrorist attacks referred to above were mass shootings. In many countries – the United States of America in particular – there have been mass shootings that could conceivably have had political motivations but were not considered terrorist attacks as the motivation was not clear. Mass shootings without political motivations can include, for example, school shootings or familicide (the perpetrator killing their family).

10 In the last two decades, many planned terrorist attacks were disrupted by intelligence and security or law enforcement agencies. For example, between 2014 and 2019, there were 16 major terrorist plots reported as prevented in Australia. And in the two years after the March 2017 Westminster Bridge attack in London, authorities in the United Kingdom disrupted 22 terrorist plots. Not all attacks prevented by authorities are reported, so there are likely to be many more that the public are not aware of.

Table 10: Recent instances of disrupted terrorist attacks

Date	Event
August 2006	United Kingdom police uncovered a terrorist plot to detonate liquid explosives disguised as canned drinks carried on board planes travelling from the United Kingdom to the United States of America and Canada.
September 2009	Eight people affiliated with Al Qaeda were arrested for a plot to bomb the New York City subway system and other targets.
March 2012	Indonesian police shot dead five people who were plotting to attack and bomb targets in Bali.
August 2016	Australian police arrested a right-wing extremist who had plotted terrorist attacks on Victorian Trades Halls and other "leftist" centres in Melbourne.

11 New Zealand has not been immune from terrorism or mass shootings in its recent history. In 1985, Greenpeace's ship the *Rainbow Warrior* was bombed in a state-led terrorist attack while it was moored in Auckland harbour.

Table 11: Recent mass shootings in New Zealand

Date	Event	Fatalities
13–14 November 1990	Mass shooting in Aramoana, Otago	14 people killed
20 May 1992	Mass shooting in Paerata, Franklin District	7 people killed
20 June 1994	Mass shooting in Dunedin, Otago	5 people killed
8 February 1997	Mass shooting in Raurimu, King Country	6 people killed

Impact of the changing threatscape on New Zealand

12 The events set out in the tables above had effects on New Zealand. New Zealand recognised that there was a new security environment, to which it needed to respond. It did so in several ways. It contributed to international military operations (in Afghanistan, for example). It strengthened its intelligence and security links with international partner countries. It supported and implemented various United Nations resolutions and conventions related to counter-terrorism.

13 New Zealand expanded its counter-terrorism effort between 2001 and 2004. Public sector agencies received a total of almost $30 million for initiatives such as extra security at airports and increased intelligence capability for both the New Zealand Security Intelligence Service and New Zealand Police.[8] The Terrorism Suppression Act 2002 was enacted quickly. It created specific new terrorist offences and created a terrorist entity designation regime to implement New Zealand's international obligations. In 2005, the *National Counter-Terrorism Plan* was finalised. For many years, that was New Zealand's principal statement about counter-terrorism, but it was never made available to the public.[9] It set out, among other things, the counter-terrorism risk management framework, the counter-terrorism coordination system, and the role of intelligence, threat assessment, strategic assessment and legislation in the counter-terrorism effort. Around the same time a strategic aim for New Zealand's counter-terrorism effort first appeared in policy documents – that New Zealand is "neither the victim nor the source of an act of terrorism".[10]

2.3 The changing nature of terrorist attacks

14 The international terrorist attacks perpetrated in the 1990s and early 2000s were primarily carried out by groups in terrorist cells. They were often sophisticated, carefully planned well in advance, involved multiple perpetrators and targets and used advanced attack methods, such as explosives. Groups such as Al Qaeda were concerned with "ever-bigger and more dramatic attacks"[11] and were discerning about whom they recruited and what targets they chose to attack.[12]

[8] Office of the Controller and Auditor-General *Managing Threats to Domestic Security* (October 2003) at page 7.

[9] Simon Murdoch *Counter-Terrorism: A review of the New Zealand CT landscape* (Department of the Prime Minister and Cabinet, May 2013).

[10] Simon Murdoch, footnote 9 above at pages 4-6.

[11] Steven Metz "Can the U.S. Counter Terrorism's Shift to Decentralised and Radicalized Violence?" (29 July 2016) *World Politics Review*.

[12] Colin P Clarke and Steven Metz *ISIS vs Al Qaida: Battle of the Terrorist Brands* (RAND Corporation, Santa Monica, California, August 2016).

15 In the years following 11 September 2001, terrorist methods evolved. For example, suicide terrorist attacks became more prevalent. Such attacks can have a much higher death and injury toll than conventional bombing attacks.[13] They coincided with what some experts saw as a move to more indiscriminate terrorist violence against civilian targets. Some experts have drawn a distinction – although it is an oversimplification – between "old terrorism" and "new terrorism".[14] Before 1990, most terrorist groups were left-wing or nationalist or separatist. This "old terrorism" was seen to be more discriminate, with terrorist groups at least sometimes carefully selecting targets that represented the authority they opposed – for example, military or government buildings. The strategy was to limit civilian deaths and injuries, as this would diminish support for their cause.[15] By contrast, Al Qaeda wanted maximum publicity *through* carnage from the 11 September 2001 attacks. Some argue that such widespread targeting of civilians is a feature of "new terrorism".[16]

16 Following the loss of key leaders and safe havens, Al Qaeda's power and influence fell considerably from its peak in the aftermath of 11 September 2001. Dā'ish emerged from the remains of Al Qaeda's affiliate in Iraq in 2003–2004. While it faded into obscurity for a period, it re-emerged in 2011 and took advantage of wars in Iraq and Syria to carry out attacks and recruit more followers. Dā'ish achieved global recognition around 2014. At its height, Dā'ish held about a third of the territory in Syria and 40 percent in Iraq.[17]

17 As intelligence and security agencies and law enforcement became better at detecting and disrupting large-scale terrorist plots, terrorists turned to smaller-scale, less sophisticated attacks.[18] Islamist extremist terrorist groups decentralised and became less discerning about whom to recruit. Groups such as Dā'ish have favoured an approach of "killing as many helpless victims as [they] can in low tech ways",[19] primarily by encouraging lone actors to commit terrorist attacks in their own countries. Such terrorist attacks killed civilians who were enjoying leisure time, perhaps at a concert, a Christmas market or a café. The aim was to instil widespread public fear.

[13] Khusrav Gaibulloev and Todd Sandler, footnote 5 above at page 279.

[14] Max Abrahms, Matthew Ward and Ryan Kennedy "Explaining Civilian Attacks: Terrorist Networks, Principal-Agent Problems and Target Selection" (February 2018) 12(1) *Perspectives on Terrorism* at page 23.

[15] Alexander Spencer "Questioning the Concept of 'New Terrorism'" (January 2006) *Peace, Conflict & Development* at page 7.

[16] Max Abrahms, Matthew Ward and Ryan Kennedy, footnote 14 above at page 23.

[17] Wilson Center *Timeline: the Rise, Spread, and Fall of the Islamic State* (28 October 2019).

[18] Clare Ellis, Raffaello Pantucci, Jeanine de Roy Van Zuijdewijn, Edwin Bakker, Benoit Gomis, Simon Palombi and Melanie Smith *Lone Actor Terrorism: Final Report* (Royal United Services Institute for Defence and Security Studies: Countering Lone-Actor Terrorism Series, London, April 2016) at page 1.

[19] Steven Metz, footnote 11 above.

18 As the list of attacks above demonstrates, Islamist extremist terrorism was not the only terrorist threat in the last two decades. Right-wing extremist terrorism was exemplified by the Oslo terrorist's attack in 2011. This threat materialised again with the Charleston church shootings of 2015 and the Quebec City Mosque shootings of 2017. All of these attacks were committed by lone actors. The latter two terrorist attacks also demonstrate a tendency of those right-wing extremist terrorists who are hostile to adherents of particular religions or minorities to target their places of worship.

19 The methods used by the extreme right-wing have some similarities with those used by Islamist extremists. Some aspects of the rhetoric are also comparable, such as threats posed by "foreign" elements undermining a particular way of life and culture, the legitimacy of violence to combat the perceived threat and seeking support and mobilisation across national borders. But, for a long time, right-wing extremism was not seen (and in some countries is still not seen) to be a threat to national and international security in the way that Islamist extremism is. In part this is because people exhibiting right-wing extremism are often not ethnically, socially or culturally distinct from the majority of the population.

The influence of technology

20 The internet has become a key platform for terrorist radicalisation and recruitment. It has been described as providing a surrogate community where people's beliefs are developed and reinforced and individuals can become radicalised without a need to establish direct face-to-face contact. The internet can also act as a training tool and is a place where many potential terrorists can obtain practical information.[20] The internet offers a global audience for extremists who wish to spread their views. These trends accelerated as the use of mobile technology proliferated after 2010.

21 Far right groups were some of the earliest to engage in politics online and to use the internet for political purposes (see Part 2, chapter 5). Recent events have underscored their increasingly pervasive use of the internet, including the upsurge of hateful content online in 2015 and 2016 associated with the 2016 United States of America presidential election, the Brexit referendum, a series of Islamist extremist terrorist attacks and the arrival of large numbers of refugees to Europe from Africa, the Middle East and Central Asia (fleeing war, famine, economic depression and political oppression in their home countries). The far right has exploited the fear and anger generated by Islamist extremist terrorist attacks and the refugee crisis to recruit new followers, usually via the internet.[21]

[20] Clare Ellis, Raffaello Pantucci, Jeanine de Roy Van Zuijdewijn, Edwin Bakker, Benoit Gomis, Simon Palombi and Melanie Smith, footnote 18 above at page 2.

[21] Maura Conway, Ryan Scrivens and Logan Macnair *Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends* (International Centre for Counter-Terrorism – The Hague, October 2019) at page 2.

22 Islamist extremists have also been adept at exploiting digital technology. In the early 2000s Al Qaeda identified the "media war" as one of the strongest methods for promoting its organisation's objectives and it allocated significant resources to this end. But an even more sophisticated use of digital media was pioneered by Dā'ish.[22] In 2014, it launched "the most advanced, massive and probably the most efficient cyber jihad campaign ever".[23] Due in part to the effectiveness of its propaganda, Dā'ish has been far more successful than other terrorist groups, such as Al Qaeda, in recruiting individuals within Western nations to its cause – either as foreign terrorist fighters or domestic terrorists.[24] At the peak of its media activity in 2014, some fifty thousand pro-Dā'ish accounts were estimated to be active on Twitter.[25]

Technology has made terrorists hard to detect

23 Terrorist groups' use of the internet provides opportunities and challenges for intelligence and security agencies.

24 There are opportunities to access detailed information remotely about the lives, contacts and plans of potential terrorists. But technology is also creating challenges for intelligence and security and law enforcement agencies. Readily available communications platforms – such as Telegram, Signal and WhatsApp – employ end-to-end encryption to secure users' messages. Apple iPhones are now encrypted by default and not even Apple can unlock a user's encrypted phone. The availability of VPNs or Tor browsers, as well as the dark web, allows individuals to access and/or download online content without leaving easily traceable digital footprints.[26] In these ways, technology is also making it harder to detect potential terrorists.

The rise of lone actor terrorist attacks

25 Lone actor terrorism has been defined as:

> *The threat or use of violence by a single perpetrator ... not acting out of purely personal-material reasons, with the aim of influencing a wider audience, and who acts without any direct support in the planning, preparation and execution of the attack, and whose decision to act is not directed by any group or other individuals (although possibly inspired by others).*[27]

[22] Ilan Berman "Technology is making Terrorists more Effective – And Harder to Thwart" *The National Interest* (United States of America, 22 February 2019) https://nationalinterest.org/feature/technology-making-terrorists-more-effective—and-harder-thwart-45452.

[23] Miron Lakomy "Cracks in the Online 'Caliphate': How the Islamic State is Losing Ground in the Battle for Cyberspace" (June 2017) 11 *Perspectives on Terrorism* at page 40.

[24] Heather J Williams, Nathan Chandler and Eric Robinson *Trends in the Draw of Americans to Foreign Terrorist Organisations from 9/11 to Today* (RAND Corporation, Santa Monica, California, 2018).

[25] Heather J Williams, Nathan Chandler and Eric Robinson, footnote 24 above at page 20.

[26] Ilan Berman, footnote 22 above.

[27] Clare Ellis, Raffaello Pantucci, Jeanine de Roy Van Zuijdewijn, Edwin Bakker, Benoit Gomis, Simon Palombi and Melanie Smith, footnote 18 above at page 3.

26 Lone actor terrorists tend to attack targets perceived as easy, such as unprotected public spaces (shopping malls, parks, roads, bridges) and often use readily obtainable weapons, such as knives or vehicles. These attacks generally require limited planning and preparation and may result from very rapid radicalisation and mobilisation to violence. And because the perpetrators are lone actors they do not need to communicate with anyone else about their plans and preparation. This makes them less detectable, and thus less vulnerable to counter-terrorism measures than group-based terrorists.

27 Dā'ish actively encouraged lone actor attacks. In October 2014, the group's magazine *Dabiq* advised:

> *The smaller the numbers of those involved and the less the discussion beforehand, the more likely it will be carried out without problems … . One should not complicate the attacks by involving other parties, purchasing complex materials, or communicating with weak-hearted individuals*.[28]

28 Lone actor terrorist attacks have not always resulted in fatalities, but have nonetheless instilled widespread public fear. The potential for an attack resulting in large numbers of people being injured or killed (illustrated by the terrorist attack on 15 March 2019, the Oslo terrorist's attack and Dā'ish-inspired high casualty attacks in Europe) means a lone actor attack is a significant concern for intelligence and security agencies.[29]

29 A 2015 report from the Southern Poverty Law Center found that, between 2009 and 2015, 74 percent of domestic terrorist attacks in the United States of America – from right-wing and Islamist extremists – were carried out and planned by a single person operating alone.[30]

An enemy within?

30 Islamist extremism was and continues to be viewed as having a religious, cultural and ideological context and geographic locus distinct to, and removed from, the West. In this way, even Islamist extremists living in Western countries have been perceived by intelligence and security agencies as "foreign".

[28] "The Failed Crusade" (October 2014) No. 4 *Dabiq* at page 44 in Clare Ellis, Raffaello Pantucci, Jeanine de Roy Van Zuijdewijn, Edwin Bakker, Benoit Gomis, Simon Palombi and Melanie Smith, footnote 18 above.

[29] Clare Ellis, Raffaello Pantucci, Jeanine de Roy Van Zuijdewijn, Edwin Bakker, Benoit Gomis, Simon Palombi and Melanie Smith, footnote 18 above at page 8.

[30] In the study, the Southern Poverty Law Center observed "there is no hard and fast agreement on what constitutes a terrorist action". The survey relied upon records maintained by Indiana State University and the University of Maryland's Global Terrorism Database, as well as the Southern Poverty Law Center's own roster of apparent domestic terror incidents. It included incidents that likely involved mental illness, but that seemed to have an obvious political aspect. It covered terrorism inspired by anti-government, Islamist extremist and various forms of race or group hatred. And it encompassed both actual terror attacks and those that were disrupted.

31 People who have far right views are not usually ethnically, socially or culturally distinct from the majority of the population. As well there are considerable overlaps between the views of the majority of the population and far right views, and radical right and extreme right-wing views. This means that it can be difficult for intelligence and security agencies to identify unique and reliable indicators of people, groups and networks with extreme right-wing ideology.

32 There have been examples in recent years of people with far right views being found embedded within the national security system in Western countries. For example, recent investigations in Germany indicate that the far right group Northern Cross had close links to the police and military. Some members were reportedly planning terrorist attacks against their political enemies. Using police computers, they collected some 25,000 names and addresses of pro-refugee local politicians. The members associated with the plan included two police officers, two army reservists and a police sniper.[31] In the United States of America, a recent report from a former special agent of the Federal Bureau of Investigation concluded that white supremacist groups had infiltrated law enforcement agencies in every region of the country.[32] In the United Kingdom in 2017, four serving members of the British Army were arrested on suspicion of being members of the banned extreme right-wing group National Action. One of them was subsequently sentenced to eight years in prison.[33] And a former Canadian Armed Forces combat engineer was linked to a violent white supremacist group and arrested in the United States of America by the Federal Bureau of Investigation after going missing for five months.[34]

33 There is some evidence of the presence of far right individuals in New Zealand's military. In December 2019 a soldier was arrested at Linton Military Camp in Palmerston North, amid suspicion they were part of a far right group.[35] And in March 2020, the Australian activist group White Rose Society claimed that a (former) New Zealand Army soldier had posted on private online message boards about forming terrorist cells in New Zealand and purchasing firearms from the black market.[36]

[31] Katrin Bennehold "Body Bags and Enemy Lists: How Far Right Police Officers and Ex-Soldiers planned for 'Day X'" *The New York Times* (New York, 1 August 2020) https://www.nytimes.com/2020/08/01/world/europe/germany-nazi-infiltration.html https://www.nytimes.com/2020/08/01/world/europe/germany-nazi-infiltration.html.

[32] Sam Levin "White supremacists and militias have infiltrated police across US, report says" *The Guardian* (Los Angeles, 27 August 2020) https://www.theguardian.com/us-news/2020/aug/27/white-supremacists-militias-infiltrate-us-police-report.

[33] Lizzie Darden "British Army Lance Corporal was recruiting soldiers for neo-Nazi terrorist group" *The Independent* (United Kingdom, 13 November 2018) https://www.independent.co.uk/news/uk/crime/british-army-officer-national-action-mikko-vehvilainen-neo-nazi-terrorist-group-recruitment-a8632331.html.

[34] Karen Pauls and Angela Johnston "FBI arrests reveal shocking details in case against former Canadian reservist Patrik Mathews" *CBC NEWS* (Canada, 18 January 2020) https://www.cbc.ca/news/canada/manitoba/fbi-arrests-the-base-georgia-wisconsin-1.5432006.

[35] Charlotte Cook "Soldier's arrest raises concerns far-right could infiltrate Defence Force" *RNZ* (New Zealand, 18 December 2019) https://www.rnz.co.nz/news/national/405784/soldier-s-arrest-raises-concerns-far-right-could-infiltrate-defence-force.

[36] Isaac Davison "NZ Defence Force says white supremacist is a former soldier" *The New Zealand Herald* (New Zealand, 13 March 2020) https://www.nzherald.co.nz/nz/nz-defence-force-says-white-supremacist-is-a-former-soldier/WAKCYC7K4ENTMF2N26RGVKW2AI/.

The changing threatscape has increased the domestic threat in New Zealand

34 New Zealand has not been immune from these global terrorism and extremism developments. In 2015, the Department of the Prime Minister and Cabinet described a "worsening [terrorist] threatscape at home". There were larger numbers of persons of interest to intelligence and security agencies. By 2017, there were usually between 30–40 individuals of counter-terrorism concern in New Zealand, most of whom were assessed as supporters of Dā'ish.

35 There were also potential threats of extreme right-wing terrorism. In January 2019 New Zealand Police executed a search warrant and discovered considerable evidence that a school student, assessed as likely holding extreme right-wing beliefs, was planning to undertake a school shooting in February 2019.

36 While the Public sector in New Zealand was adjusting to the new and shifting threatscape and developing its counter-terrorism capabilities, it had to navigate numerous events and controversies to which we now turn.

2.4 Controversies and other events affecting the agencies

Operation Eight controversy

37 On 15 October 2007, 17 people, including some Tūhoe activists, were arrested after an investigation (Operation Eight) by New Zealand Police discovered evidence of secret military-style training camps in Te Urewera.[37] An attempt was made to charge them under the Terrorism Suppression Act, but the then Solicitor-General found that the evidentiary threshold required under that Act had not been met and declined to give permission to lay terrorism charges. In 2013, the Independent Police Conduct Authority found that New Zealand Police had "unnecessarily frightened and intimidated" people during the raids, which included the coordinated execution of 41 search warrants throughout the country along with road blocks in the Tūhoe area. In 2014, the then Commissioner of New Zealand Police, Mike Bush, apologised for mistakes made during the raids.

38 The entire episode attracted widespread media attention in New Zealand, much of which was critical of New Zealand Police. The merits of New Zealand Police activity are not our concern. What is important is that it diminished public confidence in New Zealand Police.

[37] Te Urewera is an area of mountains, forests, lakes and river valleys in the North Island of New Zealand. Te Urewera is "the homeland and heartland of the Tūhoe people". See Te Urewera Board land management plan *Te Kawa o Te Urewera* (2017) at page 43.

Dotcom controversy

39 In 2012, the United States of America requested the extradition of Kim Dotcom, the developer of Megaupload.com, to face charges relating to conspiracy to infringe copyright. Kim Dotcom held a New Zealand resident visa and was living in Auckland with his wife and young family. A dramatic raid was conducted on his home by New Zealand Police. It turned out that the Government Communications Security Bureau, acting on a request from New Zealand Police, had intercepted Kim Dotcom's communications. This interception was unlawful, because at the time, the Government Communications Security Bureau was prohibited from intercepting the private communications of New Zealand permanent residents, a status held by Kim Dotcom.

40 Then Prime Minister Rt Hon John Key apologised for the error, and the incident prompted a review of compliance at the Government Communications Security Bureau.[38] That review, undertaken by Rebecca Kitteridge, was published in early 2013. It identified systemic problems with the Government Communications Security Bureau's legal compliance systems, and suggested that at least 88 people might have been subject to unlawful surveillance over the previous decade.[39]

41 Again, there was substantial media scrutiny of what had occurred, much of it very critical of the Government Communications Security Bureau and New Zealand Police.

Snowden revelations

42 In 2013, The Guardian newspaper in the United Kingdom began to publish a series of articles containing leaked classified information about the United States of America's surveillance programme, which came from Edward Snowden (a former contractor for the National Security Agency).

43 In New Zealand, the leaks were the basis for media reporting that the Government Communications Security Bureau conducted "full take" collection on Pacific Island states and trading partners. The leaks also led to reporting that New Zealand spied on countries for economic advantage and that the Government Communications Security Bureau used its capabilities to help the New Zealand Minister of Trade's unsuccessful bid to become the Director-General of the World Trade Organization. While two subsequent Inspector-General of Intelligence and Security reports found that the Government Communications Security Bureau had acted appropriately (and made specific findings on the "full-take" allegations), the activities nonetheless led to questions from many New Zealanders about the appropriateness of the activities of the Government Communications Security Bureau and further undermined public confidence.[40]

[38] Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (Cullen-Reddy Report) (29 February 2016) at page 14.

[39] Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).

[40] Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM, footnote 38 above at page 24.

Accusations against the New Zealand Security Intelligence Service by the Leader of the Opposition

44 In July 2011, the Southland Times newspaper published allegations that there had been Israeli intelligence activity in Christchurch at the time of the 22 February 2011 Canterbury earthquake. Then Leader of the Opposition, Hon Phil Goff, stated publicly that he had not been briefed on the issue. The New Zealand Security Intelligence Service advised the then Prime Minister, Rt Hon John Key, that the Leader of the Opposition had been briefed, and the Prime Minister said so publicly on 24 July 2011. As a result of the conflicting statements, journalist and blogger Cameron Slater requested information from the New Zealand Security Intelligence Service. It responded by giving him three redacted documents. These documents formed the basis of a public challenge to the credibility of Hon Phil Goff. In November 2014, the Inspector-General of Intelligence and Security found that the New Zealand Security Intelligence Service had supplied Cameron Slater with incomplete, inaccurate and misleading information.[41]

45 The consequence was a decrease in public and ministerial confidence in the intelligence and security agencies. Rightly or wrongly, this episode created a perception that the New Zealand Security Intelligence Service had become politicised.

"Jihadi brides"

46 In December 2015, Rebecca Kitteridge, Director-General of Security, told a public session of Parliament's Intelligence and Security Committee that there was a developing trend of New Zealand women travelling to Dā'ish-controlled areas in the Middle East. She prefaced this statement with comments about the "threat to domestic security posed by foreign fighters and other extremists". Then Prime Minister Rt Hon John Key, who chaired the Committee, asked if the women could be "jihadi brides". He repeated the phrase in a media conference after the Committee hearing.

47 What Rebecca Kitteridge had said to the Committee was literally correct in that a few women with New Zealand citizenship had travelled to Dā'ish-controlled areas. However, the women in question had been living in Australia and had departed for the Middle East from there. The misconception that the women had been living in, and had departed from, New Zealand was not addressed for some time. This is because the New Zealand Security Intelligence Service needed the approval of international partner agencies before it could publicly state that the women had departed from Australia.

[41] Office of the Inspector-General of Intelligence and Security *Report into the release of information by the NZSIS in July and August 2011* (November 2014).

48 The "jihadi brides" remarks were picked up by the media and generated considerable controversy and ill-will towards members of New Zealand's Muslim communities. Muslim communities reported that at that time they faced an increase in hostility, particularly Muslim women who were subjected to increased abuse and threatening behaviour. This was exacerbated by the delay in correcting the misconception.

2.5 Institutional reviews

49 Components of the New Zealand national security system and the Public sector agencies comprising it have been the subject of many reviews over the past two decades. By our count there have been at least 35. Not all of the reviews listed are publicly available.

Table 12: Reviews of components of the New Zealand national security system (2003–2019)

Date	Review
2003	Office of the Controller and Auditor-General *Managing Threats to Domestic Security* (October 2003)
2009	Michael Wintringham and Jane Jones *A National Security & Intelligence Framework for New Zealand* (September 2009)
2009	Simon Murdoch *Report to the State Services Commissioner: Intelligence Agencies Review* (October 2009)
2011	New Zealand Police *National Security Capability Assessment* (March 2011)
2011	Department of the Prime Minister and Cabinet *New Zealand's National Security System* (May 2011)
2012	Simon Murdoch *Review of CTAG* (April 2012)
2013	Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013)
2013	Simon Murdoch *Counter-Terrorism: A review of the New Zealand CT landscape* (Department of the Prime Minister and Cabinet, May 2013)
2013	*Performance Improvement Framework – Review of the Department of the Prime Minister and Cabinet* (*DPMC*) (June 2013)
2013	Jacki Couchman *Review of Arrangements for Coordinating National Security and Intelligence Priorities* (Department of the Prime Minister and Cabinet, July 2013)

Date	Review
2014	Government Communications Security Bureau *Government Communications Security Bureau Functional Review* (March 2014)
2014	*Performance Improvement Framework – Review of the agencies in the core New Zealand Intelligence Community (NZIC)* (March 2014)
2014	Office of the Inspector-General of Intelligence and Security *Report into the release of information by the NZSIS in July and August 2011* (November 2014)
2015	Steve Long *Independent Review of Current Activity and Development of a Counter-Terrorism Strategy* (2015)
2015	*Performance Improvement Framework – Follow-up Review of the Department of the Prime Minister and Cabinet (DPMC)* (February 2015)
2015	New Zealand Police *National Security and Counter-terrorism Capability Review* (September 2015)
2015	New Zealand Security Intelligence Service *Strategic Capability and Resourcing Review* (2015)
2015	New Zealand Security Intelligence Service *Review of the New Zealand Intelligence Community's Security Intelligence Operating Model (Project Aguero)* (2015)
2015	New Zealand Law Commission *The Crown in Court: A Review of the Crown Proceedings Act and National Security Information in Proceedings Report 135* (December 2015)
2016	Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (Cullen-Reddy Report) (February 2016)
2016	New Zealand Security Intelligence Service *The NZSIS 10-Year Operational Strategy (Project Sterling)* (June 2016)
2016	Office of the Controller and Auditor-General *Governance of the National Security System* (November 2016)
2016	Simon Murdoch *Review of the Integrated Targeting and Operations Centre* (July 2016)

Date	Review
2017	Office of the Inspector-General of Intelligence and Security *Report into the Government Communications Security Bureau's process for determining its foreign intelligence activity* (2017)
2017	Office of the Controller and Auditor-General *Report on Border Security: Using information to process passengers* (June 2017)
2018	New Zealand Intelligence Community *NZIC Follow-up Self Review* (2018)
2018	New Zealand Security Intelligence Service *Performance Improvement Framework: Follow-up Self Review of the New Zealand Security Intelligence Service Te Pa Whakamarumaru* (March 2018)
2018	Simon Murdoch *CTAG 2018: Its placement in New Zealand's counter-terrorism system architecture and its location; an independent view* (July 2018)
2018	Office of the Inspector-General of Intelligence and Security *Complaints arising from reports of the Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009–2015* (July 2018)
2018	*Performance Improvement Framework – Follow-up Review for the New Zealand Intelligence Community (NZIC) Te Rōpū Pārongo Tārehu o Aotearoa* (August 2018)
2018	Office of the Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018)
2018	Office of the Inspector-General of Intelligence and Security *2016–17 Review of NZSIS requests made without warrants to financial service providers: Report* (November 2018)
2018	Office of the Inspector-General of Intelligence and Security *Warrants Issued under the Intelligence and Security Act 2017: Report* (December 2018)
2019	New Zealand Security Intelligence Service *The 2019 Terrorist Attacks in Christchurch: A review into NZSIS processes and decision-making in the lead up to the 15 March attacks (Arotake Review)* (June 2019)
2019	Office of the Inspector-General of Intelligence and Security *Report on a review of the New Zealand Security Intelligence Service relationships at the border* (6 September 2019)

50 Individually and collectively, these reviews provide snapshots of Public sector agencies' performance. They also should have informed decision-making. While we have drawn on them as part of our inquiry, we have also seen that some of the deficiencies previously identified have yet to be fixed (see Part 8, chapter 3).

2.6 The Strategic Capability and Resourcing Review programme

51 In 2014, the New Zealand Intelligence Community received a very adverse *Performance Improvement Framework* review.[42] Cabinet was subsequently advised that the New Zealand Intelligence Community was facing significant changes in the domestic and international operating environments and its ongoing funding was not sufficient. In response, the New Zealand Intelligence Community undertook the Strategic Capability and Resourcing Review. This addressed resourcing and resulted in the approval in 2016 of $178.7 million to be invested in the New Zealand Intelligence Community over four years.

52 The implementation of the recommendations that followed the Strategic Capability and Resourcing Review and the progressive enhancement of the capability and capacity of the New Zealand Security Intelligence Service form an important part of our assessment of its contributions to the counter-terrorism effort before 15 March 2019 (see Part 8, chapter 5).

[42] *Performance Improvement Framework: Review of the agencies in the core New Zealand Intelligence Community (NZIC)* (March 2014).

Chapter 3: Leadership and oversight

3.1 Overview

1 In New Zealand, many Public sector agencies contribute to the counter-terrorism effort. Each agency is responsible for its own performance and contribution. Leadership and oversight of the collective counter-terrorism effort is not exercised through a single agency or ministerial portfolio.

2 In this chapter we:

a) describe political ownership and public engagement in the counter-terrorism effort;

b) assess leadership and coordination of the counter-terrorism effort;

c) examine strategy and priority setting;

d) describe oversight and performance monitoring;

e) discuss gaps in the leadership and oversight of the counter-terrorism effort; and

f) set out developments since 15 March 2019.

3.2 Political ownership and public engagement

3 Political ownership of, and public discussion on, terrorism risk provide transparency and enhance social licence for the counter-terrorism effort.

4 In New Zealand, prime ministers and ministers actively engage on national security issues that are well recognised by the public, such as natural hazards, biosecurity and border security. They rarely speak publicly about the terrorism threat or violent extremism, and far less so than we observed or were told about in Australia, Norway and the United Kingdom. One senior official told us that ministers "pay attention to national security questions when they're put in front of them and not otherwise".

5 In 2014, the government created a new role of minister for national security and intelligence, with responsibility for leading the national security system. This was separate to the existing role of minister responsible for the intelligence and security agencies.[43] Then Prime Minister, Rt Hon John Key, made a significant national security speech on 5 November 2014.[44] In this speech he disclosed, for the first time, the watch list of 30–40 individuals of national security concern and the terrorism threat level and publicly confirmed that New Zealand was a member of the Five Eyes.

[43] Rt Hon John Key *National Security and Intelligence role created* (6 October 2014) https://www.beehive.govt.nz/release/national-security-and-intelligence-role-created.

[44] Rt Hon John Key *Speech to NZ Institute of International Affairs* (6 November 2014) https://www.beehive.govt.nz/speech/speech-nz-institute-international-affairs-0.

6 In 2016, the then Attorney-General, Hon Christopher Finlayson, undertook public engagement on the Intelligence and Security Bill (see Part 8, chapter 14). This included community hall meetings and visits to masajid.

7 As we will outline in Part 8, chapter 4, ministers and the public generally understood that there was a relatively benign terrorist threatscape in New Zealand. Before the 15 March 2019 terrorist attack, the threat and risk of domestic terrorism (and especially of non-Islamist terrorism) were lightly covered in assessments and policy advice to ministers, such as when the National Security and Intelligence Priorities were approved. For example, the regular intelligence briefs provided by the National Assessments Bureau to the prime minister included little on the domestic extremism or terrorism environment. From 2010 to 15 March 2019, these briefs contained fewer than twenty references to domestic extremism in New Zealand.

8 Overall New Zealand's relative geographic isolation and the comparative absence of terrorist attacks on New Zealand soil led to low levels of public and official concern about domestic terrorism threats. The overall threat of terrorism in New Zealand was assessed as "low" (terrorist attack is assessed as possible but is not expected) or "very low" (a terrorist attack is assessed as very unlikely) between 2010 and 2018. This perception of the terrorism risk impacted on the pace at which policy decisions were progressed. An example involves the delays in updating relevant legislation (see Part 8, chapter 13).

9 Informed public debate can provide a sense of society's appetite for activities to address threats to national security. From our inquiries, we are satisfied that agencies have had successes in countering and disrupting terrorism and violent extremism in New Zealand. But these domestic counter-terrorism successes occured well out of the public eye and their stories have not been told publicly. Instead, we heard that the Dotcom and Snowden controversies (see Part 8, chapter 2) diminished politicians' interest in promoting public discussions or counter-terrorism initiatives that might include the intelligence and security agencies' roles.

10 Former and current ministers and senior officials appear to have been concerned that public-facing strategies and public discussion about countering terrorism might have had adverse impacts on communities (particularly Muslim communities), given rise to unwarranted community anxiety or created expectations of mitigations the government could not provide. In addition, New Zealand was still facing fiscal constraints in the aftermath of the Global Financial Crisis and the 2010–2011 Canterbury earthquake sequence. As a result of these factors, and the impact of public controversies, ministers have approached any changes to the counter-terrorism effort conservatively.

11 The absence of a widespread or regular national public dialogue on New Zealand's national security and counter-terrorism effort was raised with us by senior officials, community groups, our Muslim Community Reference Group and in submissions. Several previous reviews highlighted the need for change in this area.[45] The Department of the Prime Minister and Cabinet recommended introducing an ongoing public dialogue on national security and counter-terrorism in the 2017 *Briefing to the Incoming Minister for National Security and Intelligence*. But this did not happen.

12 There was very little engagement between those responsible for the counter-terrorism effort and the public before 15 March 2019. This meant there was neither well-informed public discussion on the terrorism threat and risk, nor information on how to identify threats. Before 15 March 2019, there was limited reporting from the public to the New Zealand Security Intelligence Service, and such reporting as there was focused largely on suspected Islamist extremists. The same was true of the reporting of possible extremists to New Zealand Police.

13 There was an understandable increase in engagement from the public immediately after 15 March 2019. Public referrals or reports to the New Zealand Security Intelligence Service and to New Zealand Police increased significantly as the public had a greater appreciation of the terrorist threat. Many of these reports involved people on the far right. For example, in the period between 15 March 2019 and the end of May 2019, New Zealand Police received 2,326 public reports or referrals, a substantial proportion of which related to people with far right views.

14 Since 15 March 2019, the Government has released more information relating to national security and the counter-terrorism effort. But this has happened quietly, and without a framework to engage the public or encourage diverse views on countering terrorism and violent extremism. For example:

a) The National Security and Intelligence Priorities (agreed in 2018) were published for the first time as an appendix to the Department of the Prime Minister and Cabinet's 2019 annual report.[46] There was no accompanying public announcement. Unsurprisingly, this did not generate public discussion about intelligence collection priorities, despite the increased interest in the counter-terrorism effort after 15 March 2019. In September 2020, the National Security and Intelligence Priorities were published directly on the Department of the Prime Minister and Cabinet's website.[47]

[45] Office of the Controller and Auditor-General *Managing Threats to National Security* (October 2003); *Performance Improvement Framework*, footnote 42 above; Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM, footnote 38 above.

[46] Department of the Prime Minister and Cabinet *Annual Report 2018/2019 for the year ended 30 June 2019* (October 2019) https://dpmc.govt.nz/publications/annual-report-2019.

[47] Department of the Prime Minister and Cabinet website *National Security and Intelligence Priorities* https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security-and-intelligence-priorities.

b) A high-level *Countering terrorism and violent extremism national strategy overview* was published on the Department of the Prime Minister and Cabinet's website in February 2020.[48] Again, this was not promoted as an opportunity for, and thus did not generate, wide public discussion.

3.3 Leadership and coordination

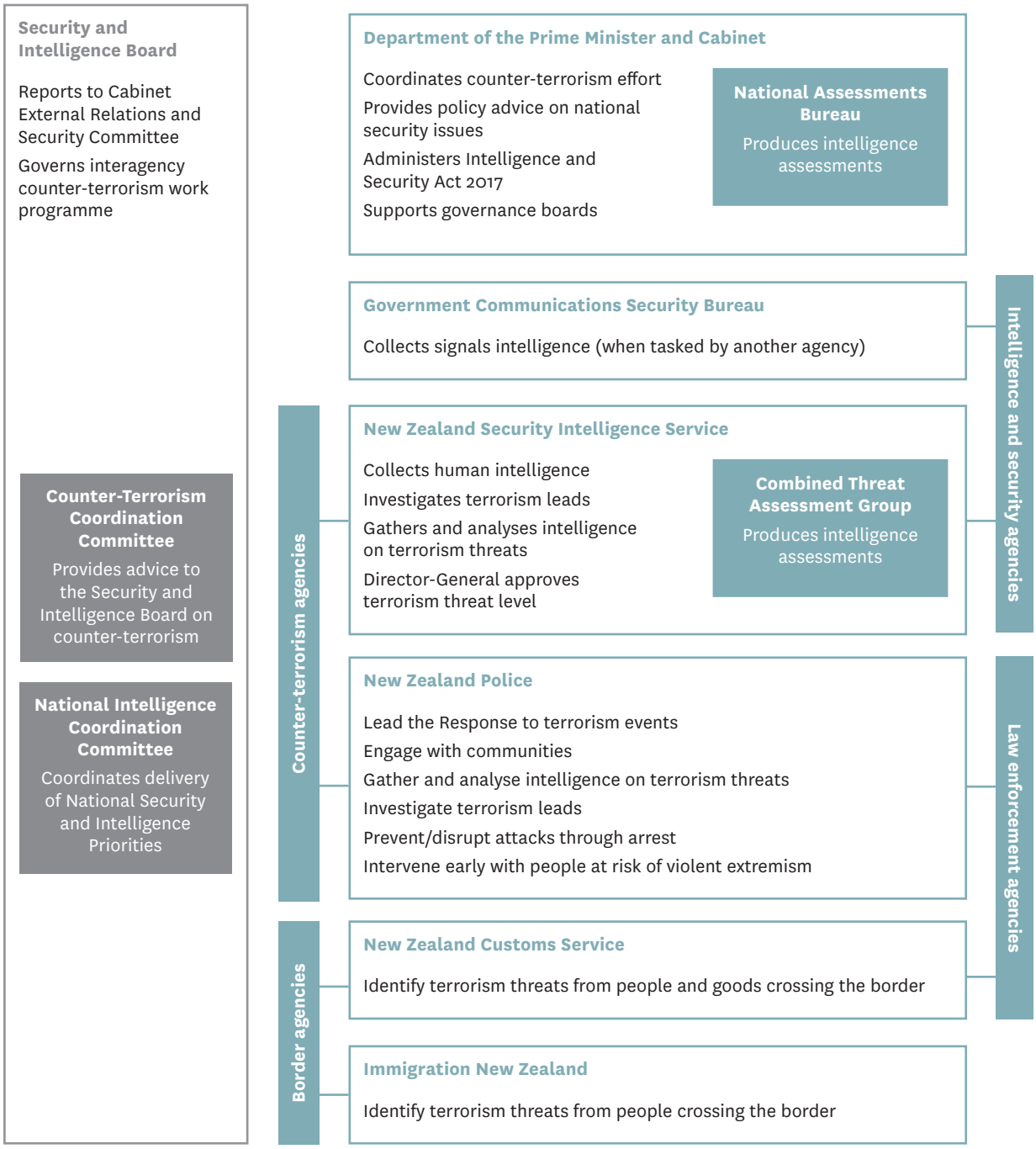
15 In this section, we discuss leadership and coordination roles within New Zealand's national security system and the counter-terrorism effort. As will become apparent, there is some lack of clarity about leadership of the different parts of the counter-terrorism effort and no one agency is currently responsible for monitoring overall system performance.

A decentralised coordinated model

16 New Zealand's counter-terrorism effort is decentralised but coordinated. It is decentralised in that no single agency has overall responsibility for the effort. Instead, it is spread across multiple agencies, with each agency responsible for its own performance and contribution. Coordination comes from the Department of the Prime Minister and Cabinet. It does not have directive control over the individual agencies or their contribution to the overall work programme.

[48] Department of the Prime Minister and Cabinet *Countering terrorism and violent extremism national strategy overview* (undated) https://dpmc.govt.nz/sites/default/files/2020-02/2019-20%20CT%20Strategy-all-final.pdf.

Figure 40: Counter-terrorism functions of Public sector agencies involved in the counter-terrorism effort



17 This model reflects the decentralised approach to the national security system as a whole (see Part 2, chapter 4). The Department of the Prime Minister and Cabinet told us that centralised responsibility for the national security system is not necessarily a preferred outcome:

> *Operating as a system, and exercising collective leadership over the national security choices that must be made, does not imply collective accountability for all outcomes. Particularly in a system of government such as that operating in New Zealand, it is not possible to centralise everything. Agencies must know where their accountabilities are, and own these.*

18 The government has identified some weaknesses with how decentralised models of accountability and governance work in the New Zealand Public sector. In August 2020, the Public Service Act 2020 was enacted to address some of these deficiencies. The Act has introduced mechanisms to facilitate collective responsibility and accountability for multi-agency programmes of work. We come back to this later in *Part 10: Recommendations*.

The role of the Department of the Prime Minister and Cabinet

19 The Department of the Prime Minister and Cabinet is the lead Public sector agency on national security. Its role is to coordinate activity across the relevant Public sector agencies involved in the national security system. Its chief executive is the "lead official for the whole National Security System" and chairs the Officials' Committee for Domestic and External Security Coordination when New Zealand is faced with a national security event. It is also responsible for coordinating government action in response to national security events, ensuring national security risks are managed appropriately, leading policy development on national security matters, hosting the National Assessments Bureau and administering the Intelligence and Security Act 2017.

20 The Department of the Prime Minister and Cabinet's current organisational structure for its counter-terrorism functions is outlined in the graphic below.

Figure 41: Counter-terrorism functions within the organisational structure of the Department of the Prime Minister and Cabinet

21 The Department of the Prime Minister and Cabinet has a limited legislative mandate for national assessments but otherwise has no directive authority or statutory mandate for its coordination of the national security system or counter-terrorism effort. The relevant agencies and chief executives each exercise their own statutory responsibilities and functions, which are not controlled by the Department of the Prime Minister and Cabinet. The Department of the Prime Minister and Cabinet's direct relationship to the prime minister creates a convening power across all Public sector agencies.

22 We were told that other agencies are uncomfortable if the Department of the Prime Minister and Cabinet is seen as too assertive on national security matters. Howard Broad, former Deputy Chief Executive of the Department of the Prime Minister and Cabinet, told us that when he explicitly raised the question of monitoring the intelligence and security agencies' performance at the Security and Intelligence Board, "there was strong pushback by the agencies and [they] generally agreed around the table that wasn't the Department of the Prime Minister and Cabinet's role". He said that, on a practical level, "no-one was indicating a desire that the Department of the Prime Minister and Cabinet increase its capability".

23 We also heard that successive prime ministers were not willing to seek additional funding for their own department (especially when they were calling for fiscal control by other ministers). Nor would they support a budget bid through another minister advocating for investment for the Department of the Prime Minister and Cabinet to coordinate national security responsibilities. The result is that the coordination role has not been well resourced.

24 The Department of the Prime Minister and Cabinet advised us that "[its own] investigations have not uncovered any policy or internal papers prepared by the Department of the Prime Minister and Cabinet which explicitly and exclusively deal with the question of its role in the national security system and work priorities directly associated with this". In its 2018–2019 Business Plan, the National Security Group in the Department of the Prime Minister and Cabinet did note that:

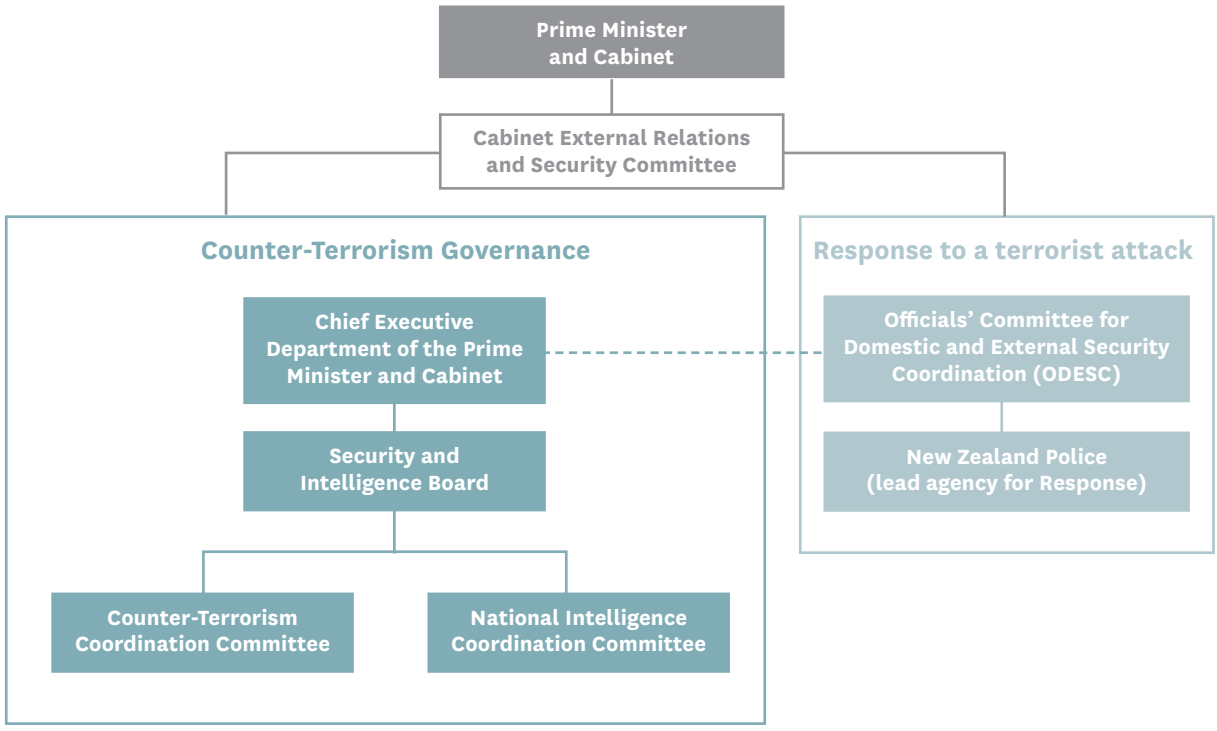
> *... a strategic refresh is needed. [It is] time to refine the purpose, goals, roles and responsibilities [of the National Security Group].*

25 This work had not been completed by 15 March 2019.

The Security and Intelligence Board

26 The Security and Intelligence Board is one of two governance boards that bring together the chief executives of agencies with national security responsibilities (see Part 2, chapter 4). The Security and Intelligence Board focuses on threats from human sources, such as terrorism or foreign interference. The other governance board, the Hazard Risk Board, focuses on threats from non-human sources, such as natural hazards, biosecurity threats and pandemics.

Figure 42: Governance of the counter-terrorism effort



27 The Security and Intelligence Board membership includes the chief executives of the Department of the Prime Minister and Cabinet (Chair), the Government Communications Security Bureau, the Ministry of Defence, the Ministry of Foreign Affairs and Trade, New Zealand Customs Service, the New Zealand Defence Force, New Zealand Police and the New Zealand Security Intelligence Service. Other chief executives may be invited by the Chair to attend meetings if required. The Security and Intelligence Board reports to the Cabinet External Relations and Security Committee.

28 The role of the Security and Intelligence Board has evolved following various reviews. Its 2017 Terms of Reference identified its vision as "a resilient New Zealand against those who would wish us harm" and its purpose as to:

Lead, build and govern the security and intelligence system that:

- *Identifies and understands threats, patterns and risks in our environment;*
- *Prioritises vulnerabilities and threats and understands the desired end state to be obtained;*
- *Hold[s] system to account for delivery:*
    - *Governance of the "[Security and Intelligence Board] deputies group" to implement [the Security and Intelligence Board's] vision;*
    - *By tracking tasking – ensuring there is a plan that is achievable;*
    - *Enabling of the system wide support of tasking;*
    - *Reporting to [the National Security Committee / Officials' Committee for Domestic and External Security Coordination] as required;*
- *Build[s] system capabilities and capacity:*
    - *Identifying gaps and weaknesses;*
    - *Developing system policies and processes;*
    - *Reviewing and learning; and*
- *Remain[s] alert to current threats and opportunities; proactive testing of the plan against "real life information" and events and be agile and responsive.*

29 The Security and Intelligence Board's deliverables include the National Security and Intelligence Priorities, an annual strategic assessment of the environment and action plans to identify threats, patterns and risks.

30 The chief executives on the Security and Intelligence Board each have statutory functions that are not controlled by the Security and Intelligence Board. They each report to their respective ministers and exercise their own responsibilities.

31 Although its Terms of Reference include "hold[ing the] system to account for delivery", the Security and Intelligence Board does not monitor the performance of the counter-terrorism effort and has not put in place a performance framework and standards for it. It has also not established a system for monitoring its own performance. A 20 June 2019 report to the Security and Intelligence Board noted that work had not yet commenced on measuring or assessing its own governance and coordination performance, the authorising environment (including social licence, transparency and legislation) or relationships (including Five Eyes and other international relationships).

32 The Security and Intelligence Board has several subcommittees. The two subcommittees most relevant to the counter-terrorism effort are:

a) the Counter-Terrorism Coordination Committee, which provides advice to the Security and Intelligence Board on counter-terrorism systems, priorities, risks, projects and resourcing requirements; and

b) the National Intelligence Coordination Committee, which coordinates the delivery of the National Security and Intelligence Priorities and the work programmes of the assessment agencies (see Part 8, chapter 4).

Leadership of the counter-terrorism effort

33 It is important that all agencies in the counter-terrorism effort are guided by a clear understanding of who does what, when, why and how across the 4Rs – Reduction, Readiness, Response and Recovery activities (see Part 2, chapter 4).

34 The government's *Counter-Terrorism Playbook*[49] states that New Zealand Police are "the designated lead agency, providing command and control of the multi-agency response to any [terrorism] event in New Zealand". The Department of the Prime Minister and Cabinet has publicly stated that "New Zealand Police are well prepared and exercised to lead the response to a terrorism incident". So the lead agency for Response to a terrorist incident is clear.

35 We did not, however, observe a similar consensus on which Public sector agency leads Reduction, Readiness and Recovery activity.

[49] Department of the Prime Minister and Cabinet *Counter-Terrorism Playbook* (2019) at page 40.

36 The Department of the Prime Minister and Cabinet told us that it, together with New Zealand Police and the New Zealand Security Intelligence Service, had been identified as the risk coordinating agencies for terrorism since the beginning of the development of the National Risk Register framework in 2015 (see 3.4 Setting the strategy). In contrast, the Security and Intelligence Board's December 2018 report on *Better Management of National Security Risks* identified New Zealand Police and the New Zealand Security Intelligence Service as the risk coordinating agencies, but not the Department of the Prime Minister and Cabinet.

37 The *National Security Handbook* refers to New Zealand Police as the lead agency for counter-terrorism at the national, regional and local levels, suggesting it is the lead agency for all of the 4Rs. The Department of the Prime Minister and Cabinet considers "[New Zealand] Police are the lead agency for all '4Rs' of the Terrorism risk, but that several parts of risk management and the [*Counter-Terrorism Work Programme*] are led by other agencies coordinated by [the Counter-Terrorism Coordination Committee] and governed by the Security and Intelligence Board".

38 In 2016, the Security and Intelligence Board discussed the overarching leadership of counter-terrorism in New Zealand and considered identifying New Zealand Police as the lead. In the associated discussions there was recognition of the significant additional burden this would place on New Zealand Police and the absence of a lead minister for counter-terrorism. In the end, there was no decision on this and leadership remained with the Department of the Prime Minister and Cabinet.

39 In October 2016, the role of Specialist Coordinator was created within the Department of the Prime Minister and Cabinet to provide system-level coordination of collective counter-terrorism activity through the Counter-Terrorism Coordination Committee, and support the Security and Intelligence Board and Cabinet National Security Committee governance functions. When it was created, the Specialist Coordinator role was expected to be responsible for "driving delivery of a co-ordinated, cross-agency programme that strives to eliminate gaps and minimises the likelihood and impact of terrorist threats to New Zealand". It was expected that the creation of this role would ensure that "the [*Counter-Terrorism Work Programme*] can respond in a timely manner to changing risk". As chair of the Counter-Terrorism Coordination Committee, the Specialist Coordinator would work with senior officials from agencies with key counter-terrorism responsibilities, including those involved in social cohesion and preventing violent extremism. After the role was filled, a high-level *Counter-Terrorism Work Programme* was developed and reported to the Security and Intelligence Board in July and September 2018. The Specialist Coordinator was the only coordinator appointed for a specific national security threat before 15 March 2019.

40 Evidence provided to us indicates there continues to be different understandings and expectations about where leadership of the counter-terrorism strategy and the counter-terrorism effort sits, and what that means in practice:

a) A former Specialist Coordinator at the Department of the Prime Minister and Cabinet (who chaired the Counter-Terrorism Coordination Committee) considered it more important that the Security and Intelligence Board had overall responsibility for collective counter-terrorism responsibilities rather than one agency. This is because backing from multiple agencies is needed to deliver the counter-terrorism effort.

b) The Government Communications Security Bureau suggested that domestic counter-terrorism efforts are co-led by New Zealand Police and the New Zealand Security Intelligence Service, as the domestically-focused law enforcement and intelligence and security agencies.

c) Rebecca Kitteridge, Director-General of Security, told us the overall lead for counter-terrorism is the Specialist Coordinator in the Department of the Prime Minister and Cabinet, as that agency can look "end to end" from social inclusion right through to prosecutions and has the coordination and policy function needed for this. She expressed concern that there had not been a proper analysis put forward when New Zealand Police were proposed as the lead. She also noted that while New Zealand Police have a wide reach into communities they are not a policy agency and, as an operational agency with a law enforcement mandate, they were not best placed to lead at the softer end of counter-terrorism activities, such as social inclusion and countering violent extremism.

d) The New Zealand Security Intelligence Service advised that it does not consider itself the "lead agency for the national counter-terrorism effort", but rather that it has the lead responsibility for "counter-terrorism security intelligence investigations, analysis and reporting".

e) A current senior manager at the New Zealand Security Intelligence Service thought the Department of the Prime Minister and Cabinet is best placed to lead the "practical … day-to-day" counter-terrorism system because it can see across sectors and agencies and houses the Specialist Coordinator. They thought the Department of the Prime Minister and Cabinet does not currently play that role and no one agency does.

f) Mike Bush, former Commissioner of Police, told us he did not see the Department of the Prime Minister and Cabinet as the counter-terrorism lead. He said the lead could be, and currently is, held jointly by New Zealand Police and the New Zealand Security Intelligence Service, but that clarity of their roles and responsibilities is essential.

g) Andrew Kibblewhite, former Chief Executive of the Department of the Prime Minister and Cabinet, suggested many agencies had a part to play (for example, the Department of the Prime Minister and Cabinet for coordination, the New Zealand Security Intelligence Service via the Combined Threat Assessment Group for assessing risk and New Zealand Police for Response).

41 Some of the opinions expressed above take a broad view of the definition of counter-terrorism, one that includes measures such as social inclusion (see *Part 9: Social cohesion and embracing diversity*). But even with that acknowledgement, the different views expressed above show that there is no common understanding about leadership of the counter-terrorism effort and what it means in practice.

3.4 Setting the strategy

42 Within the New Zealand public sector, multiple Public sector agencies often contribute to a single programme of work. In this situation it is common to create a strategy to clarify roles and responsibilities and coordinate, prioritise and align agencies' work.

43 In this section we discuss efforts to develop a counter-terrorism strategy, an approach to national risk management and priorities for collection and assessment of national security intelligence.

Counter-terrorism strategy

44 The need for a counter-terrorism strategy has been highlighted in a number of reviews. In 2013, *Counter-Terrorism: A review of the New Zealand CT landscape* noted that "New Zealand does not have an overarching policy document describing our national approach to counter-terrorism" and that "in the main, agencies are left to their own judgement with respect to the activities they embark upon with respect to reducing the risk of terrorism".[50] Also in 2013, the *Review of Arrangements for Coordinating National Security and Intelligence Priorities* recommended that a national strategy should be urgently completed to "provide a single set of organising principles for the national security system to prioritise and plan".[51] While this point was made about the lack of a strategy for the national security system, it also applies to the lack of a counter-terrorism strategy.

45 A 2015 report reiterated the need for a New Zealand counter-terrorism strategy. That report identified an insufficient emphasis on risk assessment, the absence of formalised arrangements that enabled ministers to weigh up the violent extremist or terrorist risk against other national security risks and the lack of whole-of-government counter-terrorism work programme management, reporting or evaluation. It also identified the continued absence of planned and regular public engagement on the terrorism risks facing New Zealanders at home and abroad and measures taken to counter those risks.

[50] Simon Murdoch, footnote 9 above at page 26.

[51] Jacki Couchman *Review of Arrangements for Coordinating National Security and Intelligence Priorities* (Department of the Prime Minister and Cabinet, July 2013).

46 Following this advice, Cabinet agreed in 2015 that the minister responsible for the New Zealand Security Intelligence Service and the Government Communications Security Bureau would lead public engagement on, and represent, the broader counter-terrorism work programme (which included the Department of Corrections, the Department of Internal Affairs, the Government Communications Security Bureau, Immigration New Zealand, the Ministry of Defence, the Ministry of Foreign Affairs and Trade, the Ministry of Justice, New Zealand Police, the New Zealand Security Intelligence Service and the Office of Ethnic Communities). Later that year, Cabinet directed officials to report to ministers with advice on the development and release of a public counter-terrorism strategy and public engagement plan.

47 In July 2016, the Security and Intelligence Board recognised the "urgent need for agencies to [sort out] New Zealand's counter-terrorism arrangements in line with ministerial expectations" and noted the continuing absence of an overarching strategy for counter-terrorism.

48 A *Counter-Terrorism Strategic Framework* was approved by the Security and Intelligence Board in 2018. This was not a detailed, comprehensive strategy document. It was a two page document intended to "support directional alignment across agencies and to act as a tool for supporting articulation of our [counter-terrorism] system". Its primary audience was not the public. It had not been developed in consultation with non-government parties. It did not assign leadership and responsibility to specific Public sector agencies for counter-terrorism prevention and Reduction activity. This was the only contemporary document guiding the counter-terrorism effort before 15 March 2019.

49 Although the agencies continued to support the development of a national counter-terrorism strategy, a strategy had not been adopted before 15 March 2019. A senior official spoke of their frustration with how long it has taken to develop a counter-terrorism strategy. They were also frustrated at the low prioritisation of counter-terrorism compared to other important national security issues such as pandemics and people smuggling.

50 As explained in Part 2, chapter 4, counter-terrorism activities have expanded to include Reduction activities to counter violent extremism. These activities range from early intervention programmes targeting those showing signs or vulnerabilities to radicalisation, through to community-based activities aiming to prevent the emergence of violent extremism by building social inclusion.

51 Before 15 March 2019, there were some activities underway that aimed to reduce the risk of violent extremism, such as the Young Person's Intervention Programme (see Part 8, chapter 6). We heard that Reduction had received little attention at the Security and Intelligence Board despite urging from some agencies and community groups (see *Part 9: Social cohesion and embracing diversity* for a description of efforts by community groups). There was progress in September 2018 when the Security and Intelligence

Board agreed to a *High-Level Framework for the Prevention of Violent Extremism*. This encompassed both the development of a multi-agency intervention programme providing tailored support to people at risk of violent extremism (building on the Young Person's Intervention Programme) and wider cross-agency efforts to promote social inclusion and diversity.

52 The *High-Level Framework for the Prevention of Violent Extremism* recognised that tension can arise when social inclusion is used as a tool for countering violent extremism, because it can risk stigmatising and alienating communities, thereby undermining social cohesion efforts. The focus was therefore on interventions with people who were noticeably at risk of engaging in violent extremism. It included broader efforts to build:

> *... strong, trust-based relationships with communities through proactive, broad-based engagement – ideally led by agencies with an enduring community presence and cultural capability. These relationships can then be accessed to engage on specific violent extremism issues in a targeting way if and where they arise.*

53 Progress was made in developing the multi-agency intervention programme. But the lack of specificity in what was being proposed for broader community engagement efforts meant that it was not clear what actions were to be taken, by when and by whom. There did not appear to be any consultation with community groups in the development of the *High-Level Framework for the Prevention of Violent Extremism*.

National Risk Management

54 In September 2015, after engaging with an expert panel, the Department of the Prime Minister and Cabinet produced a report recommending an approach and methodology for developing a National Risk Register. There was broad ministerial and interagency agreement for the development of a National Risk Register.

55 A 2016 report by the Auditor-General recommended that the Department of the Prime Minister and Cabinet should improve governance of national security risks (especially to provide better definition and clearer accountabilities of risk governance and management).[52] The Department of the Prime Minister and Cabinet responded to this in 2016 by developing a risk framework.

56 By November 2016, over 30 Public sector agencies had undertaken indicative risk assessments and considered existing agency risk management arrangements across the 4Rs. These agencies identified gaps and connections, developed some credible event scenarios, and assessed the likelihood and potential impacts of these events occurring over the next five years.

[52] Office of the Controller and Auditor-General *Governance of the National Security System* (2016).

57 In June 2017, the Department of the Prime Minister and Cabinet established the National Risk Unit to develop a National Risk Register. The first draft National Risk Register was produced in August 2018. It comprises approximately 40 risk profiles, including the Terrorism Risk Profile, each of which includes a description, rating and risk management measures. Although not approved by ministers, the draft National Risk Register has been informally adopted by the Department of the Prime Minister and Cabinet and shared with Public sector agencies to be used as part of their agency planning and their development of risk mitigation processes.

58 Following informal discussions with ministers in late 2018, officials recommended the release of the National Risk Report (a high-level summary of the National Risk Register) in January 2019. Officials suggested the audience for the National Risk Report would be key decision-makers in public and private organisations, including central and local government agencies, essential utilities and infrastructure providers. Officials suggested that its purpose would be to build public understanding and facilitate an open and transparent public debate about national risks. Despite strong recommendation from the Department of the Prime Minister and Cabinet, ministers did not agree to authorise public release of the National Risk Report.

59 In December 2018, officials recommended to the Security and Intelligence Board several changes to terrorism risk management across Reduction and Response activities. These included the introduction of a new annual strategic risk management cycle, commencing with a Combined Threat Assessment Group terrorism threat assessment (see Part 8, chapter 4). The first annual Combined Threat Assessment Group terrorism threat assessment was produced in December 2019 but was not publicly released. Officials also recommended elevating the responsibility for setting the New Zealand terrorism threat level from the Head of the Combined Threat Assessment Group to the Director-General of Security. This change occurred in mid-2019.

The government's priorities for national security intelligence

60 Two reviews into the intelligence system in 2009[53] recommended setting clear intelligence collection priorities for all agencies involved in collecting intelligence for national security purposes.

61 Before 2012, the Government Communications Security Bureau operated to requirements for collecting foreign intelligence set by the old Domestic and External Security Coordination system and endorsed by the Cabinet Committee of the same name.[54] Other Public sector agencies involved in intelligence collection initially did not have similar set requirements.

[53] Michael Wintringham and Jane Jones *National Security and Intelligence Framework for New Zealand* (2009); Simon Murdoch *Report to the State Services Commissioner: Intelligence Agencies Review* (2009).

[54] Office of the Inspector-General of Intelligence and Security *Report into Government Communications Security Bureau's process for determining its foreign intelligence activity* (2017).

62 In 2012 the first National Intelligence Priorities were developed for intelligence collection and assessment, and ranked to guide the level of effort. In 2012, counter-terrorism was set at a medium intelligence priority, as the threat of terrorism (as assessed by the Combined Threat Assessment Group) was "very low". At the time, the Officials' Committee on Domestic and External Security Coordination noted that the government's priorities "will be supplemented by more specific papers to be approved at officials' level (the national intelligence priorities papers)". The National Intelligence Priorities were expected to be reviewed every two years.

63 By March 2015, the Department of the Prime Minister and Cabinet had prepared a revised process for the continual review and updating of New Zealand's National Intelligence Priorities and advised that it would work with partner agencies to "translate these high-level questions into agency-specific actions". The Department of the Prime Minister and Cabinet recognised that this was needed in the absence of "an explicit overarching strategy for New Zealand's intelligence community".

64 In September 2015, ministers agreed 16 National Intelligence Priorities to replace the 2012 Priorities. The Priorities were in three groupings. Terrorist and violent extremist threats to New Zealanders at home and abroad were included in the high priority grouping. Ministers expected these National Intelligence Priorities would be used by chief executives to align the focus of intelligence sector efforts, prioritise work and reallocate additional resources when required. The associated Cabinet paper recorded expectations that the Priorities would support any specific warrants or other ministerial approvals required and ensure active sharing of information, expertise and resourcing across the New Zealand intelligence sector. They directed officials to "report back to Ministers in March 2016 on progress by the [wider intelligence sector agencies] in implementing the intelligence priorities, before the first annual report due to ministers in June 2016 on the performance of the intelligence sector delivering the priorities". This reporting back did not occur.

65 The Security and Intelligence Board agreed that the National Intelligence Coordination Committee would be responsible for the delivery of the Priorities overall and that it would focus on the top nine of the 16 Priorities (to set the intelligence requirements for assessment and collection). Eleven cross-sector intelligence Priority Coordination Groups were established, each with a coordinator. However, in October 2016 the Department of the Prime Minister and Cabinet reported to the Security and Intelligence Board that the "national intelligence priorities do not yet fully inform agency priority and planning processes". It was also reported that the Priority Coordination Groups had delivered mixed results, as there was:

a) neither a clear mechanism to provide assurance that customer requirements are being clearly communicated nor a consistent framework to assess progress or gaps;

b) no coordinating mechanism to support better measurement of resource allocation and outputs against each National Intelligence Priority; and

c) no comprehensive framework to underpin any future queries about New Zealand Intelligence Community collection against specific issues or targets.

66 Faced with these problems, some Public sector agencies developed their own internal prioritisation guidance. For example, the New Zealand Security Intelligence Service compensated for this lack of clarity by developing its *10-Year Operational Strategy (Project Sterling)* in 2016.[55] This resulted in the establishment of a strategic analysis function (see Part 8, chapter 5).

67 In 2017, the Department of the Prime Minister and Cabinet advised the Security and Intelligence Board that the intelligence prioritisation and coordination frameworks were not doing what they were designed to do. Following a new cross-agency process led by the Department of the Prime Minister and Cabinet, the Cabinet External Relations and Security Committee approved 16 equally-weighted National Security and Intelligence Priorities in December 2018. The paper seeking Cabinet approval of the new National Security and Intelligence Priorities noted that the Priorities would not prescribe how different agencies should implement their intelligence work plans. The paper observed that the actual level of an agency's ability to deliver on the Priorities depends on legislation, resourcing and capability. Also in December 2018, the Security and Intelligence Board agreed to disestablish the Priority Coordination Groups and replace them with a new system for delivering the National Security and Intelligence Priorities, facilitated by Sector Coordination Groups.

68 Despite their revised name, the National Security and Intelligence Priorities remain priorities for intelligence collection and assessment. An organising framework identified three types of intelligence and assessment effort and provided guidance on the relative focus for each of the priorities. These were:

a) the priorities where specialised secret intelligence collection capabilities can add value (this included terrorism);

b) the priorities where broader intelligence activities across a range of Public sector agencies are needed; and

c) the priorities where intelligence activity focuses on reporting and assessment, rather than significant New Zealand intelligence collection.

69 The 2012 and 2015 National Intelligence Priorities were expected to lead to prioritised areas of work and resources.[56] The 2018 National Security and Intelligence Priorities were not designed to guide day-to-day operational and longer-term strategic decisions of the intelligence and security agencies or the other Public sector agencies involved in the national security system.

[55] New Zealand Security Intelligence Service *The NZSIS 10-Year Operational Strategy (Project Sterling)* (June 2016).

[56] *Performance Improvement Framework*, footnote 42 above.

70 We were told that the National Security and Intelligence Priorities may be used by some agencies as a point of reference but their high-level nature means they are not helpful for providing guidance on how to prioritise both within and across the Priorities (for example, foreign interference versus terrorism). We were also told that the 2018 restructure of the National Security and Intelligence Priorities into an equally-weighted alphabetical list made them less clear as priorities and few Public sector agencies appear to have incorporated the Priorities into their organisational plans.[57]

71 The Government Communications Security Bureau and the New Zealand Security Intelligence Service interpreted the National Security and Intelligence Priorities as the "government priorities" under the Intelligence and Security Act (see Part 8, chapter 14), setting the outer parameters of their intelligence activities. Beyond that, their relevance is unclear. In a 2018 internal document, New Zealand Police expressed concerns about the costs of participating in the development of the National Security and Intelligence Priorities. They also had concerns about the "poor targeting of the performance framework".

72 The first three Sector Coordination Groups were established in February and March 2019 for the Priorities of foreign interference, Pacific regional security, and malicious cyber activity. Since 15 March 2019, responsibility for coordinating the terrorism National Security and Intelligence Priority is exercised jointly by the Counter-Terrorism Coordination Committee and the National Intelligence Coordination Committee.

The 2018 terrorism National Security and Intelligence Priority

73 The terrorism priority approved in December 2018 focused Public sector agencies on domestic as well as international terrorism threats. The domestic terrorism threats were described as "those that may arise in and against New Zealand or be carried out by New Zealanders overseas ... [and the] scope includes emerging trends and characteristics associated with overseas terrorist networks' links to New Zealand". The international terrorism threats were described as "threats against New Zealand's interests overseas in areas that have the greatest exposure for New Zealanders, and the trends and characteristics of emerging regional and global terrorism threats" which may impact on New Zealand. We note that the concepts "domestic terrorism" and "international terrorism" are used in ways which appear to differ from our glossary definitions.

74 This characterisation of terrorism as pervasive and not constrained by geographic distance and national boundaries was also reflected in the 2018 *Counter-Terrorism Strategic Framework*, which stated that terrorism is a threat that "New Zealand actively confronts, both globally and at home".

[57] The New Zealand Security Intelligence Service *The 2019 Terrorist Attacks in Christchurch: A review into NZSIS processes and decision-making in the lead up to the 15 March attacks (Arotake Review)* (June 2019) at page 20.

3.5 Performance monitoring and oversight

Performance monitoring

75 Several reviews of components of the national security system (see Part 8, chapter 2) have highlighted the light-touch approach to performance monitoring as an issue that should be addressed.[58]

76 The 2011 *New Zealand's National Security System* review stated that "given the significant spending on national security, government needs to ensure that it is achieving its goals in the most efficient manner possible".[59] Similarly, the 2014 *Performance and Improvement Framework* review stated that:

> *... the performance challenge for the [New Zealand Intelligence Community] is to clarify the scope of its role and then to create more seamless collaboration and efficient resource allocation amongst individual agencies ... . In setting national security priorities and determining the scope of the [New Zealand Intelligence Community's role], there should be a set of practicable and measureable targets ... against which the sector's performance can be assessed.*[60]

77 In 2017, the Department of the Prime Minister and Cabinet was working on a full set of performance measures for delivery of the National Intelligence Priorities approved in 2015 and updated in 2016. It advised the Security and Intelligence Board that there were still no measures to demonstrate impact. It noted that one of the factors "stopping intelligence and assessment about the national intelligence priorities from informing decision-making and policy-making to the fullest extent" was that:

> *... current priority descriptions are not clear enough, and don't provide enough guidance around what areas are of most importance within the priority, why they are important and what outcomes are sought. This also inhibits the development of an effective performance framework.*

78 We also observed that performance measures (as recorded in some agencies' annual reports) were subject to change between years.

79 The current position is that there is still no performance framework in place to measure the efficiency and effectiveness of New Zealand's intelligence community or counter-terrorism effort, or their delivery against the National Security and Intelligence Priorities.

---

[58] Simon Murdoch, footnote 9 above at page 26; Jacki Couchman, footnote 51 above.

[59] Simon Murdoch *New Zealand's National Security System* (April 2011) Section V: Value for Money at page 15.

[60] *Performance Improvement Framework*, footnote 42 above.

The role of the central agencies

80 In the New Zealand Public sector, the Department of the Prime Minister and Cabinet, Te Kawa Mataaho Public Service Commission (formerly the State Services Commission) and the Treasury are collectively called the central agencies.

81 Central agency oversight has involved a focus on advising chief executives how to achieve system-wide leadership and system results. The efforts of the central agencies, particularly Te Kawa Mataaho Public Service Commission and the Department of the Prime Minister and Cabinet, have concentrated on removing barriers to good performance and encouraging relevant parts of the Public sector to work together.

82 The Public Service Commissioner has had an oversight role in relation to leadership and governance of the intelligence and security agencies since the enactment of the Intelligence and Security Act. The Public Service Commissioner's functions include acting as the employer of chief executives and reviewing the performance of departments. This involves considering the overall performance of the chief executive and the agency. It may also include specific matters for performance development and feedback, as agreed with the chief executive, but does not extend to an ongoing assessment of the operational decisions of the agencies. An Assistant Commissioner at Te Kawa Mataaho Public Service Commission told us it was not the role of Te Kawa Mataaho Public Service Commission to monitor the collective performance of the counter-terrorism agencies nor the Public sector agencies involved in the counter-terrorism effort.

83 A senior manager at the Treasury advised that while the Treasury monitored the financial performance of Public sector agencies (at the appropriation level), it does not monitor the outcomes or outputs that agencies produce with this funding. The Public Finance Act 1989 makes chief executives responsible for what is achieved with their resources.

84 The Department of the Prime Minister and Cabinet advised that it is "not its role or mandate to monitor national security and intelligence sector agencies' performance against [the National Security and Intelligence Priorities]", rather it is interested in "how the sector performs in relation to collectively providing intelligence and assessment to support decision-making". This includes the counter-terrorism effort.

Oversight by the Office of the Auditor-General

85 The Office of the Auditor-General carries out annual audits of Public sector agencies' financial reports. The Auditor-General is usually responsible for auditing the performance of Public sector agencies to examine their efficiency and effectiveness. Performance audits provide the public with independent assurance that Public sector agencies are delivering what they have been asked to and are operating lawfully.

86 Under the Public Finance Act 1989, Public sector agencies must provide financial and performance information to the Auditor-General at the end of each financial year for audit.[61] But the intelligence and security agencies are not required to provide end-of-year performance information to support the annual appropriations (funding) legislation.[62] The Office of the Auditor-General has interpreted this to mean that the intelligence and security agencies are excluded from the Public Finance Act requirement to provide performance information for audit by the Auditor-General. The Treasury has confirmed this interpretation. The Auditor-General does not, therefore, audit the performance or operational effectiveness of the intelligence and security agencies.

Oversight of the intelligence and security agencies

87 Significant oversight of the Government Communications Security Bureau and the New Zealand Security Intelligence Service is specified in the Intelligence and Security Act.

88 Because the Intelligence and Security Act gives broad powers to the Government Communications Security Bureau and the New Zealand Security Intelligence Service to fulfil their functions and objectives, robust and multi-layered oversight is important. The Inspector-General of Intelligence and Security and the Parliamentary Intelligence and Security Committee are the primary external oversight mechanisms for the Government Communications Security Bureau and the New Zealand Security Intelligence Service. Both of these oversight bodies were established by legislation in 1996 and are now governed by the provisions of the Intelligence and Security Act (see Part 8, chapter 14 for more information on the oversight roles of these bodies).

3.6 Developments since 15 March 2019

89 Cabinet approved a high-level *Countering terrorism and violent extremism national strategy overview* in September 2019, which was published on the Department of the Prime Minister and Cabinet's website in February 2020.[63] It:

a) identifies broad, thematic counter-terrorism activities focusing on Reduction but also includes Readiness, Response and Recovery;

b) identifies the importance of public engagement and a public information plan; and

c) recognises the linkage to social cohesion activities.

90 It was not developed in consultation with communities, local government and the private sector.

[61] Public Finance Act 1989, section 45D.

[62] Public Finance Act 1989, section 15A(4)(a).

[63] Department of the Prime Minister and Cabinet, footnote 49 above.

3.7 Gaps in the leadership and oversight of the counter-terrorism effort

Lack of political ownership and informed public debate

91 There has been limited political ownership of, and public discussion on, the threat and risks of domestic terrorism in New Zealand. And the overall counter-terrorism effort is not well understood by most ministers, other politicians, the wider public service or the New Zealand public.

92 Any public discussion has largely focused on controversies that have caused embarrassment for intelligence and security and law enforcement agencies (see Part 8, chapter 2). The few public-facing documents produced about the counter-terrorism effort are not particularly revealing and did not actively engage the public. This means there has been little informed public debate about the threat of domestic terrorism, what is done on behalf of the public by the Public sector agencies involved in the counter-terrorism effort and how the public can contribute.

Absence of strategic analysis and advice across the counter-terrorism effort

93 Good Public sector management practice includes following and implementing relevant regulatory frameworks, existing policy, operational guidance and administrative procedures in ways which give effect to their intended purposes.

94 In addition, the public service has a duty of stewardship to look ahead and provide advice about future challenges and opportunities New Zealand faces. It is the responsibility of chief executives to steward their agency's capability, and capacity to offer free and frank advice. This involves providing proactive advice on emerging problems, vulnerabilities and opportunities for policy performance improvement. In many New Zealand Public sector agencies, these functions are exercised by strategic policy teams.

95 It is not clear who holds responsibility to look across the counter-terrorism effort to identify such risks and gaps and provide advice to ministers. Although the Department of the Prime Minister and Cabinet has a national security policy team, it does not exercise this role. Despite this role being in the Security and Intelligence Board's Terms of Reference it has not carried it out (see 3.3 Leadership and coordination). The assessment agencies provide ministers with intelligence products, but they stop short of providing advice on what to do about the risks or opportunities that may be identified in those products. That responsibility falls on the policy or operational agency relevant to the specific issue (see Part 8, chapter 4). This is due to a separation of assessment from policy making. We heard from one minister that they were surprised and frustrated by this arrangement and the effect was that ministers received threat assessments without proposed policy or operational responses.

96 The minutes of the Security and Intelligence Board and the Counter-Terrorism Coordination Committee do not demonstrate that these interagency coordinating groups were working together to provide collective insights from assessments.

Limited availability of external advice

97 New Zealand's *National Security Handbook* observes that "local government, quasi-government agencies, and the private sector have increasingly important roles in the public sector". Think tanks focused on national security issues are an example of such "quasi-government agencies". They are an established feature of the national security landscape overseas. Such organisations can encourage and inform public debate, facilitate interaction between the private and public sector and offer contestable external advice to government and Public sector agencies.[64]

98 We did not observe similar relationships between the New Zealand national security system and think tanks in relation to counter-terrorism. Although there are think tanks in New Zealand that focus on national security issues, such as the Centre for Strategic Studies, they do not appear to be utilised by Public sector agencies involved in the counter-terrorism effort in the ways that such bodies are in other countries.

No system-level standards or performance monitoring

99 There is no framework for setting system-level performance standards and accepted best practice for the counter-terrorism effort. This means there is no way to monitor performance or measure the effectiveness of the counter-terrorism effort as a system or to hold Public sector agencies to account if their contributions do not meet the standards.

[64] Allan Gyngell "The Rumble of Think Tanks: National Security and Public Policy Contestability in Australia" in *War, Strategy and History: Essays in Honour of Professor Robert O'Neill* edited by Daniel Marston and Tamara Leahy (ANU Press, Acton, Australia, 2016) at pages 265–284.

3.8 Concluding comments

100 Leadership and coordination of New Zealand's decentralised counter-terrorism effort is non-directive. The Department of the Prime Minister and Cabinet's leadership role was never more than coordination of the multi-agency counter-terrorism effort.

101 Between 2014 and 2019 progress was made:

a) A new ministerial portfolio for national security and intelligence was created in 2014.

b) The Specialist Coordinator for the counter-terrorism effort was appointed in 2016.

c) The Intelligence and Security Act 2017 was passed, which reformed the intelligence and security agencies' authorising environment.

d) A National Risk Register was developed in 2018. While the Register has not yet been approved and published by the government, the risk profiles are being used by officials to support a more strategic and proactive approach to risk management.

e) A more clearly defined interagency counter-terrorism work programme was progressed by the Security and Intelligence Board in 2018 (largely driven by the Specialist Coordinator).

f) The Security and Intelligence Board approved the *Counter-Terrorism Strategic Framework* and the *High-Level Framework for the Prevention of Violent Extremism* in 2018.

102 However, there have been significant challenges and, as just described, there are gaps in the leadership and oversight of the counter-terrorism effort that have yet to be addressed.

103 In later chapters we will discuss how this has played out in practice, in particular between the counter-terrorism agencies as to their respective roles and coordination of activities, online capability, target discovery and information sharing.

Chapter 4: Assessment of the terrorism threatscape

Distressing Content

4.1 Overview

1 Our Terms of Reference required us to make findings as to whether relevant Public sector agencies failed to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats.

2 Making informed decisions about where to concentrate counter-terrorism resources requires a comprehensive understanding of the threatscape. Critical to this is strategic intelligence assessment on the threat of terrorism. Such assessment enables the counter-terrorism effort to scan the horizon to look for new and emerging threats. It lifts the focus from today's presenting threat and reminds operational agencies of the need to anticipate future threats.

3 In this chapter we:

a) review the role and expectations of the two agencies whose primary function is to produce intelligence assessments – the National Assessments Bureau and the Combined Threat Assessment Group;

b) discuss the development of a national assessments programme and the focus and capacity of the National Assessments Bureau and the Combined Threat Assessment Group;

c) set out the gaps we observed in the assessment system;

d) scrutinise the perception of the terrorism threatscape before 15 March 2019;

e) examine the perception of the threat of right-wing extremist terrorism before 15 March 2019; and

f) describe the terrorism threat level assessments.

4 Other agencies also have assessment functions. The New Zealand Security Intelligence Service's Strategic Intelligence Analysis team, established in 2016, is discussed briefly in this chapter, but in more depth in Part 8, chapter 5. New Zealand Police's assessment function is discussed in Part 8, chapter 6. In Part 8, chapter 9, we discuss practices related to the sharing of strategic intelligence assessments across Public sector agencies.

4.2 Roles of the National Assessments Bureau and the Combined Threat Assessment Group

5 The National Assessments Bureau and Combined Threat Assessment Group combine multiple pieces of intelligence from various sources (for example, intelligence from other Public sector agencies and international partners) to produce assessments.

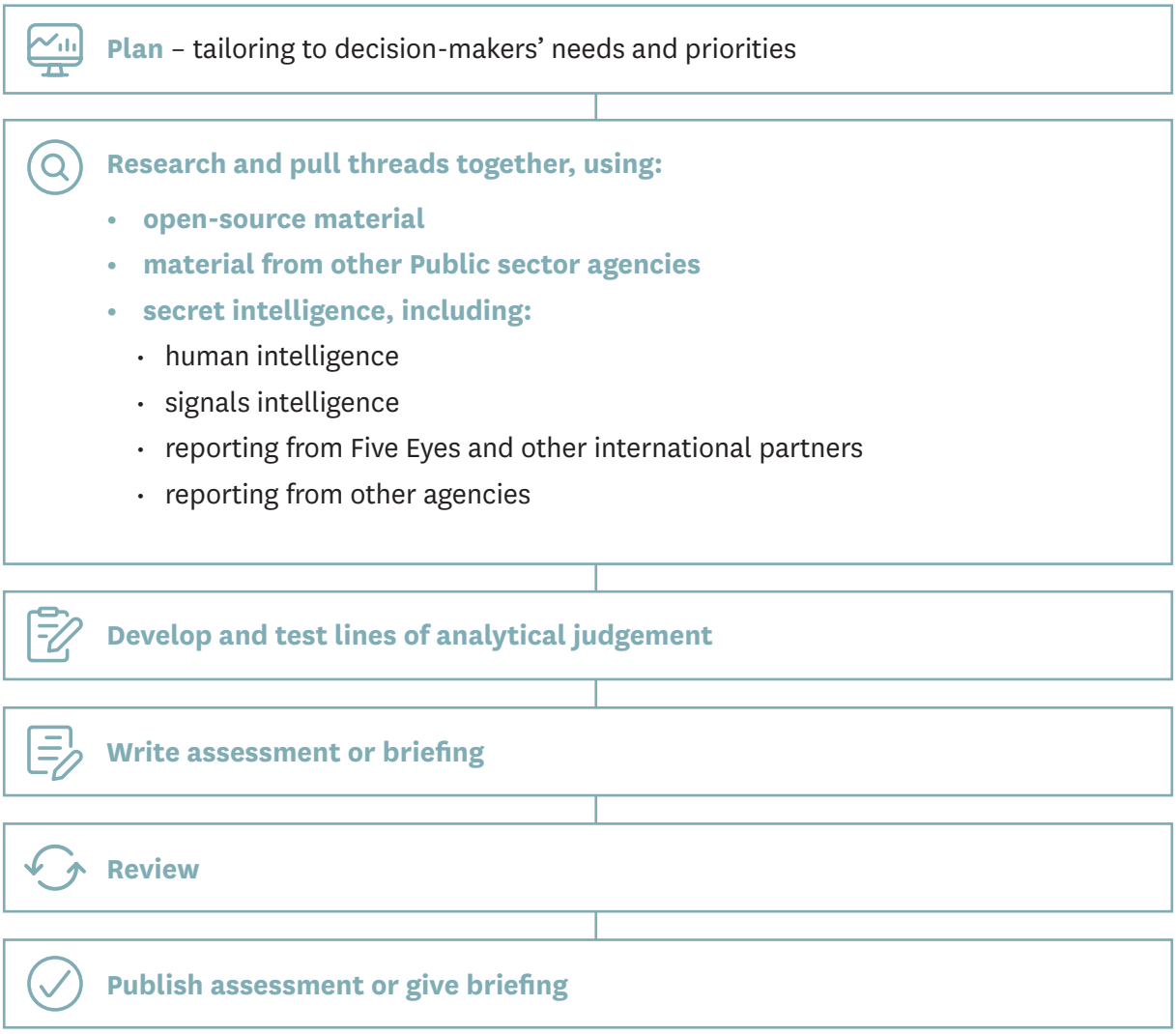
6 The National Assessments Bureau is part of the Department of the Prime Minister and Cabinet (see Part 8, chapter 3). The National Assessments Bureau provides medium to long-term assessments on a broad range of issues. These include, but are not confined to, terrorism. Its products are generally designed to inform policy formation and decision-making. The National Assessments Bureau does not make recommendations or offer advice in relation to its assessments. This is done by policy agencies responsible for the specific policy issue (such as the Ministry of Business, Innovation and Employment, the Ministry of Foreign Affairs and Trade and the Ministry of Justice).

7 The Combined Threat Assessment Group is an inter-agency group hosted by the New Zealand Security Intelligence Service. The Combined Threat Assessment Group's mandate is to assess threats from terrorists likely to result in harm to New Zealand, its citizens or interests, both domestically and internationally.[65] As is the case with the National Assessments Bureau, it does not make recommendations or offer advice in relation to its assessments. The Combined Threat Assessment Group supports agencies such as New Zealand Police and the Ministry of Foreign Affairs and Trade to make tactical or operational decisions. That said, the Combined Threat Assessment Group sometimes provides broader strategic assessments, such as its *New Zealand Terrorism Threatscape* assessment.

8 The Combined Threat Assessment Group's terrorism mandate is more focused than that of the National Assessments Bureau. We were told that the National Assessments Bureau was not focused on the domestic terrorism threatscape because of an agreed division of effort with the Combined Threat Assessment Group. There is however, no written memorandum of understanding or other formal agreement to this effect. In 2012, 2016 and 2018 the National Assessments Bureau produced strategic intelligence assessments used to inform the development of the National Security and Intelligence Priorities, including the terrorism priority (see Part 8, chapter 3).

[65] The Combined Threat Assessment Group also has a mandate for assessments relating to violent protest in New Zealand and abroad, but this forms a minimal part of its work.

Figure 43: How intelligence assessments are prepared



4.3 Expectations of the National Assessments Bureau and the Combined Threat Assessment Group

9 Expectations of the National Assessments Bureau have been established through Cabinet decisions and legislation.

10 In 2010, Cabinet amended the mandate of the National Assessments Bureau to enable its Director to "deliver assessment products that call on resources of all [New Zealand Intelligence Community] agencies and are relevant to all aspects of Cabinet-agreed national security agenda and priorities". Cabinet also made the Director of the National Assessments Bureau responsible for the "development of a national assessment programme that includes domestic and external intelligence" and for "leading the [New Zealand Intelligence Community] in delivering the national assessments programme as mandated by Cabinet and ensuring effective integration of agency contributions to it".

11 The Intelligence and Security Act 2017 provides for the chief executive of the Department of the Prime Minister and Cabinet to designate an employee to undertake "intelligence assessments on events and developments of significance to New Zealand's national security, international relations and well-being and economic well-being to Ministers, departments and any other persons considered appropriate and advising departments on best practice in relation to the assessment of intelligence".[66] In practice, this is delegated to the Director of the National Assessments Bureau.

12 A 2012 review of the Combined Threat Assessment Group noted its core function should be to enable intelligence and security agencies to recognise and address threats arising from terrorism that are likely to require a multi-agency operational response.[67] A follow up review in 2018 stated that "evidence about possible attacks in New Zealand" has "brought a greater focus to the homeland security risk environment", such that there is "a need to expand our own indigenous threat intelligence effort".[68]

[66] Intelligence and Security Act 2017, section 233.

[67] Simon Murdoch Review *of CTAG* (April 2012) at page 4.

[68] Simon Murdoch *CTAG* 2018: *Its placement in New Zealand's counter-terrorism system architecture and its location; an independent view* (27 July 2018).

13 In addition, the terrorism National Security and Intelligence Priority as agreed through Cabinet decisions of 2012, 2015, 2016, and 2018 set broad parameters for the assessment of intelligence with respect to terrorism threats. The parameters of the 2018 terrorism Priority provide for:

> *The assessment of intelligence to identify and understand domestic terrorism threats … [for] domestic terrorism scope includes emerging trends and characteristics associated with overseas terrorist networks' links to New Zealand. Beyond domestic threats, the narrower international scope of this Priority focuses on the use of intelligence and assessment to identify and understand terrorist threats against New Zealand's interests overseas … and the trends and characteristics of emerging regional and global terrorism threats, which may impact New Zealand, New Zealand's interest and New Zealanders.*

14 Effective identification of emerging threats requires capability and capacity to look five to ten years ahead (horizon scanning). In 2003, the then Auditor-General reported that an "over the horizon" function was critical to New Zealand's national security system.[69]

4.4 A national assessments programme?

15 As noted, in 2010 Cabinet mandated the development of a national assessments programme led by the National Assessments Bureau with functions extending to the assessment of intelligence on domestic as well as international issues. Between 2011 and 2012, some progress was made in fulfilling the Cabinet mandate. The separate but associated National Assessments Committee, chaired by the Director of the National Assessments Bureau and comprised of eleven members,[70] coordinated the production of ten national security assessments on threats to New Zealand's security, including terrorism.

16 In May 2013, the National Assessments Bureau presented a paper to the Officials' Committee for Domestic and External Security Coordination. The paper proposed that the National Assessments Bureau would implement its changed mandate, and progress a shared national assessments programme, by reshaping the National Assessments Committee so that it had greater emphasis on tasking, oversight and quality assurance for assessment reporting.

17 Several high quality assessments focused on New Zealand's domestic terrorism environment were produced during this time (2013–2014) through the National Assessments Committee. These included a report by the New Zealand Security Intelligence Service and two reports from New Zealand Police, which discussed the terrorist threat posed by the extreme right-wing.

[69] Office of the Controller and Auditor-General, footnote 8 above at pages 39–40.

[70] The National Assessments Committee comprised the Combined Threat Assessment Group, the Department of the Prime Minister and Cabinet, the Government Communications Security Bureau, Immigration New Zealand, the Ministry of Defence, the Ministry of Foreign Affairs and Trade, New Zealand Customs Service, the National Assessments Bureau, the New Zealand Defence Force, New Zealand Police and the New Zealand Security Intelligence Service.

18 In 2014, the National Assessments Committee was replaced by the National Intelligence Coordination Committee. Our review of the National Intelligence Coordination Committee's meeting minutes since 2016 show that it was predominantly focused on the coordination and implementation of the National Security and Intelligence Priorities, with little attention devoted to a coordinated national assessments work programme. We have seen no evidence of a coordinated national assessments programme since 2014, despite it being the responsibility of the National Assessments Bureau – as directed by Cabinet – to ensure there was such a programme.

4.5 Focus of the National Assessments Bureau

19 The threat of domestic terrorism was not a priority for the National Assessments Bureau and it did not provide any assessments solely focused on domestic terrorism.

20 The National Assessments Bureau's focus was geopolitics and security dynamics within different countries and regions and what they meant for New Zealand's national security interests. It tended to concentrate more on the foreign policy and trade aspects of national security, rather than the domestic aspects (though there is overlap between the two).

21 In response to feedback from the agencies using their intelligence products, the National Assessments Bureau became increasingly customer focused after February 2013. We were told that assessments are of no value unless they are supporting decision-making and that if someone "is not really interested in reading [an assessment], then you have to ask yourself, what is the value, what is the point [of the assessment]".

22 This meant the National Assessments Bureau primarily addressed topics or themes on which its customers – usually the Ministry of Foreign Affairs and Trade – had asked for assessments. This explains its focus on foreign policy, security and trade issues, as highlighted by the 2014 *Performance Improvement Framework* review of the New Zealand Intelligence Community. That review observed that the National Assessments Bureau's customers were reluctant to accept a reduction in foreign policy assessments in favour of a greater attention to national security issues.[71] We heard from Howard Broad, former Deputy Chief Executive of the Department of the Prime Minister and Cabinet, that:

> *[When] you start to press [the National Assessments Bureau] on domestic issues and the relationship between foreign and domestic ones, they run out of legs a bit. We didn't have the capability.*

[71] *Performance Improvement Framework*, footnote 42 above at page 23.

4.6 Focus of the Combined Threat Assessment Group

23 We were told that, before 15 March 2019 "the vast numerical majority of [the Combined Threat Assessment Group's] product [was] focused internationally". Of the products that did focus substantively on the New Zealand terrorism threatscape, most were tactical reports about security arrangements for visiting international dignitaries. Increased demand for these tactically-focused threat assessments meant the Combined Threat Assessment Group lacked the capacity to produce in-depth strategic assessments on the domestic terrorism environment. The New Zealand Security Intelligence Service told us that in response, from late 2017, its Strategic Intelligence Analysis team assumed the function of strategic assessment for counter-terrorism. Even so, the primary focus of the Strategic Intelligence Analysis team was guiding the operational activity of the New Zealand Security Intelligence Service. This meant it performed a different function to the Combined Threat Assessment Group, whose assessments are intended to inform the approach to counter-terrorism at a whole-of-system level. We discuss the Strategic Intelligence Analysis team more below and in Part 8, chapter 5. The New Zealand Security Intelligence Service told us that in June 2020 the strategic assessment function was transferred to the Combined Threat Assessment Group.

24 Of the Combined Threat Assessment Group's regular domestic products, the *National Terrorism Threat Assessment* has the most significant implications for the counter-terrorism effort. It informs the approach to counter-terrorism at a whole-of-system level. The *National Terrorism Threat Assessment* is comprised of two components – the threat narrative, which describes the terrorist threatscape in New Zealand and internationally, and the threat level, which assesses the likelihood of a terrorist attack in New Zealand.

25 In the second half of 2018, the Counter-Terrorism Coordination Committee chaired by the Specialist Coordinator (see Part 8, chapter 3) reviewed the terrorism risk management system, including the relationship between threat assessment, risk assessment and risk mitigation. One weakness they identified was the lack of an annual national terrorism threat assessment. A subsequent draft Cabinet paper said that:

> *… moving to an annual assessment would support a more deliberate and systematic approach to counter-terrorism. If done well it will have the potential to better inform counter-terrorism system gaps and priorities.*

26 In December 2018, a paper to the Security and Intelligence Board proposed the "production by [the Combined Threat Assessment Group] of an annual New Zealand terrorism threat assessment to inform security posture and as a key input to support determination of counter-terrorism priorities". This was seen as the "key starting point" for the terrorism risk assessment cycle and was proposed to be a "strategic assessment document that provides a comprehensive picture of the New Zealand terrorism threatscape". The Security and Intelligence Board then confirmed that the Combined Threat Assessment Group would produce an annual New Zealand terrorism threat assessment and "[a]greed that a regular terrorism threat statement/update would be published". It is unclear from the meeting minutes whether this meant published for officials only or for the public.

4.7 Capacity of the National Assessments Bureau and the Combined Threat Assessment Group

National Assessments Bureau

27 For much of its existence, the National Assessments Bureau has had a full-time equivalent staff of 30, including 21 analysts split across three teams, each with a manager and overseen by a director. The National Assessments Bureau seldom reached full analytical capacity, partly because of the significant time lag in bringing staff on board, which was contributed to by the lengthy security clearance process. We were told that in 2015 staffing was so low as to be below a credible minimum.

28 The 2016 Strategic Capability and *Resourcing* Review had envisaged growing the strategic assessments function from 21 analysts to 34 over four years. But reprioritisation over the past five years saw the increased resourcing shift to other areas. In July 2019, there were only three more analysts (and a further four recruitments in progress) at the National Assessments Bureau than there were before the Strategic Capability and *Resourcing* Review.

Combined Threat Assessment Group

29 For much of its existence, the Combined Threat Assessment Group has had a full-time equivalent staff of five to seven analysts plus a manager, usually seconded from the wider New Zealand Intelligence Community or international partner agencies. A 2012 review of the Combined Threat Assessment Group commented on its capacity issues.[72] At that time it had an acting manager, plus five seconded staff.

30 We were told that the secondee model for the Combined Threat Assessment Group has its strengths, contributing to agency diversity, experience, access to systems and relationships. However, it also creates vulnerabilities as the workforce can be subject to staff turnover and associated lack of institutional memory. Some agencies have not replaced secondees or there have been gaps between secondments.

[72] Simon Murdoch, footnote 68 above at page 13.

31 To mitigate these vulnerabilities, the New Zealand Security Intelligence Service has increased its contribution to the Combined Threat Assessment Group staffing, management and governance since the 2012 review. It now contributes six staff to the Combined Threat Assessment Group (only two of whom are funded by a cost-sharing arrangement between contributing agencies). More recently the Combined Threat Assessment Group has hosted secondees from New Zealand's Five Eyes partners. Despite the New Zealand Security Intelligence Service's increased contribution, the Combined Threat Assessment Group's overall capacity had not improved since the 2012 review.

32 We were told that nine months after 15 March 2019, the Combined Threat Assessment Group still had the same number of staff (six analysts) as before the terrorist attack and that having six to eight analysts split across the domestic and global environments presented "real capacity challenges". It was suggested to us that a modest expansion of three to four analysts would improve the Combined Threat Assessment Group's capacity to assess threats to New Zealand, domestic and international.

4.8 Gaps in the assessment system

Lack of a national assessments programme

33 The National Assessments Committee offered a promising vehicle for the coordination of a national assessments programme, but it was disbanded in 2014. Its replacement, the National Intelligence Coordination Committee, was predominantly focused on coordinating the implementation of the National Security and Intelligence Priorities. As a result, there is no coordinated national assessments programme.

34 Greater coordination and integration of the assessment function is required. One way of achieving this would be to co-locate or combine the National Assessments Bureau and the Combined Threat Assessment Group. Both agencies have an independent assessment mandate, while operating within other agencies. They use similar methods and in some areas their products overlap. To encourage more integration of the assessment function, the 2016 Cullen-Reddy Report recommended that the government review the current placement of the Combined Threat Assessment Group within the New Zealand Security Intelligence Service and consider whether it might be more appropriately situated within the National Assessments Bureau.[73] This review does not appear to have been done. We return to this question in *Part 10: Recommendations*.

[73] Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM, footnote 38 above at page 60.

Lack of regular strategic assessment of the threatscape

35 The lack of a regular system-wide strategic assessment of the threatscape was identified by the Department of the Prime Minister and Cabinet in a 2014 paper to the Security and Intelligence Board. This paper reported that there was a "lack of understanding of the potential changes and future developments in the New Zealand security environment". The paper also:

a) noted that the Combined Threat Assessment Group assessments "tell us what the threat level is now" and that "planning and investment for the medium-to-long term could be hampered by a lack of ongoing assessment of terrorism trends and activity in New Zealand, including trends relating to terrorist tactics, weapons and methods"; and

b) recommended that the National Assessments Committee produce an assessment of the New Zealand terrorism threatscape at least annually, with a focus on Islamist extremist terrorism and violent extremism, including assessing trends over the coming three to five years.

36 An assessment of the domestic threat from Islamist extremist and other sources of terrorism was produced in 2014, including trends over the coming three to five years, but this assessment was not repeated.

37 In July 2015 the Combined Threat Assessment Group produced the *New Zealand Terrorism Threatscape*. An updated version of this assessment, although scheduled for July 2017, was not produced until January 2018 (due to a lengthy review and consultation process). During this period, the National Assessments Bureau produced no strategic intelligence assessments of New Zealand's terrorism threatscape.

38 The New Zealand Security Intelligence Service's Strategic Intelligence Analysis team began producing its quarterly *New Zealand Terrorism Updates* in December 2017.

39 We were told that the New Zealand Security Intelligence Service's baselining project (see further below and Part 8, chapters 5 and 10) was initiated, in part, to compensate for the lack of strategic intelligence assessments on the evolving terrorism threatscape produced elsewhere in the system.

Limited horizon scanning capability

40 Seventeen years after the 2003 Auditor-General review had reported that an "over the horizon" capability was critical to New Zealand's national security system (see 4.3 Roles of the National Assessments Bureau and the Combined Threat Assessment Group), the intelligence assessment agencies (and indeed the entire national security system) are still lacking capability in this area.

41 We heard from several senior officials about their concern with the lack of horizon scanning capability and capacity in New Zealand's national security system. We were told that the National Assessments Bureau's "focus and resourcing did not prepare it particularly well for that longer-term work". That same person reflected:

> *What I don't see across [the National Assessments Bureau and the Combined Threat Assessment Group] is a foresight function designed to look beyond the tactical and say, five to ten years out. … I don't see the teams who are using data analytics tools or good quantitative data; a lot of it is judgement and pulling pieces of covert data together.*

42 Andrew Kibblewhite, former Chief Executive of the Department of the Prime Minister and Cabinet, agreed that the national security system's capability to regularly scan the horizon in the medium to long term for emerging threats and matters of strategic importance was not well developed. He said it was done "in bits and pieces in the system at the moment". Howard Broad, former Deputy Chief Executive of the Department of the Prime Minister and Cabinet, said that the Security and Intelligence Board sometimes engaged in horizon scanning, but it "was not systematic". He noted that, "to some extent", dedicated horizon scanning was "an expectation placed on the National Assessments Bureau".

43 We were told that Singapore, the United Kingdom and the United States of America have dedicated horizon scanning units that look five to ten years ahead, but that this is not the case in New Zealand because of the National Assessments Bureau's limited resources and customer focus.

44 Rebecca Kitteridge, the Director-General of Security, also commented on this gap:

> *I always thought it would be tremendous … if you had periodically, at the centre, a strategic look forward into what is the environment and what does that mean for us and what does it mean for our capability and resourcing and priorities, that gives you a natural forward look. You don't have that at the moment.*

Lack of assessment of the online world

45 There was limited analysis by the National Assessments Bureau and the Combined Threat Assessment Group of the formative role of the internet in the radicalisation, mobilisation and preparation activities of terrorists. We have seen only one shared report in the past decade, published by the Combined Threat Assessment Group and the New Zealand Security Intelligence Service, that substantively assessed online extremist activity in New Zealand.

Lack of focus on non-Islamist extremist threats

46 As we will illustrate in the next section, in the years before 15 March 2019 the primary focus of intelligence assessment was on the presenting threat of Islamist extremist terrorism. Before 2018, assessments by the National Assessments Bureau and the Combined Threat Assessment Group did not feature the threat of non-Islamist extremist terrorism.

47 When we asked Andrew Kibblewhite, former Chief Executive of the Department of the Prime Minister and Cabinet, about whether the system was looking beyond the risk of Islamist extremist terrorism, he told us:

> *I would have expected the [New Zealand Security Intelligence] Service and [the Combined Threat Assessment Group] to be looking at the whole violent extremism terrorism type risk.*
>
> ...
>
> *If you'd said "is there a terrorist risk out of right-wing extremism?" I would have said "yes", but ... I probably would have used the precise words "I don't think we are that concerned about it [in New Zealand]".*
>
> ...
>
> *I would have thought that [right-wing extremism] would have been within what [the New Zealand Security Intelligence Service and the Combined Threat Assessment Group] would have scanned. It would have been within their scanning space. I wouldn't have known how intensively they had scanned it.*

48 Andrew Kibblewhite noted further to us that:

a) *[the Security and Intelligence Board] tended to be guided by experts (in this case mainly by [the New Zealand Security Intelligence Service and Combined Threat Assessment Group]) on matters of the terrorism threat;*

b) *in this case those experts were not identifying right-wing extremism as a particular risk; and*

c) *this contributed to [the Security and Intelligence Board] itself not emphasising the importance of right-wing extremism as a risk.*

49 Andrew Kibblewhite's comments are understandable. For instance, the Combined Threat Assessment Group's July 2015 *New Zealand's Terrorism Threatscape* assessment was that Islamist extremist terrorism was the primary threat. This could be taken to imply that other threats had been assessed. As far as we can tell, this was not the case.

4.9 Perceptions of the terrorism threatscape before 15 March 2019

A focus on international terrorism...

50 In examining the terrorism threatscape as perceived before 15 March 2019, we have considered the assessments issued by the National Assessments Bureau, the Combined Threat Assessment Group, intelligence products from other agencies, and what we were told in interviews and by community members, including Muslim individuals and communities.

51 The primary focus of terrorism intelligence assessments by the National Assessments Bureau and the Combined Threat Assessment Group was international terrorism. These assessments rarely discussed the domestic terrorism threat.

52 Between 2010 and 2018 the National Assessments Bureau published just under 400 formal assessments on terrorism and/or violent extremism. None of these was solely focused on the threat of domestic terrorism.

53 We were told that the National Assessments Bureau focused more on the international terrorism environment and less on the domestic terrorism environment because that was the agreed division of effort with the Combined Threat Assessment Group.

54 The Combined Threat Assessment Group receives significant numbers of international partner intelligence assessments. Unsurprisingly, the vast majority of assessments distributed by the Combined Threat Assessment Group were internationally focused. Such assessments can be produced and distributed quickly. We were told that:

a) at least half of the effort of two senior staff in the Combined Threat Assessment Group (who were presumably supported by analysts within the Combined Threat Assessment Group) was on domestic terrorism;

b) domestic reporting takes more time and requires more analysis and coordination (primarily with other Public sector agencies) than reporting on international terrorism; and

c) therefore, the ratio of domestically-focused to internationally-focused assessments produced by the Combined Threat Assessment Group in a given year does not provide the full picture of its effort.

55 Most of the Combined Threat Assessment Group assessments that focused substantively on the domestic terrorism threat were reports about security arrangements for events and therefore were operational in character. There were few strategic assessments of the domestic terrorism environment.

56 Threat assessments dealing with terrorism indicated that the terrorist threat to New Zealanders was greater when they were outside New Zealand. For example, in 2016, the National Assessments Bureau stated that "international terrorism is almost certain to remain a serious threat to New Zealanders, mostly abroad". And in January 2018, the Combined Threat Assessment Group assessed that there was a higher general likelihood of a New Zealander being harmed in an international terrorist incident than one occurring in New Zealand.

57 Andrew Kibblewhite, former Chief Executive of the Department of the Prime Minister and Cabinet and Andrew Hampton, Director-General of the Government Communications Security Bureau both confirmed the dominant focus for intelligence assessments about terrorism had been on international rather than domestic terrorism.

… primarily on the threat of Islamist extremist terrorism

58 From 2010–2019 the intelligence assessments of the National Assessments Bureau and the Combined Threat Assessment Group considered the terrorist threat to New Zealand and New Zealanders as coming largely from Islamist extremism. So too did assessments from the New Zealand Security Intelligence Service and New Zealand Police.

59 Such assessments reflected the rise of the new "main terrorist threat", Dā'ish, in the Middle East. As described in Part 8, chapter 2, the prevalence of lone actor terrorists inspired by Dā'ish presented serious challenges for intelligence and security agencies around the world.

60 There were numerous Dā'ish and Al Qaeda-inspired attacks in Western countries, including in Denmark, France, the United Kingdom and Australia. Dā'ish-inspired terrorism was a real threat in New Zealand, requiring at times the full focus of the resources available to the counter-terrorism agencies.

61 From 2016 onwards, assessments continued to evaluate Islamist extremism as the primary terrorist threat to New Zealand and New Zealanders. For example:

a) In 2016, a New Zealand Police intelligence report, *New Zealand's Islamist Extremist Landscape,* stated that more New Zealanders were vulnerable to extremist messaging due to the pervasive nature of Dā'ish's propaganda, which had proven more effective at attracting disaffected young males than other extremist groups.

b) The Combined Threat Assessment Group's 2018 assessment of the New Zealand terrorism environment stated that "in spite of ongoing losses in Syria and Iraq, [Dā'ish] will continue to exert itself as a terrorist and insurgent group with international influence and reach … the overall level of support for [Dā'ish] among New Zealand-based Islamist extremists does not seem to have changed markedly … though the manifestation of support for radical Islam continues to evolve".

c) The New Zealand Security Intelligence Service similarly concluded in 2018 that "[Dā'ish's] territorial decline has not had any marked impact on the New Zealand extremist environment".

d) Two papers produced by the National Assessments Bureau in 2018 discussed the "persistent threat from Jihadist terrorism".

62 During this period, there was also significant focus on the threat to New Zealand's national security posed by the return of New Zealand citizens who had travelled to Syria or Iraq to engage with terrorist entities in both combat and non-combat roles (called "foreign terrorist fighters").

4.10 Perceptions of the threat of right-wing extremist terrorism

Assessments in the wake of the 22 July 2011 Oslo terrorist's attack

63 In August 2011, one month after the Oslo terrorist's attack, the Combined Threat Assessment Group shared an assessment from an international partner that assessed the potential – in terms of the availability of firearms – of a "Norwegian-style attack" occurring in that country.

64 One month later, in September 2011, the Combined Threat Assessment Group issued a threat assessment titled *Availability of Firearms in New Zealand to Terrorists, Violent Extremists and Acutely Disaffected Persons*. The assessment judged that a terrorist or violent extremist could legally acquire firearms, including military style semi-automatic firearms, for use in an attack. It looked at New Zealand's firearms licence vetting process and considered that it was beyond the scope of, and it would be unrealistic to expect, the vetting regime to reliably identify a terrorist, extremist or acutely disaffected person posing as a legitimate firearms applicant. The Combined Threat Assessment Group considered the assessment was timely in regard to assessing the potential for terrorists or violent extremists planning to threaten New Zealand's hosting of the Rugby World Cup 2011.

65 This assessment was not well received by some Public sector agencies. There were questions about whether the Combined Threat Assessment Group was stepping outside of its mandate in issuing an assessment that identified a vulnerability in the New Zealand system that was not tied to specific warnings or indicators. There was a strong suggestion that the Combined Threat Assessment Group was not the right agency "to be 'auditing' at this level – as distinct from making an input into a risk register which the agency with the main legal and financial/regulatory accountabilities has to maintain".[74]

66 In October 2011, the Department of the Prime Minister and Cabinet wrote to Mike Bush, then Deputy Commissioner of New Zealand Police, seeking New Zealand Police's view on whether further firearms control measures were needed. A second letter is believed to have been sent to New Zealand Police in April 2012. New Zealand Police responded by providing statistics that highlighted that firearms crimes make up a small portion of total crimes and there had been a slight decrease in firearms crimes over the decade. After discussing the Combined Threat Assessment Group assessment with the Deputy Commissioner of New Zealand Police, and reviewing information provided by New Zealand Police, the Department of the Prime Minister and Cabinet concluded that the information did not indicate an immediate problem or reveal an urgent need for a review of firearms controls. As a result, no changes were made to fix the vulnerability that had been identified in the Combined Threat Assessment Group's report. The Department of the Prime Minister and Cabinet did, however, encourage New Zealand Police to inform the Officials' Committee for Domestic and External Security Coordination if the situation changed or New Zealand Police were of the view that firearms control needed to be re-examined.

[74] Simon Murdoch, footnote 68 above at page 9.

National Assessments Bureau assessments

67 In 2013, the National Assessments Bureau produced an assessment titled *Far Right Rising: A Dangerous Myth*, which observed that during the European debt crisis, far right movements across Europe stepped up their anti-immigrant and anti-Muslim rhetoric. However, this assessment did not cover terrorism and/or violent extremism implications. Rather, it focused on the changing political landscape in Europe and what this might mean for New Zealand's interests in trade, investment and immigration to the European Union.

68 The National Assessments Bureau's first comment on the terrorist threat of the extreme right-wing in New Zealand was in September 2018 in its *Global Terrorism Update*. In an annex to the main assessment was a small section on "extreme right terrorism", in which it observed that "between 12 September 2001 and 31 December 2016 in the United States of America, there were more extreme-right incidents than Islamist terrorist incidents resulting in fatalities". It concluded that there had been an emerging threat from extreme right-wing terrorism for some time, but groups were fragmented with limited international coordination. The assessment went on to note that "[e]xtreme-right-wing groups are present in New Zealand and have an online presence, but have not been active".

Combined Threat Assessment Group assessments

69 In 2018 the Combined Threat Assessment Group noted the "limited intelligence coverage of extremist left-wing and right-wing groups internationally". One of the reasons for that limited coverage was explained in an earlier Combined Threat Assessment Group paper from September 2017. It noted that it "rarely sights intelligence regarding right-wing extremist groups and this is likely due to Western jurisdictions defining this more as a law enforcement matter". This was a reference to extreme right-wing attacks not necessarily being considered matters of national security in some countries. Rather, they were seen as matters for law enforcement authorities. So some of New Zealand's international partners did not have a mandate to collect or assess intelligence on the extreme right-wing.

70 In its January 2018 assessment of the New Zealand terrorism threatscape, the Combined Threat Assessment Group noted that:

> *Open source reporting indicates the popularity of far right ideology has risen in the West since the early 2000s. Since 2014, the "new" right-wing movements have been strengthened by opposition to refugee settlements and Islamist extremist attacks in the West, especially in Europe and Scandinavia.*
>
> *[The Combined Threat Assessment Group] has not sighted any reporting to indicate [established New Zealand far right groups have] the intent or capability to promote their ideology by an act of terrorism. As has been evidenced in similar jurisdictions to New Zealand, an extreme right-wing lone actor attack remains a possibility, albeit a remote one.*

71 Leaving aside the assessments to which we have just referred, the Combined Threat Assessment Group reported on the threat of extreme right-wing terrorism only in the context of intelligence products it had received from international partners between 2011 and 15 March 2019. These were generally in connection with events, including international terrorist attacks motivated by extreme right-wing ideology (such as the murder of British Member of Parliament Jo Cox and the Finsbury Park Mosque and Quebec City Mosque terrorist attacks) and the designation of extreme right-wing groups (including National Action in the United Kingdom) as terrorist organisations.

72 We were informed by the New Zealand Security Intelligence Service that the domestic and international partner agency information available to the Combined Threat Assessment Group on extreme right-wing threats before 15 March 2019 was "very limited compared to the amount of information related to Islamist extremism threats".

New Zealand Police assessments

73 New Zealand Police were the first agency in New Zealand's counter-terrorism effort to produce regular intelligence assessments on the extreme right-wing. Since the 1990s, New Zealand Police had been examining and reporting on individuals and groups that were assessed to be white supremacists. New Zealand Police increased their focus on and broadened their awareness of the extreme right-wing around 2009.

74 From 2010 to 2014, New Zealand Police produced intelligence assessments on the criminal activities (including assault, theft and drug offending) of several extreme right-wing groups in New Zealand. The potential for members of these groups to commit acts of terrorism was not assessed. By 2013, New Zealand Police had identified more than 100 individuals of interest to New Zealand Police due to their links to extreme right-wing groups.

75 Although New Zealand Police secondees to the Combined Threat Assessment Group would have had access to these New Zealand Police assessments, they do not appear to have formed the basis of the Combined Threat Assessment Group's assessments. We have not seen evidence that they were brought to the notice of the National Assessments Bureau or the New Zealand Security Intelligence Service. The New Zealand Security Intelligence Service suggested to us that the reason why New Zealand Police assessments were not shared may have been that they were not seen as having a clear connection to national security. New Zealand Police told us that, at the time, they understood that the New Zealand Security Intelligence Service had no interest in or mandate to examine the extreme right-wing and thus they saw no reason to share the assessments.

76 In 2014, a New Zealand Police assessment titled *The Right-wing in New Zealand: Myth vs Reality* was published by the National Assessments Committee. The paper assessed that while the actions of established extreme right-wing groups in New Zealand were confronting to wider society, there was no evidence to suggest they posed a national security threat.

77 Later in 2014, another New Zealand Police assessment titled *Domestic Extremism: Unlikely but not out of the question* was published by the National Assessments Committee. This assessed the risk to New Zealand from forms of extremism other than Islamist extremism. It reiterated that the far right was characterised by "discord and discoordination" and that experienced activists were unlikely to pose a risk to national security in the next three years. It noted that the growth of the internet allowed people to connect and reinforce their ideas and that it was hard to identify individuals of security concern outside the domestic activist environment because many of their characteristics and behaviours were found in the general population. It concluded that an extremist could purchase firearms or the components of an improvised explosive device with minimal risk of discovery and assessed there was 25 to 50 percent chance of an extremist act.

78 In both of these 2014 assessments, New Zealand Police addressed the possibility of firearms being used in a terrorist attack, specifically by the extreme right-wing. The first assessment noted a "propensity for [extreme right-wing] members to acquire and use firearms". New Zealand Police concluded that the relative ease of access to semi-automatic firearms in New Zealand meant that a lone actor terrorist attack remained a possibility. In the second, New Zealand Police assessed "if someone has the intent, the relatively permissive environment for purchasing firearms and/or [improvised explosive device] components will allow them to develop actionable capability with minimal risk of discovery" (see Part 8, chapter 6 for more discussion on what New Zealand Police were doing about the extreme right-wing before 15 March 2019).

79 New Zealand Police had given some thought to the possibility that Muslim communities in New Zealand could be the target of threats. In May 2018, an internal New Zealand Police report, *National Security Situation Update,* noted calls from Dā'ish for attacks during Ramadan and observed:

> *Internationally, Ramadan is also a time of increased risk for the Muslim community, due to either the backlash following terrorist events, the increased profile of the Muslim community during this period, or a combination of the two. In addition to vandalism, verbal altercations, and online harassment, this has also led to violence. During Ramadan in 2017, verbal harassment of Muslims escalated into a stabbing incident where two men were killed in Portland, USA, and a vehicle ramming attack on worshippers exiting the Finsbury Park Mosque in London, UK.*

NZ Context

The national terrorist threat level in New Zealand is currently assessed as LOW – an attack is possible, but is not expected. There is no intelligence as to any specific threat.

However, this intelligence could be incomplete or the situation could change at short notice. Internationally, attacks have taken place with little warning.

The Muslim community in New Zealand has experienced sporadic incidents of vandalism and abuse. While not frequent, incidents do create widespread concern among the community when they do occur, as well as attention from the media.

80 New Zealand Police's last intelligence assessment related to extreme right-wing groups and activities was in 2015 but focused on an annual event and did not address national security issues. It was primarily a New Zealand Police document, but the Combined Threat Assessment Group was on the distribution list. New Zealand Police's strategic intelligence capability declined after 2015, which we were told meant limited focus on counter-terrorism from its intelligence system.

81 As we will discuss shortly, in late 2018 the New Zealand Security Intelligence Service sought the support of New Zealand Police with their project to establish a baseline picture of emerging domestic threats. This included a discussion to understand the interaction between each agency's mandate on non-Islamist extremism (see Part 8, chapter 12). We were told that New Zealand Police took preliminary steps to undertake their own national assessment of the extreme right-wing environment but that effort on this work was still in its initial stages at the time of the 15 March 2019 terrorist attack.

New Zealand Security Intelligence Service assessments before 2018

82 In December 2011, the New Zealand Security Intelligence Service observed the "notable increase in groups across Europe espousing hard-line nationalist and anti-immigration rhetoric" and the resurgence of neo-Nazi groups in the United States of America and Europe. It assessed that the Global Financial Crisis and New Zealand's economic and immigration policies could "stir up extreme right-wing and/or nationalist groups [in New Zealand] to protest against perceived increasing inequalities and lead to the adoption of more violent methods to effect political change". In 2014, the New Zealand Security Intelligence Service assessed non-Islamist extremist domestic terrorism as a threat, "although comparatively minor". The threat of right-wing extremist terrorism was not further addressed until 2018, just ahead of the New Zealand Security Intelligence Service baselining project.

Reports received from the Government Communications Security Bureau

83 Before 15 March 2019, the Government Security Communications Bureau had no specific intelligence about a heightened risk to New Zealand's national security from the extreme right-wing or requests from other Public sector agencies to investigate the matter. The Government Communications Security Bureau has emphasised to us (see Part 8, chapter 7) that:

> *[The Government Communications Security Bureau] is not a lead agency nor an assessment agency for counter-terrorism, [so] it is not [its] role to assess the prevalence of right-wing extremism in New Zealand. [The Government Communications Security Bureau] carries out intelligence collection and analysis activities at the request of the other New Zealand government agencies which have the lead on the counter-terrorism priority.*

84 The Government Communications Security Bureau informed us that in the second quarter of the 2018–2019 financial year, it received 7,526 intelligence reports from international partners about terrorism and violent extremism. None of those reports related to right-wing extremism.

New Zealand Security Intelligence Service baselining project

85 The New Zealand Security Intelligence Service started a project to develop a baseline picture of emerging terrorism threats in May 2018. We describe this baselining project in greater detail in Part 8, chapters 5 and 10.

86 The extreme right-wing was identified as requiring further attention due primarily to global terrorist incidents and trends. The New Zealand Security Intelligence Service sought to identify any similar potential threats in New Zealand. This involved a 12 month project focusing on right-wing extremist activity in New Zealand, which started in May 2018. In July 2018, the New Zealand Security Intelligence Service produced its *Information & Intelligence Requirements Extreme Right-wing (XRW) Activity in New Zealand*. This set out the state of the New Zealand Security Intelligence Service's knowledge and the intelligence gaps and questions to be addressed. We discuss this further in Part 8, chapter 5.

New Zealand Security Intelligence Service assessments in 2018

87 From December 2017, the Strategic Intelligence Analysis team within the New Zealand Security Intelligence Service started producing quarterly *New Zealand Terrorism Updates*. Three of these reports were produced before 15 March 2019. They are relatively short and focus almost exclusively on the threat of Islamist extremist terrorism in New Zealand and overseas. Two of these reports produced in the second half of 2018, and one produced in the first quarter of 2019, referred to the threat of extreme right-wing terrorism. The *New Zealand Terrorism Update* dated 5 September 2018 noted that "[the New Zealand

Security Intelligence Service] is not aware of any credible indications of terrorist threats from supporters of non-Islamist terrorist groups or other extreme ideologies". The next *New Zealand Terrorism Update* in this series was dated 4 December 2018 and was more cautious:

> *Non-Islamist terrorist threats from extreme political, religious and issues-motivated groups are plausible in New Zealand, especially given heightened political partisanship internationally and the spread of disinformation online. Various radical groups are present in New Zealand, some of which have extreme elements that could plausibly turn violent; however, terrorist acts by them are currently not expected.*
>
> ...
>
> *The spread of highly partisan political content online, especially over social media, has almost certainly contributed to acts of non-Islamist extremist violence in Western countries. Several attempted and realised attacks in the United States in 2018 were linked to extreme right-wing, conspiratorial, or racist agitation in social and other media, judging from press reporting.*

88 The final *New Zealand Terrorism Update* published before 15 March 2019, which was dated 5 March 2019, stated that:

> *[The New Zealand Security Intelligence Service] and [Combined Threat Assessment Group] analysts note that extremism exists in the fringes of non-Islamist New Zealand political, religious, and issues-motivated groups and could plausibly result in violence. However, [the New Zealand Security Intelligence Service] is not aware of any credible threats from such groups.*

89 These assessments reflect the New Zealand Security Intelligence Service's developing but still limited understanding of the threat of right-wing extremism in New Zealand as at 15 March 2019.

A training exercise

90 A counter-terrorism tabletop training Response exercise was carried out by the New Zealand Security Intelligence Service and New Zealand Police in October 2018. Two hypothetical counter-terrorism scenarios were presented and discussed. One of the scenarios tested was an extreme right-wing attack outside a masjid in Christchurch. This scenario assumed a Finsbury Park Mosque-style terrorist attack, with a vehicle hitting pedestrians leaving what was described in the scenario as the "[an-Nur] Mosque adjacent to Hagley Park in Christchurch". The hypothetical attacker in the scenario shouted anti-immigration and Islamophobic slurs as he fled the scene.

91 The locations of the assumed attack and the first phase of the 15 March 2019 terrorist attack are the same. We must emphasise that this is a coincidence, albeit a striking one. The design of the exercise was not informed by intelligence suggesting that Masjid an-Nur was at risk as there was no such intelligence.

92 The objectives for the exercise were focused on increasing the understanding of agencies' processes and procedures during the Response to a terrorism scenario. Importantly, for present purposes, what the exercise demonstrated was an awareness of the possibility of the threat from the extreme right-wing – and that such an attack could potentially occur in New Zealand.

A system view – looking back

93 Andrew Kibblewhite, former Chief Executive of the Department of the Prime Minister and Cabinet, told us "we weren't unaware of a white supremacist threat but it wasn't where our focus was". He used the metaphor of an iceberg. The system knew about the threat of the extreme right-wing but saw it as a "small iceberg", so there would be the "occasional paragraph" about the extreme right-wing in intelligence products. But there was no deeper investigation beneath the surface. Andrew Kibblewhite said that it had become apparent after the 15 March 2019 terrorist attack, in light of the leads received on possible extreme right-wing activities, that the "iceberg was bigger than we realised and it was our job, as a system, to know the size of that iceberg".

Community concerns

94 In the two or three years before 15 March 2019, members of Muslim communities in New Zealand raised many issues with Public sector agencies including Islamophobia, discrimination and harassment. Minutes tended not to be taken at the meetings at which these concerns were raised and, if notes were taken, they were not shared with community members. This, along with the effect of the passage of time on the memories of the officials involved in the meeting, means that it is hard to be sure as to the extent to which the concerns raised at particular meetings extended to the risk of right-wing terrorism.

95 Despite these doubts and difficulties, we are confident that concerns relating to the rise of the alt-right, right-wing extremist terrorist attacks overseas and the safety of Muslim communities were shared with Public sector agencies on some occasions. For example:

a) The speech notes of a Muslim speaker at a meeting on 23 March 2017, at which a senior New Zealand Police representative was present, raised concerns about the "alt-right (neo-Nazis)" and "fear of an attack". The notes included a question to Public sector agencies about whether they had a strategy in place to deal with these issues.

b) An email to a government official in August 2017 from Muslim individuals records how they had raised concerns with a minister about events overseas, an increase in Islamophobia experienced by Muslim women in New Zealand and the rise of the alt-right in New Zealand.

c) Three separate meetings were held in 2018 between the New Zealand Security Intelligence Service and different Muslim individuals. The New Zealand Security Intelligence Service's notes from these meetings show concerns were raised about Islamophobia and discrimination experienced by Muslim individuals and communities. We were told by the individuals that concerns were also raised by about the alt-right and right-wing extremism. Such concerns were recorded in some but not all of the New Zealand Security Intelligence Service's notes from the meetings. For instance, an email exchange between Muslim individuals following the November 2018 meeting recorded that they had raised concerns about hate groups and an offensive pamphlet being placed in the letterbox of a Muslim whānau. The New Zealand Security Intelligence Service's record of the same meeting records that concerns were raised about anti-Muslim activity and right-wing extremism and includes a reference to the pamphlet.

d) An email sent to New Zealand Police shortly before the 15 March 2019 terrorist attack from a member of the Muslim community about their previous report of an abusive phone call, their wider concerns about the rise of Islamophobia in New Zealand and the need for New Zealand Police to develop a strategy to counter this before it escalated.

4.11 Terrorism threat level assessments

96 From 2010 to 2018, the New Zealand terrorism threat level set by the Combined Threat Assessment Group was mostly at "low" (terrorist attack is assessed as possible but is not expected) or "very low" (a terrorist attack is assessed as very unlikely). It set these levels on the basis that "New Zealand has not experienced a completed Islamist extremist terrorist attack and [the Combined Threat Assessment Group] is not aware of any current and/or advanced plan to conduct one". It emphasised, however, that the low threat level meant that the threat of terrorism in New Zealand was real, even at "low".

4.12 Concluding comments

97 The assessments outlined above generally judged that the terrorism threat to New Zealanders was greater offshore and the primary threat was Islamist extremist terrorism. There were few strategic intelligence assessments about terrorism threats in New Zealand and hardly any on emerging threats such as right-wing extremism.

98 In part this was because the two key assessment agencies were not well-situated to provide assessments of emerging terrorism threats in New Zealand. The National Assessments Bureau saw terrorism as primarily the responsibility of the Combined Threat Assessment Group. Its focus was largely international and customer directed. The Combined Threat Assessment Group's assessments were short-term and tactical in nature rather than long-term and strategic. Both agencies had limited resources and neither had a dedicated horizon scanning capability. The lack of a coordinated national assessments programme meant that the gaps in strategic assessment were less likely to be identified and addressed.

99 We see the way these agencies viewed their respective roles, and the focus of their efforts, as a function of the way the counter-terrorism effort operated as a whole and thus not within the control of a single agency. We address this further in our evaluation in Part 8, chapter 15.

Chapter 5: The New Zealand Security Intelligence Service

5.1 Overview

1 The New Zealand Security Intelligence Service is New Zealand's human intelligence agency.

2 In this chapter we:

a) describe what human intelligence brings to the counter-terrorism effort;

b) discuss the roles of the New Zealand Security Intelligence Service;

c) explain its leads process;

d) discuss the rebuild of the New Zealand Security Intelligence Service; and

e) assess the evolution of their counter-terrorism efforts.

5.2 What does human intelligence bring to the counter-terrorism effort?

3 Human intelligence can enrich intelligence obtained from other sources, by providing insights into the motivation and intention of individual actors, which may not be apparent from signals intelligence alone (see Part 8, chapter 7). Intentions and motivations will vary from one person to another and change over time. Understanding people and all their complexities is crucial to the collection of human intelligence.

4 A human intelligence agency offers the national security system and the counter-terrorism effort expertise in making sense of information from multiple sources with a view to developing a deeper understanding of the security environment.

5 Ideally a human intelligence agency's all source analysis will generate a strong understanding of the threatscape. It is used to identify emerging threats, supports disruption and enforcement carried out by law enforcement agencies and informs decision-making elsewhere in government (for example, immigration decision-making).

5.3 Roles of the New Zealand Security Intelligence Service

6 The New Zealand Security Intelligence Service is a specialised human intelligence agency.[75] Its objectives include the protection of New Zealand's national security,[76] including protection from terrorism and violent extremism.[77] It operates by obtaining human intelligence from people with knowledge of, or access to, information. It also obtains information through a range of other collection methods. These include physical surveillance, open-source research and activities conducted under intelligence warrants, such as the use of tracking devices, telecommunications interception and listening devices.

[75] Intelligence and Security Act 2017, section 7.

[76] Intelligence and Security Act 2017, section 9.

[77] Intelligence and Security Act 2017, section 58.

7 The New Zealand Security Intelligence Service has a broader remit than its comparable international partner agencies. For example, in Australia there are separate agencies for managing domestic security threats (Australian Security Intelligence Organisation), foreign intelligence (Australian Secret Intelligence Service) and vetting (Australian Government Security Vetting Agency). All of these activities are undertaken by the New Zealand Security Intelligence Service. This broad range of functions impacts on its decision-making, including its prioritisation and resourcing decisions.

5.4 Leads process

8 A security intelligence investigation always starts with information, which is assessed for its relevance to national security by an investigator.

What is a lead?

9 Lead information can take many forms, such as a name, a phone number or an activity of security concern. A lead is formally raised if the information and intelligence is both relevant to New Zealand and shows a possible threat to national security (such as terrorism or foreign interference).

10 Information or intelligence that does not meet these two criteria is not raised as a lead or investigated further by the New Zealand Security Intelligence Service. It may, however, be referred to another domestic agency (such as New Zealand Police), particularly where the information suggests criminal activity is taking place.

Where does lead information come from?

11 Lead information comes from a wide range of sources, including:

a) other New Zealand Security Intelligence Service investigations or business units;

b) international partners;

c) other Public sector agencies (such as New Zealand Police or Immigration New Zealand); and

d) the New Zealand public.

12 Lead information received (or generated) by the New Zealand Security Intelligence Service that relates to terrorism is dealt with and managed by the New Zealand Security Intelligence Service's Counter-Terrorism Unit. During 2017–2018, the Counter-Terrorism Unit received about 150 terrorism-related leads. Most of these leads related to individuals allegedly viewing violent terrorist propaganda, supporting or seeking to support the activities of Dā'ish or attempting to travel from New Zealand to join extremist groups or terrorist entities.

Progressing lead information to a lead and then to an investigation

13 Lead information is initially dealt with by a leads coordinator, who is responsible for making a preliminary assessment. The leads coordinator determines whether the information is relevant to New Zealand and shows a possible threat to national security.

14 The leads coordinator is responsible for allocating the lead information to an investigating officer. The leads coordinator is not formally responsible for progressing the lead information once it has been allocated to an investigator. The investigator is responsible for evaluating the lead information and recommending whether a formal lead should be opened based on whether it presents a current matter of national security concern. This will be approved or declined by a counter-terrorism manager. A counter-terrorism manager will maintain oversight of the lead process and provide guidance where necessary.

15 Investigating officers must capture all leads in what is known as the Leads Workflow Tool. This tool provides for the active management of leads, ensuring that decisions are documented and that actions taken against each lead are accurately recorded and tracked.

16 The Leads Workflow Tool requires investigating officers to assign a priority to the lead. The New Zealand Security Intelligence Service prioritises leads according to whether they are high, medium or low priority:

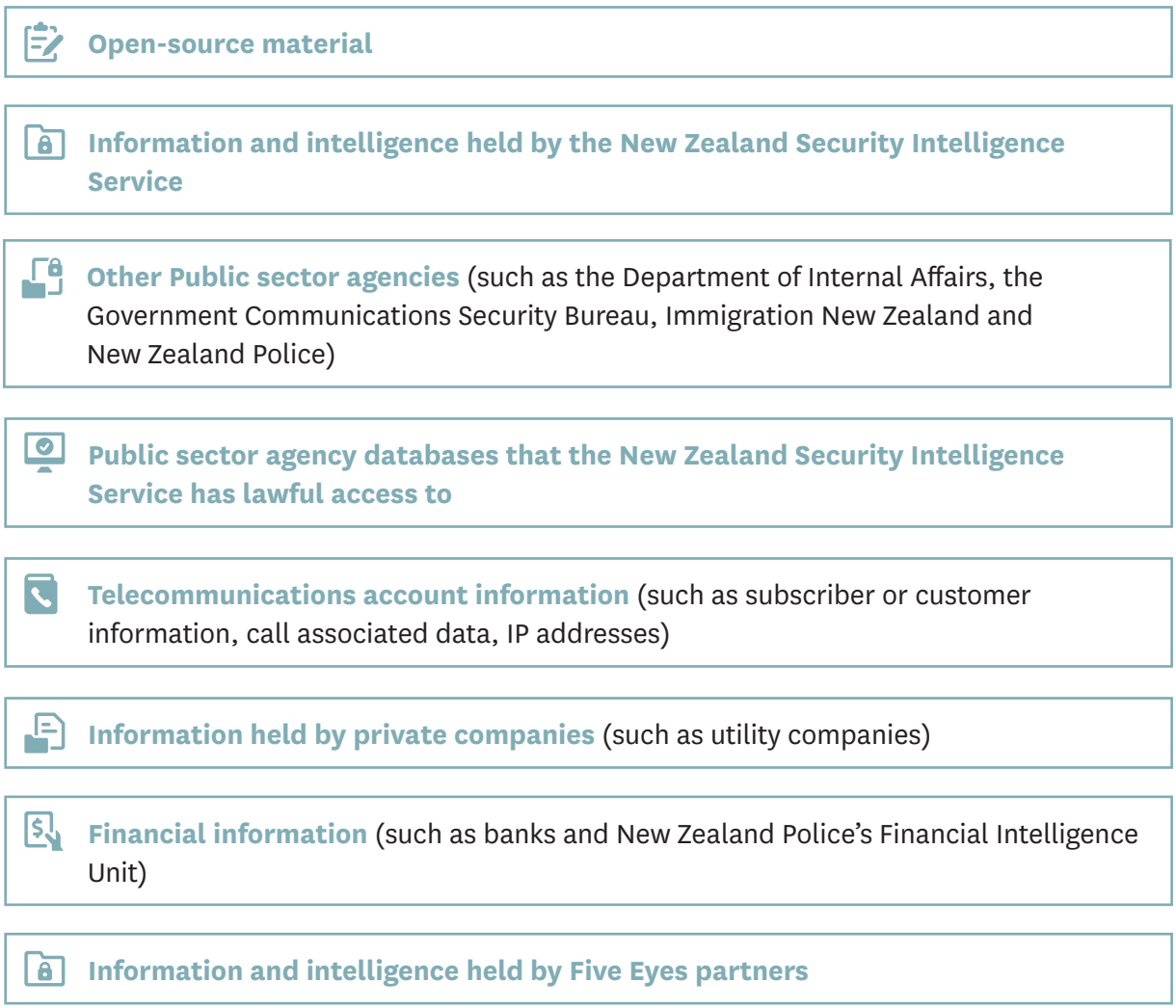
a) High/critical – time sensitive and requires immediate action (for example, involves a threat to life).

b) Medium – time sensitive, has an accountable deadline and must be actioned in a timely manner.

c) Low/routine – not time sensitive and must be worked on when the investigator has capacity or cannot be looked at due to limited resources.

17 Once a priority is assigned, the lead is actioned in the Leads Workflow Tool by the assigned investigator. The investigating officer will identify the intelligence gaps that exist in relation to the lead and seek to address those by carrying out various inquiries. These involve checking one or more of the sources outlined in the figure below.

Figure 44: Information and intelligence that may be checked during a lead assessment



18 Through these enquires the investigating officer seeks to understand more about the lead information, such as the nature of the links to national security, the credibility of the information and the urgency it presents. Depending on what information comes to light, the lead may be progressed to an investigation.

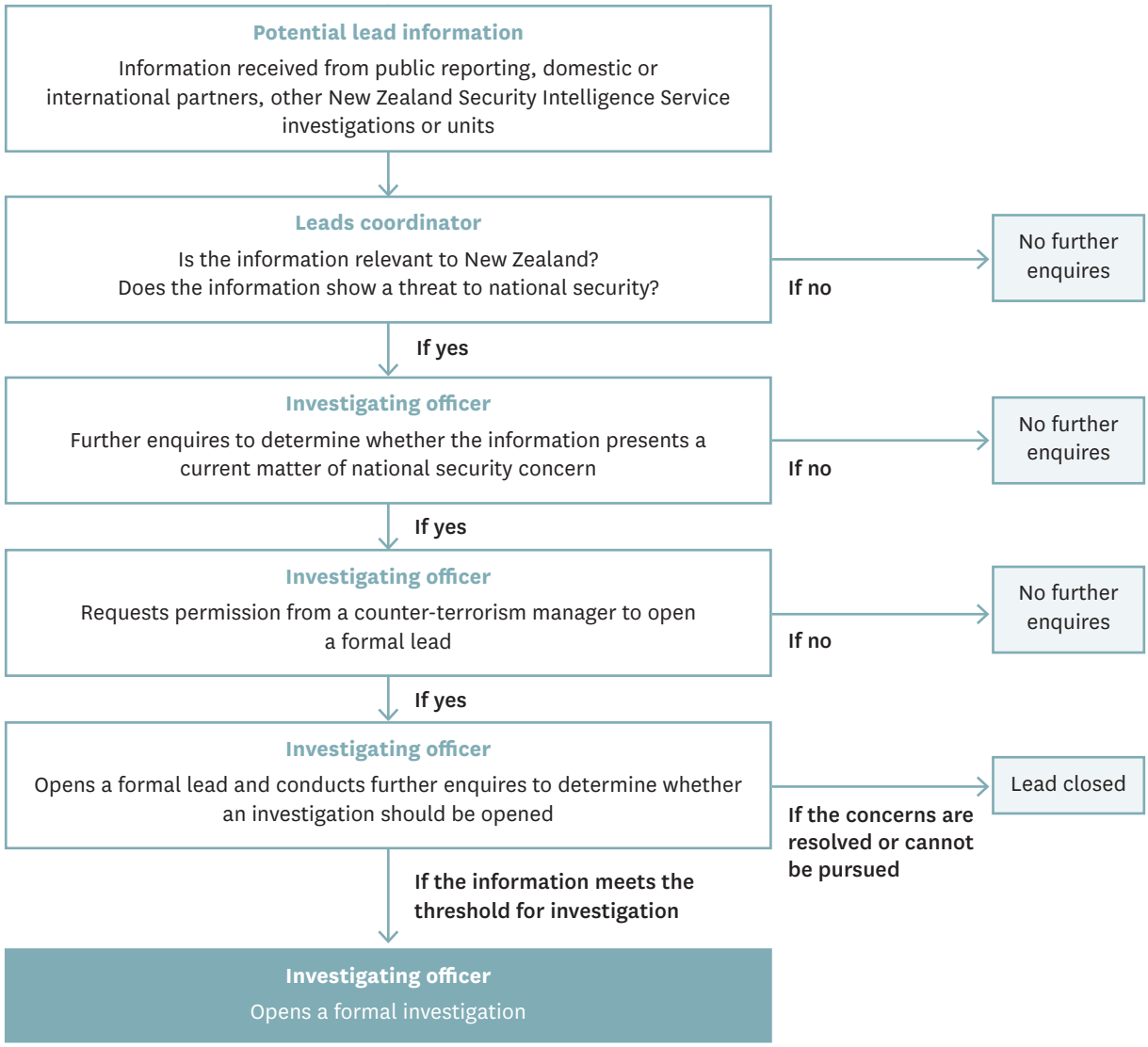
19 Although the New Zealand Security Intelligence Service has guidelines for the commencement of an investigation, there are no hard and fast rules for deciding if a lead should move to a full investigation. Instead, it requires the judgement of the investigator (and their manager) to the particular facts relating to the lead. Depending on the nature of the lead, some factors (such as the imminence of harm) may outweigh other factors (such as the reliability of the lead). Given each lead is unique, a definitive threshold is not applicable.

20 An investigation may extend to covert collection, which may require an intelligence warrant to undertake activities that would otherwise be unlawful.

21 The principles of proportionality and necessity will be relevant in determining what investigative activity to undertake (see Part 8, chapter 14). The principle of proportionality requires investigators to consider both the intrusiveness of the proposed action and the priority of the lead. Counter-terrorism managers are responsible for overseeing whether the proposed actions are necessary and proportionate.

22 If the investigator's enquiries resolve national security concerns or cannot usefully be pursued, the lead is closed with an explanation of the reasons recorded in the Leads Workflow Tool. If the lead has been referred to another Public sector agency, such as New Zealand Police, this will be recorded.

Figure 45: Progressing lead information to a lead and then to an investigation



Post-15 March 2019 developments

23 In August and September 2019, the New Zealand Security Intelligence Service conducted a review of its leads processes. It decided to adopt the Australian Security Intelligence Organisation's leads triage and assessment framework. This provides a standardised set of criteria for the evaluation of information, including security and radicalisation indicators, and outlines the process for the assessment and management of leads (see Part 8, chapter 12).

24 The framework sets out three stages for assessing a lead:

a) Evaluation and prioritisation (Stage 1) – incoming lead information is triaged and prioritised according to security indicators and urgency. Information gaps are identified and inquiries are made to fill the gaps.

b) Development and assessment (Stage 2) – based on the information gathered, an assessment is made and inferences are drawn to determine the requirements for further enquiries.

c) Action (Stage 3) – the lead is either elevated to become a formal investigation or closed.

25 At Stage 1, the New Zealand Security Intelligence Service applies the Reasoned Assessment Model to assist investigators in evaluating and prioritising incoming lead information. Under this model, incoming lead information is evaluated and prioritised by a preliminary assessment of:

a) the threat posed by the lead information – this is measured by the intent (motivation, desire and confidence to carry out an attack), capability (knowledge and resources for conducting an attack, such as access to, and ability to use, weapons) and imminence of the threat;

b) the relevance to national security;

c) the plausibility, reliability and credibility of the threat and corroboration of the lead information (this includes assessing the source of the lead information, including the chain of acquisition and motivation of the source); and

d) the connection between the lead information and New Zealand.

26 To assist staff in prioritising leads, the New Zealand Security Intelligence Service has produced a table that sets out various security indicators and the priority associated with them. For example, "Skills/Knowledge – Research into basic weapons, firearms and ammunition" is identified as a critical indicator of security relevance for assessing whether a person has the capability to carry out a terrorist act. The number of security indicators (and the priority associated with them) that a lead displays is relevant to its overall prioritisation. The New Zealand Security Intelligence Service guidance sets out that where a lead displays two or more security indicators, it can be prioritised as medium.

5.5 The rebuild of the New Zealand Security Intelligence Service

27 The New Zealand Security Intelligence Service's capability and capacity were severely degraded by 2013–2014.[78] As at 30 June 2014, it had 225 staff. Around 35 to 50 percent of these staff were allocated to security vetting and just 4.5 full-time equivalent staff (including the manager) worked on terrorism investigations. This was less than one staff member working on terrorism investigations per million people in New Zealand. The staff working on terrorism investigations were supported by intelligence collection and analytical staff.

28 By 2016 there had been an appreciable increase in the Counter-Terrorism Unit's investigative staffing. But a large proportion of this was associated with a dedicated one-off investment by the government for a specific and narrow purpose.

Strategic Capability and Resourcing Review programme

29 From July 2016, the New Zealand Security Intelligence Service received increased funding associated with implementation of the Strategic Capability and Resourcing Review (see Part 8, chapter 2). This allowed significant growth over four years in its capacity and capability. The increased funding was approved with the condition that the New Zealand Intelligence Community would not seek additional funding until at least February 2019, unless there was a major security or global shock.

30 The anticipated capability increase was described in this way in a February 2016 Strategic Capability and Resourcing Review Cabinet paper:

> *The capability increases from a current state where partial monitoring of watch-list targets is possible and there is minimal coverage outside Auckland, to a future where there is a New Zealand-wide baseline threat picture … .*

31 Since 2016, the New Zealand Security Intelligence Service has undergone rapid organisational growth and organisational and business renewal. It has engaged in the development and implementation of a fundamental redesign of its governing legislation (the Intelligence and Security Act 2017) and responded to enhanced and more rigorous oversight.

[78] *Performance Improvement Framework*, footnote 42 above.

32 Growing capacity and capability in intelligence and security agencies is not straightforward. This was recognised by United Kingdom agencies in their response to questioning by the Parliamentary Intelligence and Security Committee inquiry into the 7 July 2005 London terrorist attacks. When asked whether agency heads ought to have sought a greater increase in funding in the previous year, the Chief of the British Secret Intelligence Service said:

> *If you try to bring in more than a certain number of new people every year, you can literally bust the system … you can only tolerate a certain number of inexperienced people dealing with sensitive subjects.*[79]

33 During the initial phases of the New Zealand Security Intelligence Service rebuilding exercise the primary focus was on enabling functions (for example, security vetting and then compliance and organisational processes and systems) rather than frontline staff. By 2018, a significant number of new investigators and some new collection staff had been brought on board and, as of late 2019, numbers had recovered considerably from where they were several years ago. A consequence of this sequencing is that the numbers of the current investigators and a certain category of collection staff is proportionately low and many have limited experience. The 2019 Arotake Review confirmed this view, noting that the majority of the investigators had less than one year's experience at the time of the 15 March 2019 terrorist attack.[80]

34 We were told that getting the balance between investigative and collection capabilities right is difficult, as a certain category of collection staff are particularly difficult to train and develop. While there is no set timeframe, as different people develop at different rates, collection staff were generally regarded as apprentices for at least their first year.

35 Capacity and capability gaps can have flow-on effects for other parts of the organisation. Investigations staff need experience to know how to effectively task collection staff. We heard that the limited experience of some investigations staff led to extremely valuable collection staff being deployed against lower priority intelligence requirements instead of developing more strategic access. The New Zealand Security Intelligence Service has sought to address this through the establishment of a Collection Hub, which facilitates interaction between investigators and collections staff. The Collection Hub ensures that intelligence requirements are refined and prioritised according to urgency and available collections resources.

---

[79] United Kingdom Intelligence and Security Committee *Report into the London Terrorist Attacks on 7 July 2005* (presented to Parliament May 2006) at page 38.

[80] New Zealand Security Intelligence Service, footnote 57 above.

36 We were also told there was, at particular points over the past two to three years, an imbalance between the number of investigators on the one hand and collection resources available to respond to the investigators' intelligence requirements on the other. While the New Zealand Security Intelligence Service moved to better manage intelligence collection needs through the formation of the Collection Hub, this development took time to start working properly. Consequently, the imbalance between investigatory and collection resources led to considerable pressure on collection resources, particularly at the point that relatively large numbers of new investigators were brought into the investigation teams.

37 The New Zealand Intelligence Community's report back on the Strategic Capability and Resourcing Review (which occurred after 15 March 2019) noted that recruitment and turnover challenges were continuing to impact the numbers of collection staff able to be deployed. It takes time for new staff recruits to be security vetted and cleared before they can be brought into the organisation and more time to train them to appropriate levels of skill and allow them to develop necessary levels of experience.[81]

Developing a Strategic Intelligence Analysis function

38 In 2015, the New Zealand Security Intelligence Service initiated a review of the security intelligence model used within the New Zealand Intelligence Community.[82] The review primarily focused on the New Zealand Security Intelligence Service. It identified the need for a stronger strategic function to support its investigative efforts by proactively identifying and analysing future security threats. The Strategic Intelligence Analysis function was established in response, despite this not being funded under the Strategic Capability and Resourcing Review. At the time, the New Zealand Security Intelligence Service was the only Five Eyes intelligence agency without a dedicated strategic intelligence analysis capability.

39 The primary purpose of the Strategic Intelligence Analysis team is to provide the New Zealand Security Intelligence Service with strategic assessment of security intelligence issues (especially espionage and terrorism). The New Zealand Security Intelligence Service described its strategic intelligence function in the following terms:

[81] The significant lead in time required to bring a new recruit up to full performance was recognised by the National Commission on Terrorist Attacks upon the United States in *The 9/11 Commission Report*. The Commission noted that it "takes five to seven years of training, language study, and experience to bring a recruit up to full performance". See *The 9/11 Commission Report: Final Report of the National Commission on Terrorist attacks upon the United States* (2004) at page 90.

[82] New Zealand Security Intelligence Service *Review of the New Zealand Intelligence Community's Security Intelligence Operating Model (Project Aguero)* (2015).

... to provide [the New Zealand Security Intelligence Service] with practical understanding of security intelligence issues as they are occurring or emerging within New Zealand, in order to inform [the New Zealand Security Intelligence Service's] decision-making. This capability enables [the New Zealand Security Intelligence Service] to look more broadly than just known threats and current investigative areas, by understanding the evolution of threats, and identifying emerging or future threat areas. This understanding is then used to guide [the New Zealand Security Intelligence Service's] investigative and operational work, as well as resource allocation. For example, strategic analysis can be used to point part of our investigative effort towards new, emerging threats in addition to established areas of investigation.

40 A Capability Directorate was established in mid-2017,[83] in part to build on the work undertaken in response to the 2014 *Performance Improvement Framework* review of the New Zealand Intelligence Community. Its role includes horizon scanning to understand the New Zealand Security Intelligence Service's future capability needs.

41 Most of the Strategic Intelligence Analysis team's work is tasked by investigative teams in the New Zealand Security Intelligence Service. It is occasionally tasked by other Public sector agencies. A few of its assessments are provided to the wider New Zealand Intelligence Community and other stakeholders. For example, its quarterly *New Zealand Terrorism Updates* were distributed to agencies represented on the Security and Intelligence Board, but it is unclear to what extent, if any, they guided the counter-terrorism efforts of those agencies.

42 In February 2019, an internal memorandum within the New Zealand Security Intelligence Service noted "enduring misconceptions of [the Strategic Intelligence Analysis team's] role and purpose". And the 2019 Arotake Review considered that the Strategic Intelligence Analysis team remained "a fledgling capability, whose role in guiding [the New Zealand Security Intelligence Service's] intelligence functions does not yet appear to be fully embedded".[84]

43 With its focus on guiding the operational activity of the New Zealand Security Intelligence Service, the Strategic Intelligence Analysis team performed a different function to the Combined Threat Assessment Group (see Part 8, chapter 4). The Combined Threat Assessment Group's assessments are intended to inform the approach to counter-terrorism at a whole-of-system level.

[83] New Zealand Security Intelligence Service *Performance Improvement Framework: Follow-up Self Review of the New Zealand Security Intelligence Service Te Pa Whakamarumaru* (March 2018) at page 8.

[84] New Zealand Security Intelligence Service, footnote 57 above at page 50.

Staffing and turnover

44 The New Zealand Security Intelligence Service's annual staff turnover target is eight percent. Annual staff turnover was 12.1 percent in 2018–2019, up from 10.3 percent in 2017–2018. Rebecca Kitteridge, Director-General of Security, told us that she would like staff turnover to be lower than what it currently is. Despite the New Zealand Intelligence Community putting in place a *Diversity and Inclusion Strategy,* retaining ethnically diverse staff has been a particular problem for the New Zealand Security Intelligence Service. Ethnically diverse staff represented 21.1 percent of turnover for 2018–2019. While the New Zealand Security Intelligence Service pointed out that its turnover rate is broadly consistent with the Public service as a whole, high turnover is problematic for an intelligence and security agency.

45 Capacity issues continue to be felt deeply in some areas. The 2019 Arotake Review singled out staffing levels in the New Zealand Security Intelligence Service's Christchurch office as a problem and requiring consideration.[85]

5.6 How has the New Zealand Security Intelligence Service pursued its counter-terrorism efforts?

Operational priorities

46 The New Zealand Security Intelligence Service's *10-Year Operational Strategy*, released in June 2016, has been a key mechanism for it to apply the National Security and Intelligence Priorities (see Part 8, chapter 3). It sets out nine long-term strategic goals. The top three goals inform its prioritisation and resourcing decisions:[86]

Goal 1: mitigation of espionage and hostile foreign intelligence threats;

Goal 2: mitigation of serious domestic terrorism threats; and

Goal 3: establishment of an effective baseline picture of emerging terrorism threats.

47 Accordingly, counter-terrorism efforts, while high on the list of goals, sat behind efforts to counter espionage and hostile foreign intelligence. In practical terms, this meant that before 15 March 2019 approximately half of the New Zealand Security Intelligence Service's investigative resources were dedicated to espionage and hostile foreign intelligence with slightly less being allocated to counter-terrorism.[87] The higher priority placed on espionage and hostile foreign interference meant that more experienced investigators tended to be concentrated on those threats.[88]

[85] New Zealand Security Intelligence Service, footnote 57 above at page 61.

[86] New Zealand Security Intelligence Service, footnote 55 above.

[87] New Zealand Security Intelligence Service, footnote 57 above at page 46. This contrasts with other comparable organisations – for example, 81 percent of MI5's resources are used to support counter-terrorism work. See Security Intelligence Service, *International Terrorism: the International Terrorism Threat to the UK* (Undated) https://www.mi5.gov.uk/international-terrorism.

[88] New Zealand Security Intelligence Service, footnote 57 above at page 57.

48 New Zealand Security Intelligence Service staff told us about the complexity of managing competing priorities. This is particularly marked in relation to counter-espionage and counter-terrorism operations. The former tend to move at a slower pace than a counter-terrorism operation and often require a longer period of operational activity in order to bring results.

Evolving focus of effort

49 Up until 2018, the resources available to the New Zealand Security Intelligence Service's counter-terrorism effort were devoted to what was seen as the presenting threat (as identified by lead information, intelligence collection, strategic assessments and international partner reporting) of Islamist extremist terrorism. These resources were almost fully engaged on the investigation of New Zealand supporters of Dā'ish seeking to participate in hostilities abroad to mount, or encourage or support terrorist attacks or undertake activities in support of terrorism in New Zealand.[89]

50 Before mid-2018 the New Zealand Security Intelligence Service was largely focused on monitoring known individuals where the nature of the threat was understood.[90] Rebecca Kitteridge, Director-General of Security, told us that this was unsatisfactory, as it tied up resources that should be actively seeking out unknown threats.

51 The 2019 Arotake Review noted that the New Zealand Security Intelligence Service had long employed a "classical model" for its investigations, which is lead-based. This model is well suited to assessing known threats using established intelligence collection techniques but is less well suited to the development of a detailed picture of emerging threats in the security environment (see Part 8, chapter 10).[91] The 2019 Arotake Review found that the classical model had served the New Zealand Security Intelligence Service well in relation to Islamist extremist threats. These threats largely (but not exclusively) dominated the New Zealand terrorism threatscape until early 2018.

52 In 2016 the New Zealand Security Intelligence Service's *10-Year Operational Strategy* identified establishing "an effective baseline picture of emerging terrorist threats" as a third goal. But this was deferred until there was sufficient capacity to carry out this work, which did not occur until May 2018. At that time, the Counter-Terrorism Unit instituted a new work programme, which required investigators to allocate 20 percent of their time to baselining and target discovery (see Part 8, chapter 10).

[89] New Zealand Security Intelligence Service, footnote 57 above at page 46.

[90] New Zealand Security Intelligence Service, footnote 57 above at page 51.

[91] New Zealand Security Intelligence Service, footnote 57 above at page 10.

53 The baselining project looked at emerging threats motivated by a range of ideologies. This included a 12 month project focusing on right-wing extremist activity in New Zealand. In July 2018, the right-wing extremism project produced a report detailing information and intelligence requirements for collection units to pursue. The report also described the "Current Intelligence Picture", which indicates that the New Zealand Security Intelligence Service had a limited understanding of the right-wing extremism environment in New Zealand at that time:

> *At present, little is known about the extreme right-wing environment in New Zealand.*
>
> ...
>
> *The New Zealand Security Intelligence Service is currently unsighted to any individuals or groups who espouse an extreme right-wing ideology and promote the use of violence to achieve their objectives.*
>
> ...
>
> *It is possible that a group or individual in New Zealand could associate with [extreme right-wing] groups or individuals offshore.*

54 In response to the intelligence and information requirements, the New Zealand Security Intelligence Service's online operations team began to look at right-wing forums.[92] Additionally, the New Zealand Security Intelligence Service was engaging with a key partner, which had a well-established and active target discovery work programme, in order to further develop its capability in this area.[93]

55 The New Zealand Security Intelligence Service's baselining project on right-wing extremism in New Zealand was not complete as at 15 March 2019. This meant it had a developing but still limited understanding of the threat of right-wing extremism as at 15 March 2019.

56 After 15 March 2019, the Counter-Terrorism Unit within the New Zealand Security Intelligence Service established a dedicated target discovery team. This team is in a "developmental stage" and has been scoping and re-scoping a number of discovery projects and engaging with other agencies who may be able to assist efforts. The Counter-Terrorism Unit's *Discovery Strategy* was revised in August 2019. Since then, the New Zealand Security Intelligence Service's organisational strategy has identified discovery as its first priority.

[92] New Zealand Security Intelligence Service, footnote 57 above at page 96.

[93] New Zealand Security Intelligence Service, footnote 57 above at page 91.

System awareness of unmitigated risk of right-wing terrorism

57 The deferral of the baselining of non-Islamist terrorism threats until the New Zealand Security Intelligence Service had sufficient additional capacity – that is until May 2018 – was consistent with the 2016 Strategic Capability and Resourcing Review Cabinet paper and the 2016 *10-Year Operational Strategy*. It was a considered decision by the New Zealand Security Intelligence Service.

58 The corollary of the recognition that there were threats that warranted baselining and the deferral of the baselining project was that there was a risk that was not being addressed. The existence of this risk was not explicitly highlighted with the Security and Intelligence Board and the Counter-Terrorism Coordination Committee. We will return to discuss this point in more detail in Part 8, chapter 15.

5.7 Concluding comments

59 In the years preceding 15 March 2019, the New Zealand Security Intelligence Service was rebuilding, from an extremely low base, its capacity to identify and respond to terrorism threats. Growing capacity and capability in an intelligence and security agency takes time and comes with particular challenges. So the rebuilding exercise was complex. It has, however, been implemented in a considered way and has resulted in an organisation that is far more capable than it was in 2016.

60 As the 2019 Arotake Review identified, the New Zealand Security Intelligence Service's lead-based investigation model was not well suited to the development of a detailed picture of emerging threats. Such resources as were available to the counter-terrorism effort were, up until 2018, largely devoted to the presenting threat of Islamist extremist terrorism. This focus of effort was also contributed to by the very limited assessments from the National Assessments Bureau and the Combined Threat Assessment Group about threats of terrorism from other sources (see Part 8, chapter 4).

61 The deferral of the baselining project meant that, for the period between mid-2016 when the Strategic Capability and Resourcing Review money became available and mid-2018 when baselining began, the national security system was carrying a risk – the threat of non-Islamist extremism – the nature of which was not understood in any detail.

Chapter 6: New Zealand Police

6.1 Overview

1 New Zealand Police are responsible for maintaining public safety and domestic law enforcement and have a core role in the counter-terrorism effort.

2 In this chapter we:

a) explain the role of New Zealand Police in the counter-terrorism effort;

b) describe reviews of counter-terrorism policing and international practice;

c) assess New Zealand Police's counter-terrorism activities;

d) explain what New Zealand Police were doing about right-wing extremism;

e) discuss what awareness the counter-terrorism system had of New Zealand Police's capacity and capability gaps;

f) describe the experiences of Muslim communities with New Zealand Police; and

g) set out developments since 15 March 2019.

6.2 The role of New Zealand Police in the counter-terrorism effort

3 As explained in *Part 2: Context*, New Zealand Police are one of two counter-terrorism agencies. New Zealand Police seek to prevent crime and improve public safety, detect and bring offenders to account and maintain law and order. Their work also includes searching for missing persons, dealing with sudden deaths and identifying lost property. They have a visible presence in communities. This provides New Zealand Police with the ability to collect and analyse information about risks in and against communities. This is critical to the prevention of crime, including terrorist activity.[94]

4 New Zealand Police are active in Reduction, Readiness, Response and Recovery activities (see Part 2, chapter 4) within the counter-terrorism effort. For example, where an individual poses a risk, New Zealand Police may take direct action to prevent or disrupt an attack. This can occur through arrest and prosecution, issuing warnings or working with individuals to connect them with social support needed to divert them from violent extremism. Where the risk is imminent, New Zealand Police lead Response activities.

[94] R Lambert and T Parsons "Community-Based Counter-Terrorism Policing: Recommendations for Practitioners" (2017) 40 *Studies in Conflict and Terrorism*.

6.3 Reviews and international practice

5 Our review of the literature and international policing practice confirms that there is no single internationally-accepted standard for counter-terrorism policing. There are, however, a range of common components evident across similar countries (including Australia and the United Kingdom). These are consistent with key conclusions from reviews of New Zealand Police's national intelligence and security systems and counter-terrorism efforts[95] – that counter-terrorism policing requires a specialised, coordinated and integrated approach that includes prevention and community engagement. More specifically there are four critical components of counter-terrorism policing practice:

a) Leadership, strategy and direction.

b) A specialist counter-terrorism function.

c) A whole-of-police effort.

d) An intelligence function.

The assessment that follows is by reference to these four components.

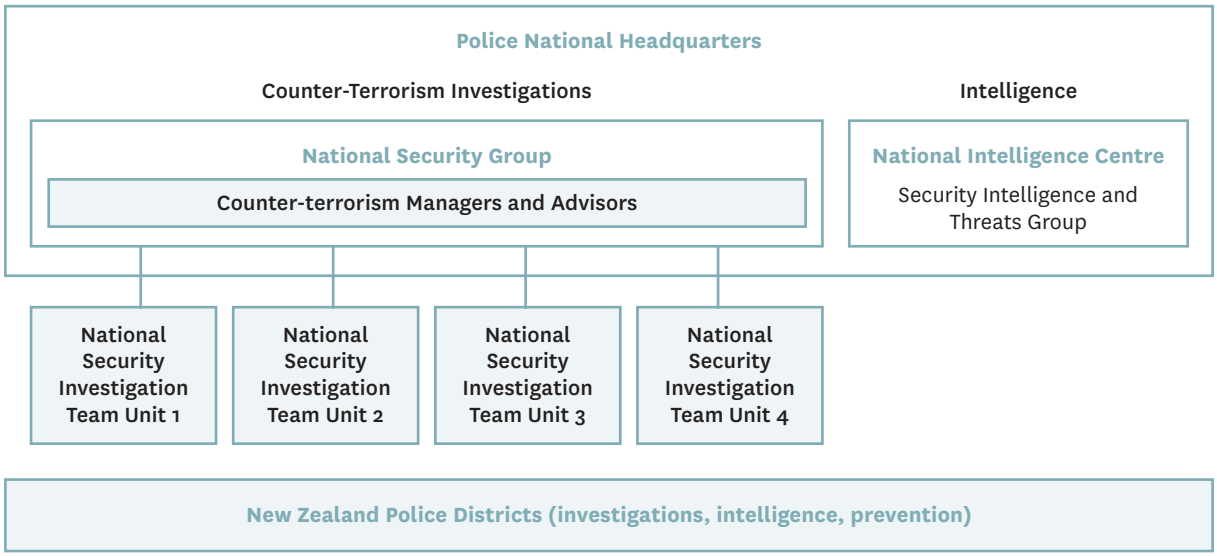
[95] New Zealand Police *National Security Capability Assessment* (March 2011); New Zealand Police *National Security and Counter-Terrorism Capability Review* (September 2015).

6.4 Assessment of New Zealand Police's counter-terrorism efforts

Leadership, strategy and direction

6 New Zealand Police's current organisational structure for its counter-terrorism functions is outlined in the graphic below.

Figure 46: Counter-terrorism functions within New Zealand Police



7 A *National Security Strategy,* which set out New Zealand Police's approach to national security (including counter-terrorism), expired in 2015 and has not been replaced. Those we spoke to within the New Zealand Police National Security Group were able to provide us with a clear and well-articulated explanation of their counter-terrorism approach. This was a New Zealand-specific model particularly focused on prevention and community policing. They attributed the lack of a current strategy document to delays in the finalisation of a whole-of-government counter-terrorism strategy with which New Zealand Police's strategy would have to align. New Zealand Police had been strongly advocating for a whole-of-government counter-terrorism strategy and for changes to counter-terrorism legislation at the Security and Intelligence Board for a considerable period (see Part 8, chapters 3 and 13).

8 The absence of whole-of-government and New Zealand Police counter-terrorism strategies, and a lack of capacity, hampered dissemination of the counter-terrorism policing model widely within New Zealand Police. The National Security Group at Police National Headquarters, which led this work, had only a few full-time equivalent staff.

Specialist counter-terrorism function

9 To operate effectively, New Zealand Police need to identify and investigate potential terrorist threats. This requires specialist teams, with investigative capability, and access to physical and technical surveillance, informant management and forensic accountancy capabilities.[96]

10 As at 15 March 2019, there was one National Security Investigations Team with four units spread across the country. These units were responsible for conducting and/or overseeing investigations related to national security threats. Their work included prevention, detection and disruption of terrorist threats.

11 Those in the National Security Investigations Team were described by New Zealand Police as experienced and capable investigators who had sufficient training in counter-terrorism investigations. Alongside investigation and prosecution, they also worked with individuals to identify what support they required to reduce their risk of engaging in violent extremism. They saw this as often more beneficial than waiting for arrest opportunities. This is consistent with international best practice, which prioritises early intervention by providing at-risk individuals with a range of support services to address their vulnerabilities.

12 International experience has also highlighted challenges with early intervention activities, as they target people who are seen as being at risk of engaging in criminal behaviour but who have not actually engaged in any criminal behaviour. The role of law enforcement agencies in early intervention therefore needs to be carefully managed to ensure that these activities are perceived by those involved as genuine efforts to safeguard and prevent harm, and not as an enforcement tool. New Zealand Police appeared to understand these challenges.

13 Through their early intervention work, New Zealand Police provided at-risk people with the structure and support needed to move them off the path towards violent extremism. They provided individually-designed case management plans or referred people to the Young Person's Intervention Programme. This programme was a multiagency scheme designed to divert young people (aged 14–20) from violent extremism, which was supported by community groups. New Zealand Police involved in the programme felt that it was a useful early intervention tool, but that it was hampered by a lack of funding and limited involvement by community groups.

[96] KM Dunn, R Atie, M Kennedy, JA Ali, J O'Reilly and L Rogerson "Can you use community policing for counter-terrorism? Evidence from NSW, Australia" (2016) 17 *Police Practice and Research* at page 196.

14 We were told that, before 15 March 2019, the National Security Investigations Team's workload was "do-able", but a "stretch". The workload made it difficult at times to devote resources to early intervention and risk Reduction activity. Taking action when specific individuals were identified as a presenting threat took precedence. This was particularly noticeable in resource-intensive operational phases (such as surveillance), during which the National Security Investigations Team had to draw on resources from other parts of New Zealand Police. Pressure of work meant that the National Security Investigations Team did not have the capacity to develop a formal operating model and there was no leads case management system. While their way of operating offered flexibility, such as allowing a focus on early intervention, it also meant that processes, such as assessing risk, prioritising leads and investigations or closing cases, were inconsistent.

15 Recognising these capacity gaps, in 2016, New Zealand Police submitted a budget bid for increased counter-terrorism resource. This was the same budget round as the Strategic Capability and Resourcing Review funding was approved (see Part 8, chapter 2). New Zealand Police's budget bid was unsuccessful. Additional resource was not approved until 2018, when funding for 18 new positions was provided to build counter-terrorism investigations capability and enhance the Police National Headquarters counter-terrorism function. There was comparatively little focus by the Security and Intelligence Board on discussing the resourcing of the overall counter-terrorism effort. This meant there was limited discussion of New Zealand Police's counter-terrorism capacity. And, at a system level, the Public sector agencies involved in the counter-terrorism effort remained unaware of New Zealand Police's resourcing gaps and their consequences.

16 Capacity issues were compounded by the lack of planning and preparation offences in the Terrorism Suppression Act 2002 (see Part 8, chapter 13). New Zealand Police devoted considerable resources to monitoring persons of concern. Some of these people were behaving in ways that may have resulted in prosecution for planning and preparation offences if such offences were provided for in the Terrorism Suppression Act.

A whole-of-police effort

17 Although counter-terrorism policing will often be driven by specialist units, these units need to be able to draw on the wider resources of the national organisation.[97] New Zealand Police have national reach and connections into a wide range of communities through their everyday policing work. The interactions that frontline staff have with communities can provide crucial opportunities to identify emerging threats or people at risk of radicalisation and what support people need to divert from violent extremism. For this to be effective, police outside of specialist units need to have some understanding of indicators of, or behaviours that might lead to, violent extremism and of their roles and responsibilities in countering terrorism.

[97] Sharon Pickering, Jude McCulloch, David Wright-Neville *Counter-Terrorism Policing: Community, Cohesion and Security* (Springer, New York, 2008).

18 The National Security Group was charged with increasing counter-terrorism knowledge and capabilities throughout New Zealand Police so they would "know what to look for and how to engage with suspects".[98] The National Security Investigations Team made efforts to build knowledge throughout New Zealand Police, through an online training module on violent extremism distributed in 2018, discussions with District leadership on the threatscape and implications for New Zealand and specialist training for some District investigators. Some of these trainings and presentations included content on right-wing extremism, including a Senior Investigation Officer course run in Australia by the Australia New Zealand Counter-Terrorism Committee (see Part 8, chapter 17 for more detail on these presentations and training). But while these efforts were reportedly well received, the small number of staff in the National Security Group meant they struggled to fulfil the role of building knowledge throughout New Zealand Police in a comprehensive and systematic way.

19 As a result, the Districts were not well integrated into the counter-terrorism effort. Some staff in the Districts and other units described the National Security Investigations Team as operating in isolation, with limited scope for the Districts to contribute. In the absence of a national case management system for managing leads, there was no obvious place for District staff to record information of relevance regarding people of national security concern. Some District staff thought that this reduced opportunities for frontline staff to look out for relevant information and contribute to the counter-terrorism effort.

20 A 2015 review of New Zealand Police's counter-terrorism capability recommended that a New Zealand Police national prevention coordinator be hired to ensure that counter-terrorism prevention activity would be embedded within District efforts.[99] This coordinator was not in place before 15 March 2019. In the absence of a coordinator, there was limited, informal, coordination between the National Security Investigations Team and other prevention and community policing resources.

21 The National Security Investigations Team's engagement with community policing resources and directly with communities was primarily focused on building relationships with Muslim communities. They did this, for example, through relationships with ethnic liaison officers (see Part 9, chapter 2) and direct engagement with masajid in some areas. The way the National Security Investigations Team went about this is in line with good practice. They were not, however, working in a planned and deliberate way with other parts of the community policing system to identify non-Islamist extremist threats, such as right-wing extremism.

[98] New Zealand Police (2011, 2015), footnote 95 above.

[99] New Zealand Police (2011, 2015), footnote 95 above.

Intelligence function

22 New Zealand Police's intelligence model was developed in 2008. As designed, it consists of national-level and District-level functions, which are coordinated under one system. The National Intelligence Centre is responsible for collecting and assessing information to develop strategic intelligence that informs the Police Executive about emerging risks and where they should direct resources. Units within the National Intelligence Centre also deliver operational and tactical intelligence, such as the Security and Intelligence Threats Group, which is responsible for national security intelligence. Each of the 12 Districts has an intelligence team. They are responsible for collecting and assessing information to develop all tactical, most operational and some strategic level intelligence on District-level issues (for example, current or emerging crime trends) to inform local deployment priorities. Strategic intelligence products created at the national level should inform District-level intelligence collection and operational priorities.

23 As at 15 March 2019, New Zealand Police's intelligence function was not working optimally. High staff turnover led to a loss of capacity and capability, variable use of intelligence across the Districts and a loss of strategic focus. In December 2018, New Zealand Police launched the *Transforming Intelligence 2021* strategy in acknowledgement that the capacity and capability of their intelligence function had degraded. That strategy put in place a plan to renew the intelligence function.[100]

24 New Zealand Police's intelligence function is central to the counter-terrorism policing effort, at both the tactical and strategic level. For counter-terrorism, tactical intelligence can involve gathering information to identify and build profiles of individuals or groups of concern, which are then used by investigators. Strategic intelligence is used to build a picture of current and emerging issues and therefore guides organisational priorities. Strategic intelligence is important in building a picture of the local counter-terrorism environment. The Financial Intelligence Unit also contributes intelligence to New Zealand Police's counter-terrorism effort.

25 New Zealand Police's strategic intelligence reporting could have provided a useful contribution to the national security system's understanding of the domestic threatscape. Before 2015, New Zealand Police had been producing strategic intelligence reports on a wide range of domestic threats. We have discussed the most relevant of these in Part 8, chapter 4 above.

[100] The *Transforming Intelligence* 2021 programme includes 11 streams of work: Intelligence Operating Model, National Security, Target Development Centre, Open Source, Child Protection Offender Register, Critical Command Information, Collections, Intelligence Systems, Performance, Training and Intelligence Support to major events.

26 New Zealand Police's strategic intelligence capability declined after 2014. There was limited strategic focus on counter-terrorism from the intelligence system. We heard that the wide remit of the Security and Intelligence Threats Group, combined with its limited capacity and competing demands, constrained what that group could realistically do on counter-terrorism. The National Intelligence Centre provided briefings to New Zealand Police leadership that included strategic level content on terrorism and violent extremism. However, the National Intelligence Centre did not produce many strategic products on counter-terrorism to inform national and District priorities. This, combined with the lack of capacity in District-level collections activity, meant that collection staff were not collecting information that would help to build a picture of the domestic extremist environment.

27 The New Zealand Police intelligence function also provides important tactical support to counter-terrorism efforts. The Security and Intelligence Threats Group runs daily scans across New Zealand Police information holdings for issues of national security concern and compiles assessments on individuals of concern. Their effectiveness relies on the quality of information being recorded in the databases. There were barriers to intelligence analysts accessing all of the information they needed, as New Zealand Police information is kept across multiple databases. Intelligence analysts in the National Intelligence Centre only recently gained access to the database that holds the National Security Investigations Team's case profiles. Information being held in many places makes it harder to create a full intelligence picture.

28 The National Security Investigations Team's North Island-based units each had their own embedded intelligence analyst. A decision to move the South Island national security intelligence analyst resources into the general pool of intelligence analysts was revisited after 15 March 2019. It was agreed that those resources could be based within the South Island unit if desired.

29 We heard that, before 15 March 2019, effort at the District level was directed to counter-terrorism (for example, scanning the local environment to generate leads) only where District leadership had an interest in it. District intelligence staff had not received specialist training on violent extremism indicators, meaning that their ability to undertake risk assessments and contribute to counter-terrorism efforts would have been limited.

6.5 What were New Zealand Police doing about right-wing extremism?

Intelligence assessments

30 In Part 8, chapter 4, we described how New Zealand Police produced intelligence reports on several right-wing extremist groups in New Zealand up until 2015. We observed that New Zealand Police had generally viewed right-wing extremism as more of a public order issue than a potential terrorist threat.

31 In 2014, New Zealand Police produced two intelligence assessments published by the National Assessments Committee of particular relevance to the extreme right-wing threat in New Zealand. These were the last formal assessments of extreme right-wing groups in New Zealand for national security purposes. This was before there was a global eruption of hateful content online in 2015 and 2016 (see Part 8, chapter 2). At this time the nature of right-wing extremism was changing. International developments demonstrated that traditional street-based organisations were being supplemented by new groupings and that the indicators of allegiance to new right-wing extremist groups were different to those of the past.

32 From 2015 until 15 March 2019, New Zealand Police were not producing strategic intelligence on far right individuals and groups. They were aware of new far right groupings, but they had not assessed the groups systematically or produced a national intelligence assessment of the contemporary far right environment. We have also seen some evidence that New Zealand Police had given some thought to the possibility that Muslim communities in New Zealand could be the target of threats, such as the 2018 *National Security Situation Update* identifying periods in which Muslim individuals and communities were potentially at heightened risk of attack, such as Ramadan.

33 New Zealand Police undertook preliminary steps to produce a national assessment of the right-wing extremism environment subsequent to a meeting with the New Zealand Security Intelligence Service in late 2018 but limited progress had been made by 15 March 2019. As a result, New Zealand Police were not in a position to update their understanding of the indicators of right-wing extremism and disseminate this information to the front line.

Leads on right-wing extremists

34 The National Security Investigations Team receives leads through a variety of channels, including from their own activities and from public reporting, frontline reporting and other agencies (for example, the New Zealand Security Intelligence Service). They described themselves as "threat agnostic" – meaning that when they receive a lead, they use the same assessment criteria regardless of the ideological source of the threat. In assessing the risk of an individual or group they look for indicators of an intention to use violence in support of an extremist ideology and the capability (the skills, knowledge and resources) to do so. There are a range of indicators that can be used to assess a person's radicalisation and mobilisation to violence, such as having accessed extremist websites, made statements inciting the use of violence, purchased weapons or conducted online research into targets.

35 The majority of the National Security Investigations Team's resources were devoted to Islamist extremism. The reason they provided for this focus of effort was that the majority of the leads they received were related to possible Islamist extremism. There were aspects of the ways New Zealand Police generated leads – for example, the nature of their engagement with Muslim communities – that were conducive to generating Islamist extremist leads. New Zealand Police were successful in mitigating the threats they identified. For example, between August 2015 and January 2018, New Zealand Police arrested 17 individuals of national security interest for a variety of offences and issued 40–50 warnings for extremism-related objectionable publication offences.

36 We were also provided examples from the National Security Investigations Team of leads related to right-wing extremism that met the risk threshold and were pursued.

37 The National Security Investigations Team acknowledged to us that they did not consistently use standardised criteria for assessing leads. Staff made decisions about whether to continue assessing an individual based on professional judgement. It is expected that individuals would use their knowledge and experience to inform their decision-making. However, neither the assessment criteria nor individuals' professional judgement were informed by detailed updated indicators of right-wing extremism after 2015-2016. Inconsistent use of assessment criteria can create risks that decisions are influenced by unconscious bias. This risk would have been greater given that New Zealand Police had limited knowledge and understanding of recent strands of right-wing extremism and therefore less experience assessing individuals associated with these ideologies.

38 We saw examples of frontline or other staff (such as ethnic, Pacific or iwi liaison officers) alerting the National Security Investigations Team to possible cases of right-wing extremism. However, to be assured that New Zealand Police were treating all reports of potential right-wing extremism seriously we would need to see that all staff could recognise indicators of right-wing extremism. We did not receive assurances that there was sufficient awareness and training on right-wing extremism for this to be the case.

6.6 System awareness of New Zealand Police capacity and capability gaps

39 The gaps in New Zealand Police's counter-terrorism efforts – the limited capacity of their investigations team, the degraded nature of their intelligence function and the fact that they were no longer producing assessments on the extreme right-wing and strategic assessments on domestic extremism – were not explicitly highlighted with the Security and Intelligence Board and Counter-Terrorism Coordination Committee.

6.7 Experiences of Muslim communities with New Zealand Police

40 Counter-terrorism policing relies on people having trust and confidence in police so that they are comfortable reporting threats against themselves and their communities and threats within their communities.

41 We heard from ethnic liaison officers about their efforts to build meaningful and mutually-beneficial relationships with Muslim communities (see Part 9, chapter 2). However, being part of the counter-terrorism effort presents challenges for the parts of New Zealand Police tasked specifically with community policing, such as ethnic, Pacific and iwi liaison officers. For police staff focused on community engagement, being involved in counter-terrorism activities can risk compromising community trust because they can be seen by communities as using the relationships they build primarily for collecting intelligence.

42 International experience has shown that to manage these tensions, police need to work in partnership with communities. A partnership approach does not exclude the collection of community intelligence. But it requires that any intelligence collection occurs alongside police prioritising the security concerns that community members bring to them, and working collaboratively to increase their safety and security.

43 The National Security Investigations Team was aware of the importance of not stigmatising and alienating communities. For example, when concerns were raised by Muslim communities about people charged for offences under the Films, Videos, and Publications Classification Act 1993, the National Security Investigations Team attended public forums and developed a brochure explaining that the reason for the charges was that downloading objectionable material was a national security indicator. They explained that they used a graduated approach where they would only charge people after they had first warned the individual. Their intention was early disengagement with charging as a last resort. However, we heard that the National Security Investigations Team did not always act in ways that were cognisant of the ethnic, Pacific or iwi liaison officers' need to maintain community trust.

44 We heard a range of concerns from Muslim individuals and communities about reports they have made to New Zealand Police about suspicious or threatening behaviour (see *Part 3: What communities told us*). In some instances they felt that staff did not have the ability to recognise behaviours, signals or patterns of incidents that could signify possible hate crimes or signs of extreme right-wing activity. We were told of instances where people did not see staff writing anything down when making reports. We heard that people rarely received any follow up from New Zealand Police after making reports. This meant that many of the Muslim individuals and communities we heard from felt that New Zealand Police did not take their concerns seriously.

45 At the same time, efforts to engage with Muslim communities have been viewed by some as primarily intended to gather intelligence about possible Islamist extremists. We have observed that Muslim individuals and communities have often been proactive and cooperative with New Zealand Police efforts to identify and mitigate the risk of Islamist extremism. However, for many, the perceived overt focus on Islamist extremism without a corresponding focus on threats they were reporting created frustration and diminished their trust in New Zealand Police.

46 A summary of New Zealand Police's interactions with members of Muslim communities since 2010 demonstrates that New Zealand Police looked into many reports of suspicious or threatening behaviour made by Muslim individuals or communities. In some cases, New Zealand Police spoke to those accused, issued warnings and pursued prosecution. In other cases, New Zealand Police staff felt unable to act due to a lack of evidence or legislative constraints regarding hate crime (see Part 9, chapter 4). Where New Zealand Police had acted, it is not always clear that they reported back to the complainants about the outcomes of their inquiries. We heard from community members that where New Zealand Police had reported back, this was not always in a way that reassured the complainant that the issue had been thoroughly investigated.

6.8 Developments since 15 March 2019

47 Since 15 March 2019, New Zealand Police have been developing a more formalised and integrated approach to counter-terrorism. They are now developing an operational model that proposes a more graduated response, where low-risk cases are managed by frontline staff and high-risk cases stay under the management of the National Security Investigations Team. There is a focus on building District capabilities across investigations, intelligence and prevention, and building connections between the National Security Investigations Team and Districts. New Zealand Police have now implemented the recommendation made in 2015 for a dedicated role focused on coordinating prevention work. A national prevention coordinator (see above) now leads the newly created Multi-Agency Coordination and Intervention Programme, which builds on the Young Person's Intervention Programme but is for adults.

48 Widespread changes to intelligence capability and capacity are occurring through *Transforming Intelligence 2021*. Changes are also being made to improve intelligence support for counter-terrorism, which is now identified as a priority area for New Zealand Police intelligence.

49 Immediately after 15 March 2019, there was an influx in public reporting of possible national security leads, including leads relating to right-wing extremism (see Part 8, chapter 3). A National Security Case Management process is being developed to formalise and standardise the leads prioritisation process and manage the increase in public reporting. A standardised risk assessment tool will be developed and the model will allow the Security and Intelligence Threats Group, National Security Investigations Team and District intelligence to manage leads through a centralised location and process. New Zealand Police also created a list of individuals of right-wing extremist concern. This list was developed by reviewing existing New Zealand Police holdings and from new information reported by the public.

6.9 Concluding comments

50 The absence of both a whole of government counter-terrorism strategy (see Part 8, chapter 3) and a New Zealand Police counter-terrorism policing strategy limited the ability of staff outside specialist units to understand the contribution they could make to preventing and countering terrorism. While the specialist units within New Zealand Police showed evidence of good practice, especially in their focus on early intervention and prevention, their efforts were hampered by their limited capacity. This also limited their ability to build counter-terrorism policing capability throughout New Zealand Police and as a result many frontline police staff lacked a clear understanding of how to recognise indicators of violent extremism. Overall, New Zealand Police lacked adequate specialist counter-terrorism capacity and were not using their full policing resource in their efforts to counter violent extremism and terrorism.

51 Before 2015, New Zealand Police had been paying some attention to right-wing extremism in New Zealand by identifying and monitoring the general criminal activities of traditional street-based groupings and by managing their potential threat to public order. The risk of right-wing extremism was assessed in the two 2014 assessments we have referred to and in passing in the 2018 *National Security Situation Update*. They also opened and pursued leads with possible connections to the extreme right-wing. But in the years preceding 15 March 2019 the focus of New Zealand Police's counter-terrorism effort was undoubtedly on Islamist extremism.

52 By 2015, New Zealand Police's intelligence function had degraded, limiting what it could contribute to understanding the domestic terrorism environment. Without an up-to-date understanding of right-wing extremism in New Zealand, including the emerging groups and networks, New Zealand Police were not well placed to understand the threat and how to identify it.

53 As noted above, since the 15 March 2019 terrorist attack, New Zealand Police have created a list of individuals of right-wing extremist concern. That this list was developed (in part) by New Zealand Police reviewing their existing holdings demonstrates that they had information on the extreme right-wing already. New Zealand Police were also able to gather much more intelligence on the extreme right-wing after 15 March 2019, as more people had become aware of the potential risks to look out for due to heightened public awareness.

54 The limited capacity of New Zealand Police's national security investigations team and the degraded nature of their intelligence function were not brought to the attention of the Security and Intelligence Board and Counter-Terrorism Coordination Committee. For this reason the residual risk the counter-terrorism effort was carrying was therefore not fully understood.

55 New Zealand Police understood the importance of community trust and confidence for their counter-terrorism activities to be successful and had made efforts in this area. However, for many Muslim individuals, the focus on their communities as potential sources of terrorist activity and perceived corresponding lack of attention paid to threats against them diminished their trust in New Zealand Police. It was evident that New Zealand Police had been acting on concerns raised by Muslim individuals and communities but this was not always properly communicated. This highlights the important role feedback loops play in providing trust and the need for more focus from New Zealand Police on providing this reassurance.

Chapter 7: The Government Communications Security Bureau

7.1 Overview

1 The Government Communications Security Bureau is New Zealand's signals intelligence agency.

2 Understanding exactly how signals intelligence works and what skilled practitioners can achieve within a particular authorising environment is not straightforward. Of all the activities in New Zealand's counter-terrorism effort, signals intelligence is the least understood by those outside of the discipline.

3 In this chapter we:

a) explain what signals intelligence brings to the counter-terrorism effort;

b) discuss reviews of the Government Communications Security Bureau, and international approaches to signals intelligence; and

c) assess the Government Communications Security Bureau's contribution to the domestic counter-terrorism effort, including its technical capability and capacity, and staffing and leadership.

7.2 What signals intelligence brings to the counter-terrorism effort

4 Among its other activities, including cyber security, the Government Communications Security Bureau conducts signals intelligence. This means it identifies, collects and reports on targets' communications (signals, such as phone calls and emails). It also collects and analyses data about communications (metadata). As well, it enables its New Zealand customers to access signals intelligence produced by its international partners.

5 The value of a signals intelligence agency to a counter-terrorism effort is that it can collect information that no other agency can. Its collection techniques can make physical distance from a target meaningless. Once access and appropriate authorisation are in place, signals intelligence collection is often much faster than other intelligence collection activities. It is also usually far less risky than human intelligence operations in terms of the personal safety of those involved.

7.3 Reviews and international approaches to signals intelligence

6 The reputation of the Government Communications Security Bureau was badly affected by the Dotcom controversy and the Snowden revelations (see Part 8, chapter 2). The 2013 review of compliance at the Government Communications Security Bureau found issues with compliance that were a consequence of underlying problems in the Government Communications Security Bureau's structure, management, capacity and capability.[101]

7 The *2014 Government Communications Security Bureau Functional Review*[102] noted that government, Parliament and the public should expect to have a signals intelligence agency that is "highly effective at conducting sophisticated intelligence activities against any legitimate targets, no matter how hard".

8 The 2014 *Performance and Improvement Framework* review highlighted several performance challenges for the intelligence and security agencies, including creating a "more seamless collaboration to achieve … products and services that are prized by its key customers".[103] In relation to the Government Communications Security Bureau, the review noted the following:

a) The increasing importance of the internet and "big data" for the Government Communications Security Bureau. It stated that "given uncertainty as to future threats, [the Government Communications Security Bureau] needs to maintain and develop technology and technical skills in areas of plausible future risk, even if these areas are not currently a priority".[104]

b) The importance of maintaining the tradecraft and skills that the Government Communications Security Bureau analysts develop through prosecuting dynamic, non-institutional counter-terrorism targets and that "the value of signals intelligence in safeguarding New Zealand against violent extremism is in identifying previously unknown threats through analysis of online behaviours".[105] Its capability to identify threats was growing and there was an opportunity to assist the New Zealand Security Intelligence Service and New Zealand Police. This was challenging new ground, given the associated privacy implications.

c) The importance of the relationship with the New Zealand Security Intelligence Service. It commented that developing a "supportive partnership … between staff [of both agencies] at all levels should be an early priority" and success would come in the form of a "close and cooperative working relationship … with staff in both agencies having an improved understanding and appreciation of each other's contribution to national security and enjoying bringing their skills to selected joint projects".[106]

[101] Rebecca Kitteridge, footnote 39 above.

[102] Government Communications Security Bureau *Government Communications Security Bureau Functional Review* (March 2014).

[103] *Performance Improvement Framework*, footnote 42 above at page 12.

[104] *Performance Improvement Framework*, footnote 42 above at pages 41-42.

[105] *Performance Improvement Framework*, footnote 42 above at page 48.

[106] *Performance Improvement Framework*, footnote 42 above at pages 43-44.

9 The 2014 *Performance and Improvement Framework* review of the New Zealand Intelligence Community also suggested:

> *To help Ministers clarify the priorities for national security and the scope of [the New Zealand Intelligence Community's] role and how that applies to the [Government Communications Security Bureau], the [Government Communications Security Bureau] needs to provide advice on the likely gains, costs and risks of allocating its collection resources to different priorities, and to help identify possible trade-offs.*[107]

10 We observed that, in other countries, human intelligence and signals intelligence agencies had deep mutual understanding of each other's capabilities, characteristics and constraints. This was also evident in the relationships between those agencies and police. We heard in other countries that co-location of different agencies can minimise these challenges. Co-location of agencies is a good first step, but the real value has been agencies working together on live operations – not just on Response activities, but also Reduction activities. Joint action on Reduction can generate valuable insight into opportunities for the counter-terrorism effort.

11 In the United States of America, the *9/11 Commission Report* commented on joint action, saying that the National Security Agency:

> *... did not think its job was to research [the identities of potential terrorists]. It saw itself as an agency to support intelligence consumers, such as the Central Intelligence Agency. The [National Security Agency] tried to respond energetically to any request made. But it waited to be asked.*[108]

12 The *9/11 Commission Report* argued that cooperation is not the same as joint action:

> *When agencies cooperate, one defines the problem and seeks help with it. When they act jointly, the problem and options for action are defined differently from the start.*[109]

7.4 Contribution to the domestic counter-terrorism effort

13 The Government Communications Security Bureau first established a standing counter-terrorism capability in 2003. From 2003 to 2016, it led an effort to close a recognised gap in the Five Eyes counter-terrorism effort. This also involved international parties outside the Five Eyes partnership. As well, the Government Communications Security Bureau provided some support to New Zealand Police and the New Zealand Security Intelligence Service.

[107] *Performance Improvement Framework*, footnote 42 above at page 42.

[108] *The 9/11 Commission Report*, footnote 81 above at page 353.

[109] *The 9/11 Commission Report*, footnote 81 above at page 400.

14 From 2016, the Government Communications Security Bureau began to change its counter-terrorism approach to more closely align its efforts with the revised National Intelligence Priorities (see Part 8, chapter 3). It shifted focus to the domestic counter-terrorism effort and explicitly became a customer-led organisation. The Government Communications Security Bureau considered the New Zealand Security Intelligence Service to be the lead agency for domestic counter-terrorism. The New Zealand Security Intelligence Service thus became the Government Communications Security Bureau's primary customer for counter-terrorism signals intelligence. All other New Zealand agencies' counter-terrorism tasking occurs through this primary customer.

15 From 2016, all of the Government Communications Security Bureau's counter-terrorism activities were the result of specific tasking by another agency. This means the Government Communications Security Bureau does not "unilaterally undertake domestic counter-terrorism investigations" and does not "self-task or identify its own intelligence questions" for any counter-terrorism activity, domestic or international:

> *[The Government Communications Security Bureau]'s counter-terrorism mission does not have any standing capability to unilaterally detect terrorist or potential terrorist activity that has not come to attention by other means. [The Government Communications Security Bureau] responds to intelligence requirements or "leads" provided by a domestic or international agency, which arise from an already instigated intelligence investigation, incidental collection, or through partner reporting. Once a "lead" or subject of investigation is established, [the Government Communications Security Bureau] is able to provide in-depth analysis including discovery of potentially previously unknown relationships.*

16 This customer-led model relies on having informed and experienced counter-terrorism customers who understand current signals intelligence capabilities and how they might be used.

17 The New Zealand Security Intelligence Service is still recovering from the significant loss of its own capability and experience (see Part 8, chapter 5). The New Zealand Security Intelligence Service, possibly correctly, does not regard it as appropriate or necessary for its staff to have a full understanding of the Government Communications Security Bureau's capability. But without an understanding of the Government Communications Security Bureau's capability, the New Zealand Security Intelligence Service's ability to maximise contributions from signals intelligence to the counter-terrorism effort is constrained.

18 The working relationship between the Government Communications Security Bureau and New Zealand Police and the border agencies is not particularly close. Staff in these agencies therefore also do not have a good understanding of the capabilities of the Government Communications Security Bureau.

19 We acknowledge the Government Communications Security Bureau's efforts to enhance its customer service, as recommended by the 2014 *Performance and Improvement Framework* review. But whether the Government Communications Security Bureau's customer-led model remains the appropriate approach for New Zealand's domestic counter-terrorism effort has not been discussed at a whole-of-system level.

20 In 2016, the Government Communications Security Bureau considered its key contributions to the counter-terrorism effort included lead generation for target discovery purposes (see Part 8, chapter 10), undertaking internet operations and using advanced data collection and analysis techniques. It expected to be able to conduct more comprehensive target discovery once the Intelligence and Security Act 2017 came into force. It identified international coverage and providing technical assistance to the New Zealand Security Intelligence Service operations as other contributions it could make.

21 In June 2017, the Government Communications Security Bureau established a new line of domestic counter-terrorism activity – New Zealand foreign fighters. Any spare capacity was to be directed at a joint effort with a Five Eyes partner on non-New Zealand foreign fighters, in line with New Zealand's international counter-terrorism effort (in this case to understand the potential problem returning foreign fighters might pose to a particular global region). In the same year, the Government Communications Security Bureau advised the incoming Minister Responsible for the Government Communications Security Bureau, Hon Andrew Little, that it was modernising its counter terrorism capability. It also advised that the traditional distinctions between signals intelligence and human intelligence were "becoming less important as the complexity of the threatscape … continues to rise … [and] multidisciplinary responses are required to keep pace with those who seek to harm New Zealand". This echoed the point made in the 2014 *Government Communications Security Bureau Functional Review.*[110]

22 The Government Communications Security Bureau counter-terrorism activities include a 24-hour watch service, which can quickly circulate threat intelligence. It also participates in international and domestic forums. For a time, the Government Communications Security Bureau was a participant in a signals intelligence effort with European partners, the benefits of which applied to both the domestic and international aspects of New Zealand's terrorism intelligence priority.

[110] Government Communications Security Bureau, footnote 102 above.

23 In 2018, the Government Communications Security Bureau's standing warrants and authorisations enabled it to conduct activity against individual and organisational targets including:

a) those listed in the United Nations Security Council's list maintained pursuant to the *United Nations Security Council Resolution 1988,* the Dā'ish and Al Qaeda sanctions list, and the list established by the New Zealand Government or listed in the Terrorism Suppression Act 2002;

b) those engaged in terrorist acts or with links to those engaged in terrorist acts; and

c) extremists and those who advocate for politically or religiously motivated violence.

7.5 Technical capability and capacity

Technical capability

24 We discuss in Part 8, chapter 2 some of the key changes in communications and the threatscape that have impacted on counter-terrorism efforts, including the prevalence of end-to-end encryption. Signals intelligence agencies around the world have responded to the latest shifts in the environment in various ways. For example:

a) They have sought to develop the technical means to exploit modern communications even as communications technology changes over time.[111]

b) They are investing in data collection and analysis. Smart analysis of bulk data (see Part 8, chapter 10) can reduce large amounts of information to a point where it can practicably be analysed by signals intelligence professionals.

c) They have changed their tradecraft through the development of tools and analytical techniques in order to exploit the wide range of communications now available.

25 The Government Communications Security Bureau has had to consider how to respond to the changing operational environment. The 2014 *Government Communications Security Bureau Functional Review* recommended that it fundamentally shift away from existing capabilities and refocus on two emerging areas of internet operations. The need for change was "urgent and the change required was revolutionary, not evolutionary if the [Government Communications Security Bureau] [was] not to be left without significant capabilities".[112]

[111] Government Communications Security Bureau, footnote 102 above.

[112] Government Communications Security Bureau, footnote 102 above at pages 5 and 10.

26 The Government Communications Security Bureau has found it difficult to make this important change quickly. One of the emerging areas of internet operations is of particular interest to us. A 2019 Treasury review of that project considered it was "mission critical" and noted that the Government Communications Security Bureau was five years behind its Five Eyes partners. According to this review, the capability was fundamental to the mission of the entire New Zealand Intelligence Community and an important bridge between human intelligence and signals intelligence:

> *[W]ithout this capability … the New Zealand intelligence community's capability to deliver intelligence has fallen, which threatens its ability to keep New Zealanders safe.*

Staffing and leadership

27 Staff numbers working on domestic counter-terrorism have been limited, because the Government Communications Security Bureau dedicates more resources to other National Security and Intelligence Priorities (see Part 8, chapter 3). It considers its unique technical capabilities are better suited to those other priorities and that counter-terrorism is covered by other agencies.

28 Approximate intelligence staff numbers (including graduates) dedicated to domestic counter-terrorism at the Government Communications Security Bureau[113] in recent years were two in 2015, four in 2016 (increased by graduates), two in 2017 and seven in 2018.

29 Leadership is important to the effectiveness and efficiency of an agency. The Government Communications Security Bureau has had seven Directors-General in ten years (six Directors-General between 2010 and 2016, when the current Director-General was appointed) and significant movement at the second tier. This is substantial change for a Public sector agency and has not helped the organisation to recover quickly from the Dotcom and Snowden controversies. Nor has it helped to achieve the transformational change envisaged in various reviews since 2013, including the Strategic Capability and Resourcing Review and the 2018 *Performance Improvement Framework* follow-up review.[114]

7.6 Concluding comments

30 The Government Communications Security Bureau has the potential to make a key contribution to the counter-terrorism effort because it can collect information that no other Public sector agency can collect. Yet in the years before 15 March 2019 the role it was playing in domestic counter-terrorism was limited.

[113] This number does not include staff in other areas of the Government Communications Security Bureau whose work may contribute in part to its counter-terrorism activity.

[114] *Performance Improvement Framework*, footnote 42 above.

31 Past reviews signalled the need for transformational change within the Government Communications Security Bureau. This has been difficult to achieve for an organisation still dealing with the adverse effects of the Dotcom and Snowden controversies, which significantly diminished public confidence in it. The absence of stable leadership between 2010 and 2016 made it harder for the Government Communications Security Bureau to recover from these incidents and make the required transformational change.

32 The Government Communications Security Bureau moved to operate as a customer-led organisation. This means that it engages in domestic counter-terrorism only when tasked by another agency. Its customer focus has limited the ability of the Government Communications Security Bureau to undertake joint action with other Public sector agencies involved in the domestic counter-terrorism effort. Its customers did not always have sufficient understanding of signals intelligence capabilities to know how its contributions could be maximised. This may be unnecessarily limiting the ability of the counter-terrorism effort to get the most out of signals intelligence. The effects of the customer-led model and whether it was the right approach for New Zealand's counter-terrorism effort have not been considered at the whole-of-system level.

33 The Government Communications Security Bureau has experienced delays in developing the new technical capabilities required to respond to well-understood trends in communications and the threatscape. This has not been helped by the small numbers of staff working on domestic counter-terrorism. The Government Communications Security Bureau's unique technical capabilities are such that we think it could and should have a more active role in the domestic counter-terrorism effort.

Chapter 8: The border agencies

8.1 Overview

1 As outlined in *Part 6: What Public sector agencies knew about the terrorist*, the border agencies did not identify the individual as presenting a terrorist threat when he travelled in and out of New Zealand. This chapter provides an assessment of the border agencies' roles in the counter-terrorism effort.

2 In this chapter, we:

a) describe the border agencies and their roles in the counter-terrorism effort;

b) explain how the agencies identify terrorism threats;

c) discuss the coordination of the border agencies with the counter-terrorism effort;

d) explain how the border agencies screened for right-wing extremist terrorist threats;

e) describe the experiences of Muslim travellers at the border; and

f) discuss developments that have occurred after 15 March 2019.

8.2 The border agencies

3 Immigration New Zealand and New Zealand Customs Service see themselves as "support" and "contributor" agencies to New Zealand's counter-terrorism effort. They both attend the Security and Intelligence Board and New Zealand Customs Service also attends the Counter-Terrorism Coordination Committee (see Part 8, chapter 3). Both agencies have accountabilities in managing border alerts and ensuring New Zealand's compliance with United Nations Security Council resolutions.

4 One of Immigration New Zealand's main functions is to manage the entry of non-New Zealand citizens who wish to visit, work, study or live in New Zealand. Immigration officers make decisions about who can enter New Zealand according to criteria set out in the Immigration Act 2009, Immigration Regulations 2010 and Immigration Instructions (which are certified by the Minister of Immigration).

5 Immigration New Zealand "does not have a dedicated counter-terrorism function" and sees itself as "peripheral to the counter-terrorism system". Immigration New Zealand told us that they contribute to the counter-terrorism effort as part of the multi-agency management and risk mitigation of potential terrorist threats with immigration elements. New Zealand's policy is to manage immigration risk offshore wherever possible rather than at the border.

6 New Zealand Customs Service's main purpose is "protecting New Zealand from risks and threats at the border" while advancing New Zealand's economy. These risks and threats cover a wide range, from illegal weapons, objectionable material, illicit drugs and hazardous substances, and people, including those of terrorism concern.

7 New Zealand Customs Service staff perform limited immigration duties on behalf of Immigration New Zealand at passport control.[115] These duties include checking travel documentation, issuing visas and granting entry permission to legitimate travellers.

8 New Zealand Customs Service state that counter-terrorism is a "priority one" focus. However, other threats such as drugs and revenue evasion present more frequently at the border.

9 New Zealand Customs Service have a counter-terrorism intelligence team that supports frontline officers to respond to potential terrorism threats identified at the border. These potential threats also include people leaving New Zealand to participate in terrorism-related activities such as seeking to join designated terrorist entities in international conflict zones. The counter-terrorism intelligence team sets its work programme based on intelligence it creates or receives on new and emerging threats (including intelligence received from the Border Five agencies,[116] which it assesses for relevance to New Zealand).

8.3 How border agencies identify terrorism threats

10 Immigration New Zealand and New Zealand Customs Service each have their own process for identifying terrorism threats. There are four main points where they can identify and act on terrorism threats. These are:

a) during the visa application process;

b) before passengers depart for New Zealand;

c) before passengers arrive in New Zealand; and

d) when passengers arrive at the New Zealand border.

11 The process the agencies use to assess risk at each of these points is described below.

Applying for a visa

12 On arrival in New Zealand, Australian citizens are eligible for a resident visa (with entitlements to work and study). This eligibility comes from the Trans-Tasman Travel Arrangement. They do not need to apply for pre-departure visas.

[115] Office of the Controller and Auditor-General *Report on Border Security: Using information to process passengers* (June 2017).

[116] The Border Five is a trusted partnership that evolved from the Five Eyes intelligence relationship. See Office of the Controller and Auditor-General, footnote 115 above.

13 Before 15 March 2019, visitors from the 61 visa waiver countries[117] could also apply for their visitor visa and entry permission together when they arrived in New Zealand by completing an arrival card and presenting it at the border. They also did not have to apply for pre-departure visas.

14 Travellers from all other countries must apply for their visa and have it approved by Immigration New Zealand before departing for New Zealand.

15 When assessing visa applications Immigration New Zealand use information they already hold on individuals and national security instructions when determining whether an individual poses a risk to national security.

16 Immigration New Zealand rely on national security instructions to determine if a visa applicant requires a National Security Check before their visa application can be processed. The national security instructions include a list of countries or territories of possible security concern, including those known for extremism. This list is primarily focused on people who have connections with African, Asian and Middle Eastern countries. If a National Security Check is required, this is carried out by the New Zealand Security Intelligence Service.[118]

Before departing for New Zealand

17 Passengers are assessed for risk by Immigration New Zealand before boarding a flight.

18 Immigration New Zealand receive passenger information through the Advanced Passenger Process. This information is sent from the airline as each flight checks in. The data is automatically checked to confirm that passengers have the correct visas,[119] that the passport details do not appear in the International Criminal Police Organization's (INTERPOL's) database of lost or stolen passports and that no border alerts have been raised about a passenger.[120]

19 Immigration New Zealand also identify risks through its Risk Targeting Programme. Flights are assessed as low, medium or high risk. Flights that are considered high risk are assigned to an immigration officer for manual screening of every passenger's information[121] against immigration risk indicators and Immigration New Zealand's target advice on terrorism. The target advice on terrorism is developed with information provided by other Public sector agencies including the New Zealand Security Intelligence Service. The targeting rules are mostly built around clusters of individual risk factors that, when present in a single travel record, indicate that the person may be a potential security risk. Flights that are considered low or medium risk are not assessed. The Risk Targeting Programme continues while the flight is travelling to New Zealand.

[117] Listed in Schedule 2 of the Immigration (Visa, Entry Permission, and Related Matters) Regulations 2010.

[118] The New Zealand Security Intelligence Service is currently undertaking a review of the National Security Check process for visa and other immigration applications.

[119] This does not apply if they are a New Zealand citizen, Australian citizen or are eligible for a visa waiver.

[120] Office of the Controller and Auditor-General, footnote 115 above.

[121] Immigration New Zealand uses the Advanced Passenger Processing data and the Passenger Name Record data. Passenger Name Record data is provided by the airline up to 72 hours before the flight's departure. It contains a range of information, including passengers' biographic data, itinerary, ticket information, contact details and means of payment. Passenger Name Record data is held by New Zealand Customs Service but Immigration New Zealand also has access to it.

20 If any risks are identified from Advanced Passenger Processing (for example, if someone is on a no fly list) or through the Risk Targeting Programme, Immigration New Zealand will instruct the airline not to allow the person to board the plane. Immigration officers may also speak to the passenger before making their final decision.[122] If the risk is identified too late to allow this to happen, an alert will be placed in New Zealand Custom Service's database and it will be addressed when the passenger arrives at the border. If a potential terrorism threat is indicated, Immigration New Zealand will also inform the New Zealand Security Intelligence Service.

21 In 2017, the Auditor-General highlighted the Immigration New Zealand process as "inefficient"[123] because, in practice, only flights classed as posing a high risk were assessed.

Before arriving in New Zealand

22 New Zealand Customs Service assess passengers for risk before their arrival in New Zealand but this generally occurs after the flight has departed.

23 New Zealand Customs Service run their automated, rules-based targeting system across the Passenger Name Record, passport and flight data.[124] The counter-terrorism rules-based targeting system is built from a terrorism risk profile developed by New Zealand Customs Service's intelligence team to aid in detecting possible border-related offending. The terrorism risk profile sets out a list of singular terrorism risks, which when combined into a rules-based targeting system can identify people of interest. Examples of individual risk factors include previous travel to certain countries or the country of origin. The terrorism risk profile is "regularly updated based on shifts in the global terrorism environment and on the analysis of risk as it relates to New Zealand".

24 Where there is a rule match, a New Zealand Customs Service officer will manually assess the passenger's potential risk. This can include inquiries into New Zealand Customs Service's own information holdings or other sources. If a potential terrorism threat is indicated, the officer will inform Immigration New Zealand and the New Zealand Security Intelligence Service and will place an alert in New Zealand Customs Service's database for actioning at the border.

25 Immigration New Zealand and New Zealand Customs Service initiated the Collaborative Passenger Targeting Trial in January 2019. Risk rules for both agencies were run across all international flights arriving into New Zealand to identify passengers meeting specific travel profiles. This is discussed more below.

[122] Immigration New Zealand currently receives Advanced Passenger Processing data on individuals travelling to New Zealand and individuals leaving New Zealand.

[123] Office of the Controller and Auditor-General, footnote 115 above.

[124] Passport and flight information is captured in the Advanced Passenger Information that New Zealand Customs Service are provided when the flight departs.

Arriving at the border

26 Passengers who have been identified by the border agencies as posing a risk through their pre-screening processes will have an alert in New Zealand Customs Service's database. Alerts can also be created by other agencies, such as New Zealand Police.

27 An alert will provide advice to a New Zealand Customs Service officer who processes the person at passport control. This may include instructions as to how the alert should be acted on, such as detaining the person for the attendance of New Zealand Police or referring them to Immigration New Zealand.

28 There are other processes that New Zealand Customs Service use to identify people who may pose a risk to national security as they move through the Customs and Immigration Controlled areas of the airport. These include the following:

a) Checking (either manually at passport control or through the eGates) that there is a match between the person's face and their passport photo to avoid impersonation.

b) Reviewing the passenger's travel documents and arrival card information for declarations made on matters including previous convictions and recent travel history.

c) Asking the passenger additional questions about their travel plans while in New Zealand to ensure the passenger is a legitimate traveller.

d) X-raying or physically checking luggage to identify any prohibited items, such as weapons. If legal thresholds are met, electronic devices such as computers or phones, and arriving and departing travellers may be searched for evidence of offending.

e) Profiling arriving passengers based on their appearance and behaviour.

f) Using detector dogs to identify any prohibited items.

29 A person of interest may be identified, questioned, searched or referred to another agency. A record of the interaction, including any outcome, is added to New Zealand Customs Service's intelligence database, which is "used to inform future analysis, risk assessment and possible interactions".

30 Immigration New Zealand may also interact with a person at the border. This occurs where they have been identified as a risk through Immigration New Zealand's earlier screening processes, through screening arriving passengers based on their appearance and behaviour, or because they have been referred to Immigration New Zealand by another agency.

31 Before 15 March 2019, if an Australian or someone from a visa waiver country was not a known threat, was not on one of the flights subject to Immigration New Zealand's Risk Targeting programme and did not meet a New Zealand Customs targeting rules, the only information available to assess risk was:

a) near real-time Advanced Passenger Processing and Advanced Passenger Information;

b) Passenger Name Record data;

c) what that person declared on their arrival card about their criminal history and whether they had been deported, removed or excluded from any country in the past;

d) what was found through New Zealand Customs Service's screening process on arrival (such as x-rays or detector dogs);

e) verbal questioning; and

f) observations of their behaviour on arrival.

8.4 Goods-related threats

32 New Zealand Customs Service receive advanced information on all goods being imported into or exported from New Zealand excluding mail items. To manage any trade-related hazards or risks, a combination of commodity-based alerts and automated rules-based targeting (that looks at broader risk factors than just the description of the goods or tariff item) is used.

33 Currently, New Zealand Customs Service do not receive advanced information on the 30 million mail items (including letters) entering New Zealand each year. Risk assessments are carried out using a variety of methods. Suspicious mail items may be detained "pending further investigation or seized".

34 For terrorism threats specifically, New Zealand Customs Service have commodity-based alerts for precursor ingredients such as "dangerous dual use chemicals", which can be used to create improvised explosive devices.

8.5 Coordination of the border agencies with the counter-terrorism effort

35 New Zealand Customs Service and Immigration New Zealand are both part of the Integrated Targeting and Operations Centre. This is "a multi-agency border security operations centre in Auckland" established in 2011. It "was designed to bring together multiple agencies in one location to better facilitate the targeting and treatment of risks presented to New Zealand's border".[125] The Integrated Targeting and Operations Centre provides a 24 hour communications hub and operating centre to support agencies as required.[126] The creation of the Integrated Targeting and Operations Centre improved coordination and information sharing between the agencies.[127]

36 Commenting on how the border agencies are strategically situated in the wider national security system, a 2016 review noted that:

> *Overall [national security] sector governance [has] perhaps 'left well alone' the border sector … It had its strategy and knew Government's priorities, its evolutionary systems developments were a work-in-progress and its operational performance overall was satisfactory.*[128]

37 The review noted that the border agencies should continue to focus on how they can align and coordinate their work in order to adapt to possible changes in the threatscape and the implications at the border.

38 New Zealand Customs Service and Immigration New Zealand are looking for similar national security risk indicators. However, as explained above, each agency has its own database and risk assessment processes. In order to better coordinate their efforts and make use of their respective data, the border agencies initiated the Collaborative Passenger Targeting Trial in January 2019. By doing this, 100 percent of passengers on all flights were screened. The results showed that over the 16 week trial period, 20 percent of passengers identified as a risk did not meet the threshold for targeting by a single agency. If the Collaborative Passenger Targeting Trial had not been conducted these passengers would not have been identified before arriving in New Zealand. Collaborative Passenger Targeting is now applied across all flights.

39 The risk rules also have the potential to identify a person of interest much earlier than manual processing, as the first set of information is received up to 72 hours before the flight departs for New Zealand. This allows agencies more time to conduct further checks and act on information.

[125] Simon Murdoch *Review of the Integrated Targeting and Operations Centre* (July 2016).

[126] Simon Murdoch, footnote 125 above.

[127] Office of the Controller and Auditor-General, footnote 115 above.

[128] Simon Murdoch, footnote 125 above.

40 We observed that the border agencies could be better connected with the counter-terrorism effort:

a) It is unclear what guidance and support the border agencies receive from other Public sector agencies such as the Department of the Prime Minister and Cabinet, New Zealand Police and the New Zealand Security Intelligence Service.

b) Neither the New Zealand Security Intelligence Service nor New Zealand Police currently receive information associated with the New Zealand electronic Travel Authority (see 8.8 Developments since 15 March 2019). Nor do they receive the Passenger Name Record data from New Zealand Customs Service. Information sharing is discussed in Part 8, chapter 9.

c) There is no Memorandum of Understanding between New Zealand Customs Service and the New Zealand Security Intelligence Service. In September 2019 the Inspector-General of Intelligence and Security's review of the New Zealand Security Intelligence Service's relationships at the border said there would be value in "documenting clearly the basis and scope for the sharing of intelligence ... and for collaboration on operations".[129] Both agencies are awaiting our report before negotiating a Memorandum of Understanding.

8.6 Identifying risks of right-wing extremism

41 Immigration New Zealand's advice on who may present a risk for terrorism at the border has a strong emphasis on Islamist extremist terrorism indicators. Before 15 March 2019, there was no specific targeting rule in place for screening for extreme right-wing terrorism threats (such as travel history, age or gender).

42 Before 15 March 2019, New Zealand Customs Service's passenger targeting rules and indicators for identifying potential terrorist threats at the border were also primarily targeted at identifying Islamist extremist terrorist threats, including those travelling to and from countries that are considered "high risk for religious extremism". New Zealand Customs Service maintain that they are neither concerned with nor have any information on a traveller's religious beliefs. Instead they focus their efforts on "where the person may have been and what [the] person may have been up to". We scrutinise this claim later in the chapter.

43 In 2013, New Zealand Customs Service added one indicator relating to white supremacy and right-wing extremism to their counter-terrorism profile to assist frontline staff. This was because they had "identified a rising global trend of extreme right-wing attacks" and because of extreme right-wing activity in Australia in 2013. We were told they started working with domestic and international intelligence and security agencies and border partners to "better understand the risk" of right-wing extremism in 2013. We have not been provided with evidence to suggest that much progress was made on this.

[129] Office of the Inspector-General of Intelligence and Security *Report on a review of the New Zealand Security Intelligence Service relationships at the border* (6 September 2019).

44 In 2018, New Zealand Customs Service included indicators of right-wing extremism in their training material for frontline officers. In December 2018, New Zealand Customs Service discussed concerns about right-wing extremism with New Zealand Police and the New Zealand Security Intelligence Service.

45 New Zealand Customs Service told us that they were detecting extreme right-wing individuals but their knowledge of the risk was "not as well developed as for some other threats to the New Zealand border". They told us this was in line with the information available, the priority of other threats and was consistent with the practice of other domestic and international border and intelligence agencies.

8.7 Experiences of Muslim individuals at the border

46 During our engagement with communities, we heard that there is a strongly held belief that there is bias against Muslim individuals at the border. Muslim communities believe that Muslim individuals are stopped and questioned more frequently than non-Muslim individuals.

47 As noted above, New Zealand Customs Service state that they are not concerned with a traveller's religious beliefs and instead focus their efforts on "where the person may have been and what [the] person may have been up to".

48 Given the strong focus on the risk of Islamist extremist terrorism and the way that risk identification rules operate, particularly on travel originating in the Middle East, Muslim individuals are particularly susceptible to being stopped, interviewed and searched at the border. This is understandably regarded as a serious issue by many Muslim individuals and communities we spoke to. They see it as demonstrating a perception amongst officials that Muslim individuals pose particular threats and as being part of a widespread securitisation of Muslim communities.

49 The religion of someone presenting at the border will often be obvious. Passports from some countries explicitly state the passport holder's religious affiliation. Religious affiliation can often be correlated with citizenship of countries that have large religious majorities. Certain surnames are often strongly indicative of religious affiliation. As well, the way a person dresses may also suggest a connection with a particular faith.

50 We acknowledge that the border agencies have put in place some training to enable their staff to act in a culturally safe manner and ensure they understand unconscious bias. However, the experiences of some community members suggest that there is further work to be done to improve staff training in this area.

51 It is also useful for the border agencies to engage with communities to ensure those communities understand the role of the agencies and the reasons for certain operational practices. We heard of good examples of this involving community forums in Auckland in 2018 that were led by the Human Rights Commission and Human Rights Foundation. These forums included officials from the Ministry of Business, Innovation and Employment, New Zealand Customs Service, New Zealand Police and the New Zealand Security Intelligence Service. At these community forums, officials discussed with Muslim communities a range of concerns, including searches conducted at the border, seizure of goods, immigration issues, objectionable material and surveillance. We heard feedback from community and Public sector agency attendees that these forums had been useful. We consider this type of engagement is worth repeating nationwide.

52 We also heard from international practitioners that gathering and publishing data on government interactions broken down by ethnicity (for example, in relation to searches) helps to dispel myths and is useful as it provides accurate information for informed public debate.

8.8 Developments since 15 March 2019

53 Immigration New Zealand's target advice was updated after 15 March 2019. It now refers to right-wing extremism and includes some relevant indicators of right-wing extremist ideology.

54 The New Zealand electronic Travel Authority was introduced on 1 October 2019. Visa waiver travellers now need to complete a New Zealand electronic Travel Authority and have it granted at least 72 hours before they depart for New Zealand. Travellers applying for a New Zealand electronic Travel Authority are currently not required to provide their recent travel history as part of the application process. Nor are they required to declare whether they have travelled to countries designated as high risk.

55 Immigration New Zealand told us that expanding the New Zealand electronic Travel Authority to collect additional information useful for risk targeting would pose "practical issues" and have "cost implications" and create "significant additional compliance burden[s]" for applicants.

56 Australians are exempt from New Zealand electronic Travel Authority requirements. This limits Immigration New Zealand's ability to assess Australian citizens' risk before they arrive in New Zealand.

8.9 Concluding comments

57 Before 15 March 2019, the border agencies' focus on terrorist threats was primarily directed towards identifying Islamist extremism. There was limited focus on right-wing extremism. Since 15 March 2019, the border agencies have been updating their risk identification rules to incorporate more indicators relevant to right-wing extremism.

58 The focus on Islamist extremism and the corresponding way that risk identification rules operated meant that Muslim individuals were commonly stopped, interrogated and searched at the border. This has reduced trust and confidence in the border agencies. This lack of trust signals the need for continued efforts by the border agencies to engage with Muslim communities to explain how their processes operate and reassure them of what is being done to identify right-wing extremist terrorist risks.

59 We do not make recommendations in relation to the border agencies. They make contributions to the counter-terrorism effort that are generally efficient and well-calibrated to what is realistic within the time constraints associated with prompt border processing of people and goods. They have made efforts recently to work more collaboratively to address inefficiencies in the system, for example through the Collaborative Passenger Targeting Trial.

60 There is, of course, scope for improvement. This includes closer integration of the border agencies in the counter-terrorism effort to ensure that the information and expertise they hold can be used in cross-agency counter-terrorism efforts. As well, there is work to be done to improve the experiences of Muslim individuals at the border. We see both issues as able to be addressed within the framework provided by our recommendations on the counter-terrorism effort and social cohesion (see *Part 10: Recommendations*).

Chapter 9: Information sharing

9.1 Overview

1 Our Terms of Reference directed us to make recommendations on:

> 5(1)(a) whether there is any improvement to information sharing and analysis practices by relevant [Public] sector agencies that could have prevented the terrorist attack, or could prevent such terrorist attacks in the future, including, but not limited to, the timeliness, adequacy, effectiveness and coordination of information disclosure, sharing, or matching between [Public] sector agencies.

2 Sharing information is well recognised as fundamental to countering terrorism. Developing an intelligence picture to prevent a terrorist attack usually requires a combination of multiple pieces of information that, individually may be of limited significance, but together, show intent and capability. As the *9/11 Commission Report* noted, no one component of the United States of America's intelligence community held all the relevant information required to "connect the dots"[130] in a way that would have enabled disruption of the 11 September 2001 terrorist attacks. But, had the information been better shared, things may have ended up differently.

3 In this chapter we:

a) discuss the balance between privacy and interagency information sharing;

b) describe previous reviews of components of the national security system related to information sharing;

c) describe legislation, policy and leadership as it relates to information sharing;

d) consider technical and human factors related to information sharing;

e) explain how highly classified information is dealt with;

f) assess the distribution of strategic assessments about terrorism threats in New Zealand; and

g) set out developments that have occurred since 15 March 2019.

4 Our focus has been primarily on the activities relevant to the counter-terrorism effort. Information sharing between New Zealand Police and the New Zealand Security Intelligence Service is discussed in Part 8, chapter 12.

[130] *The 9/11 Commission Report*, footnote 81 above.

9.2 The balance between privacy and interagency information sharing

5 Public sector agencies, including those involved in the counter-terrorism effort, regard personal information as a resource to be used. Their ability to access and use such information is constrained by the Privacy Act 1993 and, more broadly, by the extent to which such access and use is acceptable to the public.

6 The Privacy Act provides for substantial privacy protection by establishing information principles that regulate the collection, use, storage and disclosure of information about individuals and for access by individuals to information that is held about them. These principles are broadly consistent with public expectations about the privacy of personal information.

7 Legislation may provide specifically for official access to, or sharing of, information. We provide some examples later in this chapter.

8 In this context, there is a need for Public sector agencies to explain to politicians and the public what information they need, how they intend to collect it, how widely it will be shared and what safeguards will be put in place to prevent that information being shared more widely than it needs to be. There is also the reality that the public has a right to be sceptical about calls for more intrusion if Public sector agencies have not complied with restrictions or have not fully used mechanisms that they have already been granted by legislation.

9.3 Previous reviews

9 Previous reviews of components of the national security system (see Part 8, chapter 2) have noted the fundamental importance of information sharing, observed weaknesses in current Public sector arrangements and made recommendations to address them.

10 In 2003, the Auditor-General observed there were "few formal processes to co-ordinate information collection and flows more widely across the various Public sector agencies".[131]

11 The 2009 review *A National Security and Intelligence Framework for New Zealand* noted that "information is the currency of the agencies which make up the sector, and it is a truism (in fact a 'no brainer') that this infrastructure should enable information to be stored, accessed, shared and distributed among the right agencies, at the right time, to the right people so that the right use can be made of it".[132]

[131] Office of the Controller and Auditor-General, footnote 8 above at page 52.

[132] Michael Wintringham and Jane Jones, footnote 53 above at page 38.

12 In 2016, the Auditor-General also identified that information flows needed to improve throughout the national security system.[133]

13 Action plans developed to record and address lessons learned from national counter-terrorism exercises[134] and from counter-terrorism operations have also repeatedly identified difficulties with information sharing. For example, issues identified during a 2016 counter-terrorism operation included some sensitive information being disseminated more widely than it should have been and information being shared with international partners but not with the appropriate domestic agencies.

9.4 Legislation, policy and leadership

Privacy Act 1993

14 The information principles under the Privacy Act provide that, generally, personal information should only be used and disclosed for the purpose for which it was collected.[135] There are exceptions that allow use and disclosure where necessary for prevention, detection, investigation, prosecution and punishment of offences, and to prevent or reduce a serious threat to public health or public safety or the life or health of any individual. As well, an intelligence and security agency that holds information collected for a particular purpose may use it for another purpose if that is necessary to enable the agency to perform any of its functions.[136]

15 The Privacy Act enables, on a case-by-case basis, one Public sector agency to seek information held by another. Such requests are assessed against the information principles. The Privacy Act also enables Public sector agencies to enter into approved information sharing agreements.[137] For example, 12 government departments have negotiated an information sharing agreement to enable them to share information and intelligence to reduce gang-related harm to individuals and New Zealand society. We heard that, even with this agreement in place, information sharing for those purposes is sometimes a challenge. There is no equivalent information sharing agreement for counter-terrorism purposes.

Agency-specific legislation

16 The Customs and Excise Act 2018, the Immigration Act 2009 and the Intelligence and Security Act 2017 contain different bespoke information sharing regimes. For example, a direct access agreement enables New Zealand Police to directly create, amend and cancel border alerts in a New Zealand Customs Service database.

---

[133] Office of the Controller and Auditor-General, footnote 52 above.

[134] Counter-terrorism exercises are run through the national exercise programme. The last national-level counter-terrorism exercise before the 15 March 2019 terrorist attack was in 2014. Comprehensive evaluation reports are prepared after each exercise, which include lessons identified and corrective action plans to address those.

[135] Privacy Act 1993 section 6, information privacy principles 10 and 11.

[136] Privacy Act 1993, section 6, information privacy principle 10(2).

[137] Privacy Act 1993, Part 9A.

17 Of the direct access agreements contemplated by the Intelligence and Security Act (see Part 8, chapter 14), only some have been put in place. This suggests that establishing direct access agreements has not been a high priority for some of the relevant Public sector agencies as a collective. Establishing such agreements requires time, effort, cooperation and technical capability to enable the access.

18 New Zealand Customs Service and Immigration New Zealand said that other Public sector agencies were reluctant to share information. They advocate further legislation to specifically allow classes of information sharing. Immigration New Zealand observed that a legislative process would enable public consideration of where the balance should lie between the rights and interests of individuals and the public interest in the effective functioning of the national security system.

National security system leadership and coordination of information sharing

19 In the three years up to March 2019, the Security and Intelligence Board's (Part 8, chapter 3) consideration of information sharing was focused primarily on practical matters such as the development of highly classified information technology systems.

20 The Security and Intelligence Board discussed on a number of occasions the Top Secret information technology system that the Government Communications Security Bureau provides other Public sector agencies. In 2017, the Security and Intelligence Board noted that the Government Communications Security Bureau-led programme was focused on "building the technology platform which will support ... new ways for the [Public] sector to operate".

21 In 2016, the Security and Intelligence Board was told that a counter-terrorism operation identified that "the system overall appears under-prepared to facilitate effectively the sharing of highly sensitive, [compartmented] intelligence to those who need it, when they need it". The Counter-Terrorism Coordination Committee was asked to address this, along with other matters identified in a corrective action plan following that operation. The Counter-Terrorism Coordination Committee referred operational coordination matters such as this to a working group established in 2016 to "address the void" in joining up operationally-focused lines of effort. This work was not completed before 15 March 2019.

22 New Zealand Customs Service raised with the Security and Intelligence Board barriers to information sharing arising through "proposed and current legislative change" in 2016. The Department of the Prime Minister and Cabinet was then to provide the Security and Intelligence Board with a clear and succinct statement of the problems associated with information sharing between Public sector agencies involved in the national security system. This did not happen before 15 March 2019.

23 The Ministry of Health raised with the Security and Intelligence Board challenges of sharing information about individuals of national security concern with frontline staff in 2018. This was addressed by New Zealand Police updating the Ministry of Health on how they had been working at the local level with health sector staff.

24 The Counter-Terrorism Coordination Committee minutes did not record any discussion on information sharing before March 2019. The 2018 risk profile for terrorism (see Part 8, chapter 3) does not include information sharing as one of the national security system's key areas of focus.

9.5 Technical and human factors related to information sharing

25 Information is primarily shared between Public sector agencies by email, rather than through shared databases. Relying on email to share information means there is a significant human factor to whether and what information gets shared.

26 Each Public sector agency involved in the counter-terrorism effort has a separate information technology system. Once information has gone from one Public sector agency to another, it is stored in the receiving agency's internal data management system (assuming it is saved). There is no secure, shared data repository or workspace accessible to multiple Public sector agencies. This is a well-recognised issue for New Zealand's counter-terrorism effort.

9.6 Dealing with highly classified information

What makes something highly classified?

27 The New Zealand Government Protective Security Requirements provide for different national security classifications depending on the level of damage the compromise of that information would pose to the national interest. The Protective Security Requirements are insufficiently detailed to inform day-to-day agency decisions on how to classify information.[138]

28 As a rule of thumb, intelligence collected by the New Zealand Security Intelligence Service using human intelligence methods is classified as Secret or above. Most intelligence collected by the Government Communications Security Bureau is classified as Secret COMINT or above, which requires more stringent handling requirements and potentially limits how many people would see it compared to a Secret report.

[138] Office of the Inspector-General of Intelligence and Security *A review of the New Zealand Security Classification System* (August 2018).

Over-classification of information

29 We have seen instances of over-classification of information. Our impression from the large quantities of information we have handled and our dealings with Public sector agencies is that there is a lack of thoughtfulness about when information needs to be highly classified and a marked tendency to over-classify information. This tendency was recently noted by the Government Inquiry into Operation Burnham.[139] We can illustrate this with two examples relating to our own work.

30 First, the New Zealand Security Intelligence Service's speaking notes for the closed session of Parliament's Intelligence and Security Committee in February 2019 marked the following passage as Secret:

> *We have seen acts of violence in likeminded countries such as Australia, the United States of America, United Kingdom, Canada and Sweden. This includes attacks on groups of people and mosques and the use of weapons, explosives and vehicles. These attacks have caused deaths and serious injuries.*

31 The New Zealand Security Intelligence Service acknowledged that this over-classification was in error. It also told us that this error "did not inhibit effective sharing of such information with domestic partners in other, lowly classified documents".

32 Second, we have also seen information becoming over-classified in misplaced reliance on a clause in the Protective Security Requirements, which provides:

> *A discrete collection of information may be assessed as requiring a higher protective marking where the aggregated information is significantly more valuable, because it reveals new and/or more sensitive information or intelligence than would be apparent from the individual data sources. Examples could include data collections that support intelligence assessments or are designed to show evidence of fraud.*

33 We received a package of Cabinet papers classified Top Secret New Zealand Eyes Only from the Department of the Prime Minister and Cabinet. This reflected the classification of the highest classified document in the package. One of the individual papers that was the subject of the Top Secret New Zealand Eyes Only classification was publicly available on the Department of the Prime Minister and Cabinet's website.

[139] Sir Terence Arnold QC and Sir Geoffrey Palmer QC *Report of the Government Inquiry into Operation Burnham* (17 July 2020) at page 381.

A secure physical space

34 The requirements for a physical space secure enough to hold highly classified information and information technology systems[140] are rigorous, which makes them expensive. There are secure physical spaces in some military facilities. However, a number of Public sector agencies do not have regular access to secure physical spaces in New Zealand outside Auckland, Wellington and Christchurch. This means they do not have easy access to a highly classified information technology system outside of those centres. This makes it difficult to share or work on highly classified information around the country. The development of a strategy to improve access was put on the Department of the Prime Minister and Cabinet's work programme in 2016. We were told that limited progress had been made.

A secure information technology system

35 Once a Public sector agency has a secure physical space, it can then make arrangements to install and use a highly classified information technology system within it. Public sector agencies either have their own highly classified information technology system or pay the Government Communications Security Bureau to run one for them. By the New Zealand Intelligence Community's own assessment in 2018, its customers had been "badly served" by highly classified information technology and changes to it "have been a long time coming".[141] Work continues on developing the Top Secret computer network.

National security cleared people

36 The people who can see highly classified information are first vetted to ensure that they are suitable to access that information. The New Zealand Security Intelligence Service conducts this process at the request of other Public sector agencies and the relevant chief executive then decides whether to grant the clearance on its advice. That Public sector agency then has ongoing obligations relating to its cleared staff to ensure those staff remain suitable to hold a national security clearance, such as watching out for any signs that could suggest that the person is unreliable or susceptible to pressure.

37 The New Zealand Security Intelligence Service has made good progress in recent years decreasing the average time taken to grant a national security clearance. That said, there will always be a delay between a Public sector agency identifying a person who requires a clearance and that person gaining the relevant national security clearance. This needs to be carefully managed within and across Public sector agencies.

[140] These secure physical spaces are referred to as SCIFs (Secure Compartmented Information Facilities) within the national security agencies.

[141] New Zealand Intelligence Community *NZIC Follow-up Self-review* (March 2018).

"Need to know"

38 Once a person has a relevant national security clearance and access to a secure physical space and network, the "need to know" principle applies. This principle means that a person should only share classified information with others who hold the right level of national security clearance *and* who need it to do their work. It also means that the risk associated with sharing information is borne by the person sharing it.

39 We would like to see Public sector agencies who produce classified information thinking hard about what "need to know" means for the information they hold and share for the purposes of the counter-terrorism effort. Our sense is that Public sector agencies are thinking about it in more restrictive terms – as a rationale for not sharing information. But the "need to know" principle is consistent with a positive or enabling mindset, which encourages Public sector agencies to think of what information they hold that other Public sector agencies might benefit from.

40 Deciding whether someone else or another Public sector agency "needs to know" information requires an appreciation of what that person and Public sector agency does in the counter-terrorism effort and how that information might be useful to them. This includes not just the counter-terrorism agencies, but also those involved in the wider counter-terrorism effort, including, local government who have a role to play. We are not confident that this knowledge and perspective is widespread in the relatively insular agencies that produce most highly classified information.

Partner-supplied highly classified information

41 Public sector agencies receive highly classified information from international intelligence and security agencies, principally those in the Five Eyes partnership. As such, New Zealand's standards for dealing with highly classified information are consistent with those of its Five Eyes partners.

42 Where there is a sensitivity, the international partner providing the intelligence requires the New Zealand Public sector agency receiving it to check before sharing it further. We have seen no evidence that this obligation has prevented intelligence relevant to counter-terrorism operations from being shared in a timely fashion within New Zealand.

Improving access to highly classified information

43 One option to make sharing highly classified information easier is to build more secure facilities in different parts of New Zealand, put the highly classified network in those spaces and clear more people in Public sector agencies to be able to use it. Obviously substantial resources would be required to do this. We were told that the New Zealand Security Intelligence Service intends to advocate for more Public sector agencies to have facilities and information technology systems that can store and send classified intelligence and more staff cleared at appropriate levels, especially for New Zealand Police and particularly in the South Island.

44 We heard that other countries have built greater numbers of secure facilities and cleared more people to enable intelligence and security and law enforcement agencies to work more closely together.

2018 Inspector-General of Intelligence and Security report

45 In 2018, the Inspector-General of Intelligence and Security undertook a review of the New Zealand security classification system to improve security, reduce costs and increase transparency. The report *A review of the New Zealand Security Classification System* recommended several areas for improvement.[142] We support the following recommendations:

a) Add [classification] principles that:

   i) no information may remain classified indefinitely; and

   ii) if there is any significant doubt about the appropriate level of classification, it is to be classified at the lower level.

b) Revise agency classification guides, ensuring they supplement not repeat primary classification guidance, using agency-specific examples. Test revised guides with staff.

c) Adopt a topic-based approach to systematic declassification of historic classified records, supervised by a multi-agency group. Consult the public, experts and Archives New Zealand on priorities for review.

d) Develop a training programme to accompany classification reform. Specify the requirements for ongoing training in classification with more particularity. Extend the requirement for refresher training beyond the holders of security clearances. Require agencies to track their compliance with training requirements.

e) Task a coordinating agency with consulting agencies on the feasibility of establishing basic ongoing measures of classified data stocks and flows. Compile this information with agency measures of their classification review activity and their compliance with training requirements. Use this information to start building a set of basic indicators of classification system function and performance.

[142] Office of the Inspector-General of Intelligence and Security, footnote 138 above.

9.7 Dissemination of strategic assessments about terrorism threats in New Zealand

46 Strategic assessments about terrorism threats in New Zealand are written to be widely shared and their volume is such – fewer than ten a year – that there should be no concerns about overloading other Public sector agencies with unwanted information. Apart from potential complications from classification, there are no legislative, policy or technical reasons of which we are aware that might limit their dissemination. How widely they were shared provides a rough indication – or a place to start – as to the state of information sharing across the counter-terrorism effort.

47 Strategic assessments produced by the Combined Threat Assessment Group, the National Assessments Bureau, New Zealand Police and the New Zealand Security Intelligence Service were distributed to the Public sector agencies on the Security and Intelligence Board with a few additions (Part 8, chapter 4). Other than New Zealand Police assessments, these were generally classified Secret, hindering their dissemination within Public sector agencies. Restricted versions of some reports were produced. These contained less detailed but still valuable information. Although they had a lower classification, they were not necessarily disseminated more widely.

48 Several ministers were routinely provided with the National Assessments Bureau assessments, but the New Zealand Security Intelligence Service and the Combined Threat Assessment Group assessments on the terrorism threat in New Zealand are not typically shared with ministers other than the Minister Responsible for the New Zealand Security Intelligence Service.

49 Ministers on the Cabinet External Relations and Security Committee received strategic assessments in 2012, 2016 and 2018 when approving the National Intelligence Priorities and National Security and Intelligence Priorities (Part 8, chapter 3). These included assessments about terrorism threats in New Zealand.

50 Members of the Intelligence and Security Committee of Parliament are not provided with assessments of terrorism threats in New Zealand except as reflected in the annual reports or statements of intent of the New Zealand Security Intelligence Service or the oral reports of the Director-General of Security.

51 The national security system involves wider groups of Public sector agencies, local government and civil society than those on the distribution list for assessment products on terrorism threats in New Zealand. Those agencies and groups require information to be able to inform their own plans and activity. An example is Civil Defence and Emergency Management groups, which are required to identify, assess and manage all relevant hazards and risks.[143] The statutory definition of "emergency" is not limited to natural hazards,[144] which means these groups are required to develop and implement Civil Defence Emergency Management plans for the risk from terrorism.[145] Most of these plans assess the threat and risk from terrorism. Nothing we saw indicates that these plans were consistently informed by the Combined Threat Assessment Group assessments or the terrorism risk profile in the National Risk Register (see Part 8, chapter 3).

9.8 Developments since 15 March 2019

52 The dissemination of the Combined Threat Assessment Group New Zealand threat assessments remained limited. Shortly after the 15 March 2019 terrorist attack, only some of the 36 agencies who should have been briefed on the increased threat level and the actions they should take were briefed. This was identified as a problem in a paper considered by the Counter-Terrorism Coordination Committee regarding agency responses to a change in the national domestic terrorism threat level.

53 In June 2019, the Counter-Terrorism Coordination Committee agreed that information access and sharing were vital to understanding the threat. It suggested removing legislative barriers, leveraging open-source intelligence capability, developing online platforms for agencies to collaborate and enhancing information sharing mechanisms between Public sector agencies and selected private organisations. We understand from the New Zealand Security Intelligence Service, which is leading this work, that its focus is on the acquisition and analysis of data to inform discovery efforts (Part 8, chapter 10).

54 The December 2019 Combined Threat Assessment Group assessment of the New Zealand terrorism threatscape was classified Restricted and disseminated to a wider group than previous assessments. This document shows that assessments can be informed by analysts' access to highly classified information but need not reference it. This provided the opportunity for a wider readership, but it could have been usefully disseminated even more widely.

[143] Civil Defence Emergency Management Act 2002, section 17(1)(a).

[144] Civil Defence Emergency Management Act 2002, section 4. "Emergency" includes a situation that "is the result of any happening, whether natural or otherwise, including without limitation, any explosion, earthquake, eruption, tsunami, land movement, flood, storm, tornado, cyclone, serious fire, leakage or spillage of any dangerous gas or substance, technological failure, infestation, plague, epidemic, failure of or disruption to an emergency service or a lifeline utility, or actual or imminent attack or warlike act".

[145] Civil Defence Emergency Management Act 2002, section 17(1)(i).

9.9 Concluding comments

55 In New Zealand's counter-terrorism effort, sharing of information between Public sector agencies is critical to the effectiveness of the system as a whole. This chapter has identified several issues in relation to information sharing practices.

Agencies do not take full advantage of current legislation for information sharing

56 Relevant Public sector agencies have not been fully using current legislation to share information as systematically and widely as they might. For example, the Intelligence and Security Act permits direct access agreements to be established between intelligence and security agencies and other specified Public sector agencies, but only some have been agreed (see Part 8, chapter 14). Our sense is that Public sector agencies are not prioritising this work.

Altering practices regarding highly classified information

57 The more highly classified a document, the fewer people can see it. The main barriers to sharing highly classified information relate to human decisions and attitudes. System-wide efforts to improve sharing of highly classified information have been inconsistent. The "need to know" principle appears to be applied as a rationale for not sharing information rather than as an opportunity to think through whose work could be better enabled by access to it. Public sector agencies tend to over-classify information. Public sector agencies could make more effort to produce information at lower classifications either through ensuring documents are correctly classified at the lowest appropriate level or producing different versions of the information.

Sharing strategic assessments – practices need to change

58 Strategic assessments about terrorism threats in New Zealand are the culmination of a great deal of investment. They should present the most authoritative and complete picture of the threatscape possible. Wherever possible, they should be classified at a level that permits distribution and enables them to best inform government decisions and activity.

Information sharing must be considered in a whole-of-system way

59 No one Public sector agency holds all of the finished intelligence or information produced by all of the Public sector agencies involved in the counter-terrorism effort. This makes it harder to connect the dots and increases the risk that something could be missed. To ensure that there is improved information sharing among Public sector agencies and other key stakeholders, it should be considered in a whole-of-system way.

60 While there have been efforts to improve secure information technology, we have not seen a coordinated effort led by the Department of the Prime Minister and Cabinet and the Security and Intelligence Board to focus attention on information sharing and to overcome barriers to sharing highly classified information with all the agencies whose work would benefit from receiving it.

Chapter 10: Target discovery

10.1 Overview

1 The terrorist attack on 15 March 2019 was carried out by an individual whose violent intentions were previously unknown to New Zealand's Public sector agencies (see *Part 6: What Public sector agencies knew about the terrorist)*. He was motivated by an ideology (right-wing extremism) that had not been the subject of deliberate intelligence collection or analysis by the Public sector agencies involved in the counter-terrorism effort until mid-2018. So, at the time of the terrorist attack, these agencies had a limited understanding of right-wing extremism and the terrorism threat and risk it presented to New Zealand

2 In this chapter we:

a) explain what target discovery is;

b) discuss how strategic intelligence assessments can guide target discovery;

c) assess the New Zealand Security Intelligence Service's target discovery efforts;

d) assess the Government Communications Security Bureau's target discovery efforts; and

e) discuss whether the authorising environment enables the intelligence and security agencies to undertake target discovery.

10.2 What is target discovery?

3 When we talk about target discovery, we mean both:

a) identifying previously unknown terrorism threats (people, groups or networks) motivated by a well-understood, *known ideology;* and

b) identifying previously unknown terrorism threats (people, groups or networks) motivated by an *unknown ideology* – one that is not well understood. This process necessarily includes strategic intelligence assessment (including horizon scanning) to identify and better understand the new ideology.

4 Target discovery is a proactive, exploratory effort to generate and investigate leads. Investigation of these leads can help to identify previously unknown, specific subjects of interest. This helps to gain a deeper understanding of not only the threat, but also the risk. The objective is to enable Reduction and Readiness activities for that threat before it crystallises.

5 Target discovery may involve analysing data and information already collected and stored by Public sector agencies (or international partners). It may also entail sourcing new data and information. This could be through intelligence gathering online, collection of large data sets or observation of public events. The data collected can then be used to test hypotheses about existing or emerging trends.

6 A useful contrast to target discovery is the "classical model" of investigation (see Part 8, chapter 5). The classical model begins with lead information, which can come from a range of domestic or international sources. The classical model "is not well configured for discovery of new leads and, where it does, these tend to be within the same [ideological] area". In this sense it is geared towards responding to known threats.[146]

10.3 Strategic intelligence assessments

7 Strategic intelligence assessments scan the global terrorism environment for emerging threats and assess these for potential impact. International intelligence and security agencies use strategic intelligence assessments to guide decisions on where to focus their target discovery resources.

8 In the years before 15 March 2019, the National Assessments Bureau and the Combined Threat Assessment Group produced limited numbers of strategic intelligence assessments on the domestic terrorism threatscape (see Part 8, chapter 4).

10.4 The New Zealand Security Intelligence Service's target discovery efforts

9 In July 2018, the Counter-Terrorism Unit produced a *Counter-Terrorism Discovery Strategy* "to establish a baseline picture of emerging terrorism threats to New Zealand … with the objective of understanding the New Zealand baseline picture based on our current holdings, the development of information requirements and outreach opportunities".

10 Part of this work was the baselining project on right-wing extremism in New Zealand, which we have discussed in Part 8, chapter 5. In the course of this project, the New Zealand Security Intelligence Service's online operations team also began to look at right-wing forums.[147] The project generated ten leads relevant to right-wing extremism, some of which remained open at 15 March 2019.

11 The 2019 Arotake Review described the *Counter-Terrorism Discovery Strategy* as "basic but sufficient", noting that it provided a framework for proposing, authorising and recording discovery projects.[148]

12 Since 15 March 2019, the New Zealand Security Intelligence Service has refreshed its *Counter-Terrorism Discovery Strategy*. It has also dedicated specific resources to a counter-terrorism discovery team. Staff are seconded into that team from other teams on a rotating basis.

[146] New Zealand Security Intelligence Service, footnote 57 above at page 88.

[147] New Zealand Security Intelligence Service, footnote 57 above at page 96.

[148] New Zealand Security Intelligence Service, footnote 57 above at page 90.

13 In addition, the New Zealand Security Intelligence Service has established a discovery collaboration group that meets monthly. That group includes discovery investigators and managers, as well as information exploitation analysts, telecommunications experts, strategic analysts and targeting and other relevant officers from within the New Zealand Security Intelligence Service. Counter-terrorism analysts from the Government Communications Security Bureau regularly participate in the discovery collaboration group, and intend to continue to do so.

10.5 The Government Communications Security Bureau's target discovery efforts

14 The Government Communications Security Bureau acts when tasked by the New Zealand Security Intelligence Service – its primary customer – and only when given a lead (see Part 8, chapter 7). The result of this position has been that, at least since 2016, the organisation has carried out limited domestic counter-terrorism target discovery. It has largely been involved in collecting intelligence on known terrorism risks motivated by a known ideology rather than discovering previously unknown terrorism risks motivated by an unknown ideology. The Government Communications Security Bureau's activities in relation to the domestic counter-terrorism effort have been shaped – inevitably – by the focus of the New Zealand Security Intelligence Service on known Islamist extremist risks.

15 In June 2019 the Government Communications Security Bureau staff participated in a target discovery week with the New Zealand Security Intelligence Service to "identify a framework to better inform joint discovery projects". The team proposed the establishment of a shared database combining lists of known behaviours and indicators of violent extremism and identifiers of those behaviours. The aim was to assist in identifying previously unknown terrorism risks motivated by an unknown ideology.

10.6 Does the authorising environment enable target discovery?

16 Target discovery activities that do not require a warrant can include:

a) collecting publicly available information;

b) analysis of some internal holdings;

c) some information requests to domestic or international partner agencies;

d) observing public events;

e) engaging with groups of interest; or

f) directly accessing other agencies' datasets under agreement.

17 Under section 58 of the Intelligence and Security Act 2017 an intelligence warrant may be sought on the basis that it will enable an intelligence and security agency to carry out an activity that "identifies, enables the assessment of, or protects against any" of a number of harms which include terrorism. This contemplates target discovery.

18 There are aspects of target discovery that may be problematic under the Intelligence and Security Act as it is likely to:

a) involve activity directed towards groups of people of whom, individually, comparatively few (and perhaps none) will prove to be of national security interest and may involve the collection of large amounts of information of which comparatively little (and perhaps none) will turn out to be of intelligence value. This means that there may be issues whether such activity can be justified as necessary and proportionate; and

b) include activity directed towards groups of people whose thinking is on the same ideological spectrum as those of terrorists but who, at the time the activity commences, are not known to have expressed support for violence. Such activity is at risk of being seen to contravene section 19 of the Intelligence and Security Act, which provides that the exercise of the right to freedom of expression does not justify activity by an intelligence and security agency.

19 In Part 8, chapter 14 we discuss in more detail how these issues may be addressed under the Intelligence and Security Act and do so under the following headings:

a) Bulk collection and acquisition of data.

b) Specificity requirements for warrants.

c) The application of the necessary and proportionate test to actions that do not require a warrant.

d) The relationships between the Inspector-General of Intelligence and Security and the intelligence and security agencies.

e) The possible impact of section 19 of the Intelligence and Security Act in limiting target discovery.

20 Since 15 March 2019, the agencies are increasingly pursuing intelligence warrants for the purposes of target discovery. An example is an application to renew a class-based intelligence warrant in October 2019 that picks up on the language of discovery in the Intelligence and Security Act (section 58). It would allow the agency to gather intelligence about New Zealanders who engage in terrorist acts or with links to those who are, or entities whose behaviour indicates they may be of intelligence interest about terrorism or violent extremism. The proposed warrant would authorise the agency to conduct various collection activities to assess whether those covered by the warrant engage in terrorist acts or otherwise have information about threats of terrorism or violent extremism.

21 As we discuss in Part 8, chapter 14 there remain uncertainties as to the extent to which target discovery is appropriate under the Intelligence and Security Act.

10.7 Concluding comments

22 Before 15 March 2019, the intelligence and security agencies were engaging in only limited target discovery activity. In part, this was due to resource constraints. The New Zealand Security Intelligence Service was focused on the presenting threat of Islamist extremist terrorism. The classical model of investigation used by the New Zealand Security Intelligence Service was better suited to identifying new individuals and groups with Islamist extremist ideology than identifying new threats outside that well-understood ideology.

23 The New Zealand Security Intelligence Service had identified understanding emerging threats as a priority in its 2016 *10-Year Operational Strategy*. The baselining project on domestic right-wing extremism in New Zealand, which began in 2018, generated several new leads.

24 After 15 March 2019, the intelligence and security agencies appear to have significantly increased their target discovery activity, and dedicated resources to support this work. We discuss the legal constraints in Part 8, chapter 14.

Chapter 11: Online capacity and capability

11.1 Overview

1 The terrorist attack on 15 March 2019 highlighted the importance of the online capabilities and activities of the Public sector agencies with counter-terrorism operational responsibilities.

2 A significant element of New Zealand's counter-terrorism effort needs to be online because the internet is widely recognised as a key platform for terrorist radicalisation and recruitment. Our report shows that it was on the internet that the individual developed, at least in part, his extreme right-wing views and, to some extent, shared them. He also used the internet to obtain operational guidance, research firearms capability and undertake some of his reconnaissance. It was also the internet that enabled him to reach a worldwide audience with his GoPro livestream and manifesto (see *Part 4: The terrorist*).

3 This chapter:

a) describes the two types of online intelligence collection;

b) explains the challenges that online intelligence collection presents;

c) outlines developments since 15 March 2019; and

d) assesses the extent to which there is there is a whole-of-system approach to online capabilities in the counter-terrorism effort.

11.2 Two types of online intelligence collection

4 There are two distinct types of online intelligence collection.[149]

5 First, collection through open-source research and monitoring. This involves searching areas on the internet that do not require difficult-to-obtain privileges to gain access. It may involve access to platforms by subscription.

6 Second, collection through covert operations. These may involve the use of automated tools to "scrape" or extract data from websites or the development of an assumed identity (in accordance with Part 3 of the Intelligence and Security Act 2017). An assumed identity can be used to support an online persona and gain access to closed online forums.

7 A key distinction between these two types of online intelligence collection lies in the intention of the originator of the information.[150] Generally speaking, open-source research and monitoring seeks to collect information that the originator was not concerned to keep hidden. In contrast, covert operations collect information that the originator did not wish to be available to people other than an intended audience, especially not to intelligence and security and law enforcement agencies.

[149] Government Communications Security Bureau, footnote 102 above.

[150] Government Communications Security Bureau, footnote 102 above.

8 More people are spending significant proportions of their lives online, more activities and interactions are being conducted online and news and views are being disseminated and accessed online. The counter-terrorism effort needs online capabilities. This is particularly so because:

a) the internet enables and facilitates contact between, and funding of, extremists globally;

b) radicalisation can be driven by both physical world and online influences, and there can be significant cross-over between groups and individuals operating in the real world and online;

c) online material can reveal the capabilities that might be utilised by someone mobilising to violence;

d) the volume of extremist material online and the ease with which it can be accessed and shared means that extremists are increasingly operating online. Their activities inspire and radicalise others with whom they could not otherwise as easily have contact; and

e) online intelligence collection capability may somewhat offset the collection (and consequential intelligence) losses resulting from encryption.

11.3 The challenges that online intelligence collection presents

9 There are several challenges for intelligence and security and law enforcement agencies in monitoring and countering extremism online. These include:

a) the size and complexity of the internet;

b) encryption;

c) anonymisation and the use of false names;

d) the rapid rate of change in the online world; and

e) the difficulty of identifying the boundary between free speech and harmful extremism.

10 The diversity of data is another challenge as data may need to be "cleaned" before it can be used. Cleaning is the process of removing or updating data that is incomplete, incorrect, improperly formatted, duplicated or irrelevant. There are also challenges in storing, managing and interrogating what may be large volumes of data in order to produce usable intelligence.

Online capabilities stocktake

11 Before 15 March 2019 the Public sector agencies involved in the counter-terrorism effort had limited online capabilities and capacity for counter-terrorism purposes.

12 In mid-2018 the Specialist Coordinator (see Part 8, chapter 3) directed a National Assessments Bureau analyst to conduct a stocktake of Public sector agencies' online activity to counter extremism. Initially, the stocktake was intended to support the Counter-Terrorism Coordination Committee to consider whether a more detailed gap analysis and consideration of potential additional measures was required.

13 The stocktake reviewed the Public sector agencies' activity in relation to online extremist activity. It found that while there were a number of relevant work streams underway, there was no common approach. The extent to which coordination was occurring was questioned. The stocktake was provided to the Counter-Terrorism Coordination Committee. It was asked to consider whether:

a) additional operational or strategic coordination was needed;

b) there was merit in clarifying the approach to online extremism; and

c) additional investment was needed.

14 The Counter-Terrorism Coordination Committee decided that the Specialist Coordinator and the National Assessments Bureau analyst would meet with agencies individually to discuss their views directly. We are not aware of any of the matters proposed for consideration by the Counter-Terrorism Coordination Committee being progressed further before 15 March 2019. Nor was the stocktake considered by the Security and Intelligence Board.

New Zealand Security Intelligence Service

15 The New Zealand Security Intelligence Service's development of covert online capability and strengthening of its open-source collection capability were two of six areas for growth identified in its 2018 *Performance Improvement Framework* self-review. This self-review followed up on the 2014 *Performance Improvement Framework* review of the New Zealand Intelligence Community.[151]

16 The 2019 Arotake Review described these capabilities, as at 15 March 2019, as "fragile".[152] There was one full-time analyst working on open source research and monitoring, with a further officer available to bolster capacity when necessary. Security constraints meant that other officers had limited suitable internet access, which was described in the review as "inadequate to replicate the techniques of the open-source team".[153]

[151] New Zealand Security Intelligence Service *Performance Improvement Framework: Follow-up Self Review of the New Zealand Security Intelligence Service Te Pa Whakamarumaru* (March 2018) at page 24; *Performance Improvement Framework*, footnote 42 above.

[152] New Zealand Security Intelligence Service, footnote 57 above at page 127.

[153] New Zealand Security Intelligence Service, footnote 57 above at page 62.

17 In early 2018, the covert team consisted of one full-time equivalent made up of two part-time officers. Both officers left in mid-2018. While new staff were recruited, they required training and on-the-job experience before they could confidently undertake their role as required.[154]

18 The 2019 Arotake Review recommended that consideration be given to increasing resources to achieve the capacity and capability required to maintain ongoing operations and expand into additional thematic areas. It noted that the nature of online operations often requires high levels of staff availability (for example, staff may need to be interacting online outside of normal working hours), along with judgement and a high level of understanding of the digital environment.[155] The 2019 Arotake Review concluded that the New Zealand Security Intelligence Service lacked capacity to fulfil many of its open-source requirements, but did not consider a substantial increase in the open-source team was required. Rather, a better solution was for more suitable equipment to be made available to other teams (including investigators). This would enable more open-source inquiries to be carried out elsewhere in the organisation and free up the specialists to undertake more complex inquiries.[156]

19 The New Zealand Security Intelligence Service now has a similar proportion of resources dedicated to online human intelligence activity as its international partners. But a senior manager at the New Zealand Security Intelligence Service accepted this had not happened early enough. Online capability and capacity were not included in the funding from the Strategic Capability and Resourcing Review. To build them has required the diversion of resources from elsewhere.

Government Communications Security Bureau

20 The Government Communications Security Bureau also has a relatively small internet operations team with open-source capabilities, which it describes as "a small focus area but a growing one". The team uses specialised tools and tradecraft and has been careful to ensure their work complements that of the New Zealand Security Intelligence Service. It provides technical tradecraft advice to other agencies. For example, it provides technical support and advice to the New Zealand Security Intelligence Service's online operations team. Its standing work programme does not include counter-terrorism activities.

New Zealand Police

21 While New Zealand Police undertook open-source, online collection of intelligence, we were told by former and current officials that there had been very little in the way of training. There were few tools to assist New Zealand Police intelligence analysts to exploit social media. They considered that there are significant opportunities to improve New Zealand Police's intelligence collection through these means.

[154] New Zealand Security Intelligence Service, footnote 57 above at page 63.

[155] New Zealand Security Intelligence Service, footnote 57 above at page 127.

[156] New Zealand Security Intelligence Service, footnote 57 above at page 61.

Department of Internal Affairs

22 The Department of Internal Affairs' Digital Safety Directorate is the lead agency in combatting objectionable material under the Films, Videos, Publications Classification Act. See *Part 9: Social cohesion and embracing diversity* for more on the Department of Internal Affairs' role.

11.4 Developments since 15 March 2019

23 We have seen Public sector agencies moving to increase online capability and capacity since 15 March 2019.

24 We understand that work is underway that will eventually provide adequate and more broadly available internet access across the New Zealand Security Intelligence Service. Some of the additional funding received in Budget 2019 was allocated to this.[157]

25 The New Zealand Security Intelligence Service told us that its online operations capability is growing. The Online Operations team is to recruit some additional people. As noted the New Zealand Security Intelligence Service now has a similar proportion of resources dedicated to online human intelligence activity as its international partners.

26 New Zealand Police have now established a dedicated open-source team. They have purchased a specialised tool that enables rapid extraction of information from the internet, including the dark web. The tool identifies connections between people, events and locations online. There has recently been a secondment of an experienced officer to the New Zealand Police to assist with the establishment of its open-source team.

27 New Zealand Police are also trying to build capability within the National Security Investigation Team to undertake online operations, including by sending investigators to training courses run by the Australia New Zealand Counter-Terrorism Committee. They are seeking additional funding to build their capability and capacity to respond to national security concerns, including their online scanning capability and online operations.

28 In October 2019, the Prime Minister, Rt Hon Jacinda Ardern, and the Minister of Internal Affairs, Hon Tracey Martin, announced that the Department of Internal Affairs would receive an additional $17 million over four years. This funding was in response to the 15 March 2019 terrorist attack and subsequent developments on the Christchurch Call. The new funding will boost the Department of Internal Affairs' investigative, forensic, intelligence and prevention work in relation to violent extremism and terrorist content online.

[157] New Zealand Security Intelligence Service, footnote 57 above at page 127.

29 On 2 June 2020, Cabinet agreed in principle to New Zealand's accession to the Council of Europe Convention on Cybercrime (the Budapest Convention) and to consult publicly to inform a further Cabinet decision. The Convention is the first, and currently only, treaty specifically seeking to address internet and computer crime. Accession to the Budapest Convention would assist New Zealand to initiate or strengthen relationships with member countries by signalling New Zealand's commitment to multilateral efforts to combat cybercrime. By providing a standardised framework for cooperation through aligned national cybercrime laws, the Convention facilitates cooperation on criminal investigations of cybercrime and wider crimes involving electronic evidence, for example private social media communications relating to a crime and stored in the cloud by companies such as Facebook.[158]

11.5 A whole-of-system perspective

30 There are now at least four different Public sector agencies (that is the Department of Internal Affairs, the Government Communications Security Bureau, New Zealand Police and the New Zealand Security Intelligence Service) undertaking online activities in relation to extremist activity online. Each has a different mandate. Different mandates might translate to differing objectives at an operational level. For example, Public sector agencies with an enforcement function in relation to offensive material online may seek to promptly shut down offending online accounts. On the other hand, intelligence and security agencies may seek to prolong online engagement with those expressing extremist and violent views in order to collect information on their intent and capability. While it is important to recognise the different mandates, this should not prevent the coordination of building capability to undertake online activities. There is a need to coordinate across these mandates to avoid duplication of effort, ensure efficient use of resources and to remain alert to any potential conflict of objectives.

31 While we have been largely concerned with coordination of capability and capacity building across Public sector agencies in this chapter, coordination of operational activity will be equally important in the future.

32 The recent expansion of capability and capacity to operate online in relation to terrorism and violent extremism has occurred without centralised coordination or consideration of the issues from a whole-of-system perspective.

[158] Department of the Prime Minister and Cabinet and Ministry of Justice *Budapest Convention on Cybercrime: Approval to Initiate the First Stage Towards Accession* (2020) https://dpmc.govt.nz/sites/default/files/2020-09/SWC-20-SUB-0053-budapest-convention-on-cybercrime.pdf.

33 To the extent there is leadership and coordination in this area, it is not being driven by the Department of the Prime Minister and Cabinet as lead agency and coordinator of the national security system. New Zealand Police and the New Zealand Security Intelligence Service have both expressed a desire for agencies to work collaboratively on how extremism is tackled online and in the development of shared complementary capabilities. Both have proposed models for multi-agency collaboration, including co-location. As well, the Government Communications Security Bureau has made efforts to work with other agencies to avoid duplication of effort. This is a good example of agencies within a small system working together to get the best return for New Zealand from limited resources.

34 Greater central oversight and coordination of resourcing and work across the different agencies is critical. Any further developments or growth should be supported by policy work. This will provide clarity on the roles and objectives of agencies and the legal parameters within which they operate. Operational protocols will be required to prevent conflicts.

11.6 Concluding comments

35 Our review of the online capabilities in the counter-terrorism effort has shown that the significance of online activity has been apparent for some time. Before 15 March 2019, limited resource was dedicated to developing adequate online capability across the relevant Public sector agencies. This was in part a consequence of the absence of a horizon scanning function (see Part 8, chapter 4).

36 There are commonalities of effort between New Zealand Police and the New Zealand Security Intelligence Service. The Department of Internal Affairs (in relation to objectionable material) and the Government Communications Security Bureau have complementary roles and capabilities. Coordination of the development of online capability is therefore sensible. Such coordination was not evident in relation to new funding approved for the Department of Internal Affairs to develop online capability in Budget 2019.

37 Since 15 March 2019, there has been little system-wide leadership and cross-agency coordination in developing policy and building and harnessing capability. Coordinated development and deployment of online capability are critical. When that capability is developed, leadership and coordination of operational activity will remain a key issue. In addition, it will also be important not only to accede to the Budapest Convention but also develop a clear and shared understanding between Public sector agencies of the legal and policy settings, and the social licence for online intelligence collection.

Chapter 12: Relationship between New Zealand Police and the New Zealand Security Intelligence Service

12.1 Overview

1 In this chapter we look at the relationship between the counter-terrorism agencies – New Zealand Police (see Part 8, chapter 6) and the New Zealand Security Intelligence Service (see Part 8, chapter 5). The quality of the counter-terrorism agencies' relationship is fundamental to New Zealand's counter-terrorism efforts.

2 We heard from international experts that an effective relationship between New Zealand Police and the New Zealand Security Intelligence Service is critical to a successful counter-terrorism effort. They advised us to look closely at it.

3 In this chapter we:

a) describe the different functions, resources and powers of the counter-terrorism agencies;

b) examine the state of the relationship between the counter-terrorism agencies;

c) discuss positive aspects of the relationship before 15 March 2019; and

d) describe the challenges that remain.

12.2 The different functions, resources and powers of the counter-terrorism agencies

4 The counter-terrorism agencies have complementary functions, powers and capabilities. Broadly, in the counter-terrorism effort, the New Zealand Security Intelligence Service's role is to identify potential terrorists and then collect and report intelligence on them. Its functions specifically do not include law enforcement. New Zealand Police have national security intelligence functions but their primary counter-terrorism role is to prevent terrorist activities, and – where they have occurred – to respond, investigate and prosecute the offenders.

5 Reflecting their different functions, the two agencies must meet different thresholds to seek warrants to gather further information on potential terrorists. For a New Zealand Police search warrant to be issued, there must be reasonable grounds to suspect a criminal offence punishable by imprisonment and to believe that the search will find evidential material related to the offence.[159] Similar grounds must be made out for a surveillance device warrant.[160] For the New Zealand Security Intelligence Service to obtain an intelligence warrant, it must show that that the activity it wishes to carry out (for instance search or surveillance) would contribute to the protection of national security by identifying, enabling the assessment of or protecting against terrorism or violent extremism.[161] It must also show that the proposed activity is necessary and proportionate for the purposes for which

[159] Search and Surveillance Act 2012, section 6.

[160] Search and Surveillance Act 2012, section 51.

[161] Intelligence and Security Act 2017, section 58.

the warrant is sought.[162] Intelligence warrants can therefore be more forward looking and directed at understanding amorphous and often unknown targets, compared to New Zealand Police warrants, which are used for known targets and past and current offending.

6 It makes sense for the counter-terrorism agencies to work closely together to pool their limited capacity and capability. Because the intelligence and security agencies in New Zealand do not have law enforcement powers, they need an enforcement agency like New Zealand Police to take action against potential terrorist threats. The intelligence and security agencies also benefit from the broad networks New Zealand Police have and the information they obtain from this. Conversely, the intelligence and security agencies can undertake activities that New Zealand Police cannot, and New Zealand Police often need the intelligence collected through these activities to fully understand the risks posed by subjects of interest.

7 Both New Zealand Police and the New Zealand Security Intelligence Service can and do collect information and produce intelligence on terrorism threats in New Zealand. New Zealand Police's presence throughout New Zealand and broad range of activities and connections in communities provide them with an enormous amount of information. Both have international relationships that provide them with valuable additional sources of information.

8 It is not an easy relationship, as tensions between the functions and organisational cultures of the two types of agency require constant management. International practitioners advised us that a great deal of effort is required to ensure collaboration and communications between counter-terrorism agencies. They described that as a difficult, often uncomfortable, process. They offered some consistent advice about practices that can support these efforts:

a) Co-location, which builds trust and assists staff within each agency to understand and appreciate both agencies' respective roles and responsibilities, and how to best use their respective skills and experience.

b) A joint leads process, which provides for the agencies to jointly assess the risk associated with lead information and then determine what level and type of resources each allocates to assess and manage that risk. It also supports better information sharing by ensuring agencies' respective information sources are brought together. For example, an international expert told us that in the United Kingdom, over half of the Security Service's leads come from the police and having a joint leads process ensures this information is promptly shared.

[162] Intelligence and Security Act 2017, section 61.

c) A joint operations protocol, which provides a clear framework for decision-making during an investigation, including which agency leads. It ensures that respective roles and responsibilities are clear and that each agency can contribute its specialist skills and information (for example, in intelligence and security agency-led investigations, police are involved early so intelligence collected can be used evidentially). It can also provide guidance on whether to extend an operation or bring it to a close, which can mitigate tensions between the agencies.

d) Joint training and secondments, which help the agencies to understand each other's capabilities and constraints.

9 International practitioners also told us that the importance of the relationship means that agencies leading the counter-terrorism effort should monitor the progress of the relationship and support the intelligence and law enforcement agencies to work in a more integrated way.

12.3 The state of the relationship between the counter-terrorism agencies

10 A clear message we received during our inquiry was that, as recently as 2015, the relationship between the two counter-terrorism agencies was not functioning effectively. Internal New Zealand Police reviews conducted in 2011 and 2015 found that the varying expectations, attitudes and organisational cultures between the two agencies inhibited collaboration.[163] There was no formal framework to guide and facilitate cooperation and coordination between the two agencies, which "resulted in restricted access to crucial intelligence and placed operation[al] relationships and effectiveness under strain".[164]

11 We were advised that, around 2015, there were high levels of mutual mistrust between the agencies. There were indications that the New Zealand Security Intelligence Service would not share information at that time with New Zealand Police staff, whom they perceived could not be trusted to securely hold highly classified information. Equally, we heard from some New Zealand Police staff that there had been a high level of resistance from New Zealand Security Intelligence Service staff to sharing information with them, and that they were not receiving information they needed to know.

[163] New Zealand Police (2011), footnote 95 above; New Zealand Police (2015), footnote 95 above.

[164] New Zealand Police (2015), footnote 95 above.

12 The relationship has improved since then. Rebecca Kitteridge, the Director-General of Security, and Mike Bush, former New Zealand Police Commissioner, both described building the relationship between the two agencies over the last five years as a priority for them. This viewpoint was consistent with what we heard from staff in both agencies. While acknowledging that the relationship was not perfect or necessarily where they would want it to be, all of these individuals told us about the effort they and others had made to strengthen the relationship and how important it was for them to work together. The 2019 Arotake Review confirmed that the relationship between the two agencies had improved in recent years and was much more productive. However, it also acknowledged that the two agencies continued to experience technical and cultural barriers that prevented them from operating in "a truly joint fashion".[165]

12.4 Positive aspects of the relationship before 15 March 2019

13 New Zealand Police and the New Zealand Security Intelligence Service noted a number of positive developments had occurred that helped improve the relationship between the two agencies.

Joint governance

14 The two agencies have created a three-tiered joint governance framework to drive cooperation:

a) External Relationship Group – the executive level group that manages the relationship between the agencies and is intended to identify capability gaps that will impact on both agencies managing counter-terrorism risk. The two agencies created a Relationship Strategy in 2016, which is managed by this group. The External Relationship Group is attended by a New Zealand Police Deputy Commissioner and the Director-General of Security.[166]

b) Joint Management Committee – maintains strategic oversight of cooperation between the two agencies on counter-terrorism operations and investigations. It includes the heads of counter-terrorism from New Zealand Police and the New Zealand Security Intelligence Service.

c) Operation Coordination Groups – these manage tactical operations and provide the key mechanism for coordinating decision-making and effort.

[165] New Zealand Security Intelligence Service, footnote 57 above at page 20.

[166] The Government Communications Security Bureau also attends.

Joint mechanisms and formal processes

15 New Zealand Police and the New Zealand Security Intelligence Service have created joint mechanisms to coordinate management of leads and investigations[167] to enhance agency interoperability:

a) Joint leads process – the New Zealand Security Intelligence Service hosts a fortnightly Combined Counter-Terrorism Investigations and Leads Meeting (the Joint Leads Meeting) attended by the Department of Corrections, Immigration New Zealand, New Zealand Customs Service, New Zealand Police and (since September 2019) the Government Communications Security Bureau. Agencies bring leads they have, and the other agencies can look across their own data holdings to provide further intelligence on the lead. We heard a range of conflicting views from individuals in the counter-terrorism agencies about whether decisions on which agency leads an operation occur at this meeting, or outside it.

b) Joint operations protocol – this governs the counter-terrorism agencies' joint investigative and operational activity and sets out the process for establishing a joint operation.

Co-location

16 Since 2018, New Zealand Police and the New Zealand Security Intelligence Service have worked in the same secure facility in Auckland. Co-location is acknowledged within both agencies as a positive step that is helping to break down organisational culture barriers, build trust and enhance information sharing. Both agencies spoke about co-location as providing the opportunity for free and frank conversations needed to cooperate successfully. They were hopeful that co-location of the counter-terrorism agencies would progressively increase nationally.

Joint training and secondments

17 Some joint training has occurred between the counter-terrorism agencies in New Zealand. According to a senior official from New Zealand Police this assists in breaking down organisational culture barriers and provides both agencies with insights into how the other operates.

[167] New Zealand Security Intelligence Service, footnote 57 above at page 20.

12.5 The challenges that remain

A shared vision and plan to meet the challenges

18 We heard from international practitioners that formal mechanisms and milestones are required to drive cooperation. With deliberate planning in place, the inevitable points of contention can be diagnosed and resolved early and purposefully.

19 The counter-terrorism agencies have a high-level vision of what the relationship could be – one in which they would not just share information but also work together cohesively as a team. But currently there is not a joint strategy (and associated planning) to ensure the relationship progresses in a purposeful way and at an acceptable pace towards agreed outcomes.

20 The counter-terrorism agencies have had a Relationship Strategy in place since 2016. This contains a high-level rationale and description of work streams, but lacks specific detail of how its aims will be achieved, by when, and how they will be measured. It is discussed regularly at the External Relationship Group. Although there was a high level of goodwill evident in these discussions, we did not see discussion of timeframes or follow-up on how the agencies were tracking against their work. There was also no evidence of discussions about the risks a more integrated way of working could present and how these would be mitigated.

21 We were told that the plan for developing the relationship was to let it grow "organically". What we heard and saw is that the good relationship between New Zealand Police and the New Zealand Security Intelligence was heavily reliant on personal relationships.[168] This dependency on personalities creates a risk.[169]

22 The Auckland co-location is a specific example of the lack of detailed planning within the relationship. While there was a Heads of Agreement governing the co-location, this did not constitute a robust project plan with agreed outcomes or a monitoring and evaluation plan. We heard that senior decision-makers reviewed the outcomes of the co-location, but the lessons from the process were not captured and assessed (at least in written format) for a wider national roll-out, despite there being a significant potential benefit that could be derived if it proves successful and a corresponding cost to national security if it fails.

23 The Department of the Prime Minister and Cabinet does not see its leadership of the national security system as extending to the relationship between New Zealand Police and the New Zealand Security Intelligence Service. We discuss the role of the Department of the Prime Minister and Cabinet in the counter-terrorism effort in Part 8, chapter 3.

[168] New Zealand Security Intelligence Service, footnote 57 above at page 61.

[169] New Zealand Security Intelligence Service, footnote 57 above at page 61.

Understanding of each other's functions

24 The *9/11 Commission Report* described counter-terrorism agencies working jointly as involving a step beyond cooperation, where agencies do not just seek assistance from the other, but rather jointly define problems and options for action.[170]

25 Before 15 March 2019, New Zealand Police and the New Zealand Security Intelligence Service did not have shared definitions of either what constituted right-wing extremism or what would meet the threshold to be prioritised for investigation. As explained in Part 8, chapter 6, New Zealand Police had been monitoring extreme right-wing groups up until 2015. They told us that they did not provide reporting to the New Zealand Security Intelligence Service until the New Zealand Security Intelligence Service initiated a meeting on right-wing extremism in December 2018. This was because they did not think that the New Zealand Security Intelligence Service had an interest in or mandate to examine the extreme right-wing. The fact that New Zealand Police did not create a list of extreme right-wing individuals of concern until after 15 March 2019 (see Part 8, chapter 6) meant that this information had not been shared with the New Zealand Security Intelligence Service, and thus did not inform its baselining project on the extreme right-wing in New Zealand, which commenced in May 2018 (see Part 8, chapter 5).

26 Because the counter-terrorism agencies did not discuss the threat posed by the extreme right-wing until late 2018, they had not by 15 March 2019 developed a joint understanding of the extreme right-wing in New Zealand and were still developing a shared understanding of each other's functions relating to it. Since 15 March 2019, the two agencies have developed a shared definition of what constitutes right-wing extremism.

27 We observed that the New Zealand Security Intelligence Service had a comparatively narrow view of New Zealand Police's functions and capability. This can be illustrated by reference to the individual and the Barry Harry Tarry comments.

28 We asked the New Zealand Security Intelligence Service what it would have done if the individual's posts on The Lads Society Season Two Facebook page using the Barry Harry Tarry username (see *Part 4: The terrorist* and Part 6, chapter 4) had come to its attention. The New Zealand Security Intelligence Service told us that it would have:

a) assessed the posts as not threatening violence and with a marginal connection to national security;

b) seen the posts as relevant to its baselining project on domestic right-wing extremism (see Part 8, chapter 5) and opened a low priority lead; and

c) regarded a lead of this nature as primarily a security intelligence discovery effort, which would fall within its function and mandate.

[170] The *9/11 Commission Report*, footnote 81 above.

29 While the New Zealand Security Intelligence Service noted that it would have shared the lead in the Joint Leads Meeting, it considered this was not the type of lead New Zealand Police would be interested in because there were no indicators of a crime having been committed or a stated intent to undertake violence.

30 We asked a senior New Zealand Police counter-terrorism officer the same question – what they would have done if the individual's posts on The Lads Society Season Two Facebook page using the Barry Harry Tarry username had come to their attention. They said they would have seen the posts as posing limited risk due to the absence of an explicit threat. However, they highlighted concerns about the language used in the posts (including some that we have not reproduced in this report), which they said demonstrated deeply entrenched views and ideological links with the global extreme right-wing movement. New Zealand Police would have recorded this information in the National Intelligence Application, so that if further information about Barry Harry Tarry came to hand, they would be able to build a better intelligence picture. New Zealand Police would thus have been interested in this lead for their own intelligence gathering activities and to stay alert to signs indicating violent extremism.

31 The senior New Zealand Police counter-terrorism officer also noted that while the New Zealand Security Intelligence Service leads in intelligence collection and New Zealand Police lead in evidence collection, this division of roles does not necessarily dictate which agency has primacy in acting on lead information received. Rather, whoever receives the information usually takes the lead. We were told that if New Zealand Police had received the Barry Harry Tarry posts, they would likely have taken the lead in collecting information even though there were no crime indicators or imminent threat present.

32 As this discussion illustrates, New Zealand Police and the New Zealand Security Intelligence Service have different views of the former's counter-terrorism intelligence role.

33 As discussed in *Part 7: Detecting a potential terrorist*, the general tenor of what we were told by the counter-terrorism agencies is that they would probably not have made inquiries at the gym to identify Barry Harry Tarry. In the case of New Zealand Police, the decision whether to make such inquiries would have been influenced by how many of the individual's other posts had also come to light.

Information sharing practices

34 Both New Zealand Police and the New Zealand Security Intelligence Service have extensive information holdings that are relevant to New Zealand's counter-terrorism effort. Neither has access to the other's holdings. The New Zealand Security Intelligence Service needs to protect its sources of information, including information from international partners. Conversely, if the New Zealand Security Intelligence Service had uncontrolled access to New Zealand Police's databases, this would likely present a risk to New Zealand Police's relationship with the public. This absence of direct access means that information is only shared where there is a conscious decision to do so.

35 The Intelligence and Security Act 2017 (see Part 8, chapter 14) allows the New Zealand Security Intelligence Service to create direct access agreements with New Zealand Police to access information related to financial intelligence and about people and locations that pose a physical threat to employees of the New Zealand Security Intelligence Service or the Government Communications Security Bureau. The New Zealand Security Intelligence Service and New Zealand Police have not yet established a direct access agreement.

36 We heard from the counter-terrorism agencies that information flows between them had improved following the creation of an information sharing protocol, but that frustrations continued in some areas, such as the declassification and sanitisation of information by the New Zealand Security Intelligence Service. Some New Zealand Police staff remained frustrated that the New Zealand Security Intelligence Service does not make enough of an effort to provide declassified or sanitised information. This means that New Zealand Police, who primarily operate in an unclassified environment, cannot share information around their organisation. The limited number of secure facilities available to New Zealand Police and limited number of cleared New Zealand Police staff also act as barriers to information sharing (see Part 8, chapter 9).

37 A key challenge for New Zealand Police is that there is no established legal or practice framework that allows the effective use of classified information in the legal process.[171] Individuals from the counter-terrorism agencies worked with the courts to create a workaround which allowed for classified information to be used in support of an application for a search or surveillance warrant.

38 New Zealand Security Intelligence Service staff interviewed considered that they shared all relevant and necessary information even where they had to seek permission from an international partner agency first. While New Zealand Police staff understood that the New Zealand Security Intelligence Service was not able to share all information, some still perceived that relevant and necessary information was held back or unduly filtered.

[171] New Zealand Law Commission *National Security Information in Proceedings* (May 2015) at page 29.

39 It was evident to us during interviews that when it came to information sharing there was a disconnect in how New Zealand Police and New Zealand Security Intelligence Service staff view the current arrangements. There are still high levels of mistrust on the part of some New Zealand Police staff, of which the New Zealand Security Intelligence Service appeared to be largely unaware. Senior officials from both agencies told us that frank conversations were being held. However, the ongoing mistrust we have referred to suggests to us these conversations have not resolved these tensions.

Joint leads process

40 New Zealand Police and the New Zealand Security Intelligence Service have the frameworks in place to work jointly. But the evidence presented to us suggests that these may not be providing sufficient guidance for the two agencies to work in a truly joint way.

41 Before 15 March 2019, the two agencies did not have a shared approach to assessing risk. They did not have a standardised set of criteria for triaging, assessing and prioritising leads and they may have been applying different approaches to risk assessment.

42 After 15 March 2019, the New Zealand Security Intelligence Service adopted the Australia Security Intelligence Organisation leads triage and assessment framework. The New Zealand Security Intelligence Service's position is that the two agencies jointly decided to use this framework to ensure they have a consistent approach to assessing risk. However, we understand this was suggested by the New Zealand Security Intelligence Service after it had already made the decision to adopt the framework. New Zealand Police's position is that they were not aware of being involved in any decision to jointly use the Australia Security Intelligence Organisation framework. New Zealand Police note they continue to use the Australia New Zealand Counter-Terrorism Committee framework, which is very similar.

43 Before 15 March 2019 the counter-terrorism agencies did not have a shared platform to enter and manage leads. Instead, they compared their respective lists at the fortnightly Joint Leads Meeting. It was not always made clear which agency had been assigned specific actions and the progress was not always recorded or jointly visible. Most interviewees acknowledged that the absence of a centralised record of a joint list created a risk that information would be missed.

44 In February 2020 the two agencies rectified this by implementing technology that supports the joint leads process.

Roles in joint investigations and operations

45 From international experience, we have seen there needs to be clear division of labour and mechanisms to decide who is leading an investigation or operation if law enforcement and intelligence and security agencies are to work effectively together. The formal mechanisms New Zealand Police and the New Zealand Security Intelligence Service have in place to guide their joint decisions on investigations and operations are the joint leads process and joint operations protocol.

46 As far as we can tell, there have not been issues between New Zealand Police and the New Zealand Security Intelligence Service with making decisions on when to move from an intelligence operation to executive action (which is sometime an issue for similar agencies in other countries). Instead, both New Zealand Police and the New Zealand Security Intelligence Service expressed frustration about what they saw as New Zealand Police's inability to take action due to the lack of precursor terrorism offences in the Terrorism Suppression Act 2002. We discuss this further in the next chapter.

47 There was not a clear and consistent understanding between New Zealand Police and the New Zealand Security Intelligence Service about how decisions are made about their joint activities, including when the decision is made about how investigations will be led and when joint activity will be pursued. We heard from some interviewees that this decision can occur in the Joint Leads Meeting. Others said that these decisions only happen in the Operational Coordination Groups. According to New Zealand Police staff, the decision to undertake a joint operation was "never that clean" and the joint operations protocol did not provide much guidance on this. The lack of clarity can result in some duplication of effort, for example where an agency may start collecting information on a lead without liaising with the other.

48 We were told that separate investigation plans and warrants may be necessary in relation to the same individual due to the different mandates and functions of the agencies. But it is important that there is a joint plan guiding these efforts. In theory, Operational Coordination Groups should ensure that investigations are coordinated and appropriate deconfliction occurs. However, from what we heard these groups seemed to be convened to provide coordination when operations were already underway and not to set a plan for joint activity at the outset of an operation. As an example, New Zealand Security Intelligence Service staff told us there had likely been at least one instance where more than one intelligence and security or law enforcement agency were surveilling an individual in the period after the 15 March 2019 terrorist attack. This was at a time when events were unfolding quickly and there were large numbers of new leads.

Community engagement practice and impact

49 Both agencies' counter-terrorism efforts rely on seeking information from members of communities and engaging with communities more generally.

50 Public trust and confidence is critical to the operation of both agencies. In Part 8, chapter 6 we described how New Zealand Police did not always communicate what actions they had taken in ways that provided reassurance to Muslim communities. We observed similar issues in relation to the New Zealand Security Intelligence Service. In some cases, the New Zealand Security Intelligence Service staff and Muslim individuals or communities they engaged with had different understandings of the purpose and expected outcomes of their interactions. This was particularly the case where people had raised concerns about potential threats against them and their communities and expected that action would be taken. The New Zealand Security Intelligence Service staff seemed largely unaware of this expectation.

51 There appears to have been limited discussion on or coordination of how the counter-terrorism agencies undertake community engagement and manage the impact of their activities as a whole on communities. In some cases New Zealand Police and the New Zealand Security Intelligence Service will be talking to the same individuals and groups in their efforts to build contacts in communities. We heard from individuals and groups that sometimes they are spoken to separately by New Zealand Police and the New Zealand Security Intelligence Service and are unsure as to whether the two agencies are aware of this. Muslim communities have continued to feel that New Zealand Police and the New Zealand Security Intelligence Service's community engagement efforts are not joined up.

52 There was concern raised by New Zealand Police that in a situation where the two agencies work closely together, negative perceptions that community members may have of the New Zealand Security Intelligence Service could negatively impact on New Zealand Police's relationships with communities.

53 There has been some discussion of all of this between the counter-terrorism agencies, but there has not yet been agreement to a high-level strategy, nor coordination, of how they undertake community engagement.

12.6 Concluding comments

54 The relationship between New Zealand Police and the New Zealand Security Intelligence Service is critical to a well-functioning counter-terrorism effort. The two agencies have made positive progress in developing their relationship. This has been aided by the development of formal mechanisms to better enable the sharing of information and cooperation on investigations.

55 Working jointly requires more than just cooperation. It requires the counter-terrorism agencies to jointly define problems and options for action. Before 15 March 2019 the two agencies were able to assist each other in developing leads and investigations. There was, however, still a tendency for them to work in parallel rather than jointly. For example, they had not developed a shared understanding of the threat of the extreme right-wing, nor developed clear and consistent approaches to joint management of leads and investigations. The future will require a deeper level of integration where both agencies have a shared understanding of the threatscape and what resources and capabilities they are each contributing to the counter-terrorism effort.

56 Despite good progress having been made, there remains a gap between what is considered international best practice, and what is happening in New Zealand. We did not observe sufficient structure and guidance to ensure the counter-terrorism agencies are compelled to push through difficulties. In letting the relationship develop organically the success of the relationship has relied on personal relationships, which risks positive developments being lost as personnel change.

Chapter 13: The Terrorism Suppression Act 2002 and the pre-criminal space

13.1 Overview

1 Acts of terrorism involve criminal offences. They attract liability under the general criminal law. So, an act of terrorism resulting in death can result in a prosecution for murder. As well, the Terrorism Suppression Act 2002 creates several offences that are specific to terrorism.

2 The ways in which New Zealand's general criminal law and the Terrorism Suppression Act operate have left a pre-criminal space in which potential terrorists can plan and prepare acts of terrorism without committing criminal offences. This space is larger than members of the public might expect, and its broad scope has significant implications for the counter-terrorism agencies.

3 In this chapter we discuss the ways in which issues associated with this pre-criminal space could be addressed through the creation of precursor terrorism and travelling offences and administrative mechanisms for reducing risks.

4 At this point brief explanations may be of assistance:

a) **Precursor terrorism offences** are offences that criminalise behaviour that is preliminary to acts of terrorism. Other jurisdictions have such offences. For example, in Australia there are offences of planning or preparing for a terrorist act, providing or receiving training connected with terrorist acts, possessing things in preparation for terrorist acts and collecting or making documents connected with preparation for terrorist acts. There are similar offences in the United Kingdom.

b) **Travelling offences** are a subset of precursor terrorism offences. They criminalise travel (and attempts to travel) internationally for terrorist purposes. Such offences address the behaviours of those who aspire to be foreign terrorist fighters. New Zealand has not created specific travelling offences.

c) **Administrative mechanisms** can mitigate risk. New Zealand has two mechanisms – withdrawal of travel documentation and control orders. Both focus on foreign terrorist fighters.

5 Our primary but not exclusive focus in this chapter is on precursor terrorism offences. In this chapter we:

a) outline the legislative history of the Terrorism Suppression Act;

b) discuss precursor terrorism offences, travelling offences and administrative mechanisms for reducing risk;

c) review the legislative stewardship of the Terrorism Suppression Act; and

d) examine whether there should be precursor terrorism offences.

13.2 Legislative history

6 Before 2002, terrorism was referred to in several statutes but the overall legislative approach was piecemeal.[172] Terrorism was not addressed systematically until the enactment of the Terrorism Suppression Act. This Act was passed to give effect to international conventions and United Nations Security Council resolutions, including Resolution 1373.[173] It was enacted with speed following the attacks of 11 September 2001.[174]

7 The Act has been amended on a few occasions, most significantly by the Terrorism Suppression Amendment Acts of 2003, 2005 and 2007. These Amendment Acts were introduced to ensure that New Zealand complied with international obligations and to keep up to date with international developments. The Act was recently supplemented by the Terrorism Suppression (Control Orders) Act 2019 (see 13.5 Administrative mechanisms for reducing risk).

8 The Act has never been subject to a comprehensive review of whether it is fit for purpose.

13.3 Precursor terrorism offences

International obligations

9 Resolution 1373 of the United Nations Security Council directed countries to:

> *Ensure that any person who participates in the financing, planning, preparation or perpetration of terrorist acts or in supporting terrorist acts is brought to justice and ensure that, in addition to any other measures against them, such terrorist acts are established as serious criminal offences in domestic laws and regulations and that the punishment duly reflects the seriousness of such terrorist acts.*

10 In 2016, the Counter-Terrorism Committee of the United Nations published the *Global survey of the implementation of Security Council resolution 1373 (2001) by Member States*,[175] which assessed countries' compliance with Resolution 1373. In commenting on a group of countries that included New Zealand, the survey provided the following observations under the heading "Planning and preparation":

> *All States have established in national legislation specific provisions that criminalize terrorist acts of planning, preparation, facilitation, support, including financial support, for terrorist acts, or conspiracy to commit terrorist acts,* ***or are able to prosecute such conduct on the basis of general criminal provisions of aiding or similar notions of assistance.***[176]

[172] See for example the Aviation Crimes Act 1972, Crimes (Internationally Protected Persons and United Nations and Associated Personnel, and Hostages) Act 1980, International Terrorism (Emergency Powers) Act 1987 and Maritime Crimes Act 1999.

[173] See Terrorism (Bombings and Financing) Suppression Bill 2002 (121-2) (select committee report) at page 1.

[174] For the background, see Matthew Palmer "Counter-Terrorism law" (2002) *New Zealand Law Journal* 456.

[175] United Nations Security Council Counter-Terrorism Committee Executive Directorate *Global survey of the implementation of Security Council resolution 1373 (2001) by Member States* (October 2016).

[176] United Nations Security Council Counter-Terrorism Committee Executive Directorate, footnote 175 above at page 101.

11 New Zealand is thus required to criminalise acts of planning and preparation for terrorism. This criminalisation can be brought about either by New Zealand's general criminal law or through specific precursor terrorism offences.

Planning and preparation offence under New Zealand's general law

12 If planning and preparation activity is closely associated in time with the intended offence (for instance, a robber lying in wait for a potential victim) the offender can be prosecuted for an attempt to commit the offence. Close proximity to the intended crime is required. And if two or more people are involved in planning and preparation for an offence, they can be prosecuted for conspiracy. But under the general criminal law of New Zealand, it is not a discrete offence to plan or prepare to commit another offence. So it is not an offence to plan or prepare to murder someone, or to rob a bank.

13 This means that New Zealand cannot claim to be in compliance with its obligations under Resolution 1373 on the basis of our general criminal law.

Relevant provisions of the Terrorism Suppression Act

14 A key feature of the Act is the definition of a "terrorist act" in section 5:

> **Terrorist act defined**
>
> (1) An act is a *terrorist act* for the purposes of this Act if—
>
> (a) the act falls within subsection (2); or
>
> ...
>
> (2) An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3), and is carried out for the purpose of advancing an ideological, political, or religious cause, and with the following intention:
>
> (a) to induce terror in a civilian population; or
>
> (b) to unduly compel or to force a government or an international organisation to do or abstain from doing any act.

(3) The outcomes referred to in subsection (2) are—

(a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act):

(b) a serious risk to the health or safety of a population:

(c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d):

(d) serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life:

(e) introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country.

15 When first passed, the Act did not create an offence of engaging in a terrorist act. This deficiency was addressed in 2007 with the insertion of section 6A. It provides:

6A Terrorist act

(1) A person commits an offence who engages in a terrorist act.

(2) A person who commits a terrorist act is liable on conviction to imprisonment for life or a lesser term.

16 There are a number of other terrorism offences created by the Act. These include financing of terrorism (section 8), providing property or financial or related services to a designated terrorist entity (section 10), recruiting members of terrorist groups (section 12) and participating in terrorist groups (section 13). With the exception of those offences, there is nothing explicit in the Act to criminalise activities that are preliminary to acts of terrorism. And those offences only apply to terrorist activity in which two or more people are involved (for example, the recruitment offence requires both a recruiter and a potential recruitee, while the financing offence requires a fundraiser as well as a donor). They do not apply to the activities of lone actor terrorists. There are thus no explicit offences that catch the activity of a lone actor terrorist that is preliminary to a terrorist act.

Is there nonetheless a planning and preparation offence?

17 For a number of years, the counter-terrorism agencies acted on the understanding that preparing or planning acts of terrorism are not offences. Recently, however, the Deputy Solicitor-General consented to a prosecution based on the view that the Act does create such offences.

18 In the prosecution that followed, the Crown relied on section 25(1), which provides:

> **25 Carrying out and facilitating terrorist acts**
>
> (1) For the purposes of this Act, a terrorist act is carried out if any 1 or more of the following occurs:
>
> (a) planning or other preparations to carry out the act, whether it is actually carried out or not:
>
> (b) a credible threat to carry out the act, whether it is actually carried out or not:
>
> (c) an attempt to carry out the act:
>
> (d) the carrying out of the act.

19 The prosecution argued that the section 25(1) definition of "carrying out a terrorist act" meant that engaging in a terrorist act under section 6A included "planning or other preparation for such an act".

20 The High Court found that this argument was not correct and that planning and preparation for a terrorist act are not, in themselves, offences.

21 We regard the result arrived at by the High Court as correct and, more importantly, as settling the law. For this reason we do not engage with the intricate issues of statutory interpretation that the case raised.

Where New Zealand stands with its international obligations

22 As New Zealand does not have precursor terrorism offences and our general criminal law does not criminalise planning and preparation to commit an offence, New Zealand is in breach of its international obligations under Resolution 1373 of the United Nations Security Council.

Practical implications

23 There were differing views, at least within New Zealand Police, as to whether section 25(1) meant that there were planning and preparation offences. Despite this, New Zealand Police and the New Zealand Security Intelligence Service generally have operated on the assumption – now shown to be correct – that there are no such offences. This has limited their ability to bring particular investigations to a conclusion.

24 We have seen case studies that indicate that if there had been planning and preparation terrorism offences, some counter-terrorism targets could have been prosecuted under them. The ability to bring a prosecution would have been assisted by a wider range of precursor terrorism offences including, say, travelling offences. Whether such prosecution would necessarily have been appropriate – for instance where planning was in its very early stages – is perhaps another matter. But the availability of such offences would have provided a point of intervention, for example, by warning the target that they could be prosecuted if they did not agree to participate in community countering violent extremism measures. As well, the absence of such offences hinders the ability of New Zealand Police to obtain warrants under the Search and Surveillance Act 2012.

25 We can illustrate the practical difficulties associated with the absence of planning and preparation offences by reference to what would have happened if the counter-terrorism agencies had become aware that the individual was planning a terrorist attack.

26 Had this happened, it would have been open to New Zealand Police to cancel his firearms licence and seize his firearms. Such action would not have prevented the individual acquiring firearms on the black market or adjusting his proposed mode of attack to involve, say, a motor vehicle. It may also have been possible to require him to return to Australia, an option that of course would not have been available if he was a New Zealand citizen.

27 Depending on the way the individual stored his semi-automatic rifles and large capacity magazines, it might have been possible to prosecute him under the Arms Act 1983 (see *Part 4: The terrorist*). But although such a prosecution would have been a completely inadequate response to his conduct, the alternative – waiting until he got sufficiently close to the intended terrorist attack to prosecute him for attempted murder or attempting to engage in a terrorist act – would not have been a very palatable option.

28 It would have been a fine judgement call as to the point at which the individual's preparation would have been sufficiently proximate to the intended crime to result in criminal liability for an attempt. To be reasonably confident of conviction, New Zealand Police would probably have had to wait until the morning of 15 March 2019 when the individual departed Dunedin for Christchurch. Keeping the individual under surveillance for a protracted period would have put New Zealand Police and the New Zealand Security Intelligence Service under extraordinary pressure and would not have been a fail-safe way of preventing an attack.

29 Internationally there is a well-recognised and longstanding healthy tension between law enforcement and intelligence and security agencies about when to transition from an intelligence investigation to executive action, such as arrest. The tension arises because the drivers for each agency are different. The imperative for an intelligence and security agency is to discover all threats to national security. An operation may yield greater intelligence gains if action is not taken at the first opportunity. Law enforcement agencies may wish to act more quickly on intelligence, particularly where public safety may be at risk. Interestingly, we have seen no evidence of such a tension between the New Zealand counter-terrorism agencies – something we see as a likely consequence of the absence of precursor terrorism offences.

13.4 Travelling offences

30 United Nations Security Council Resolution 2178 of 2014 requires states to:

> *... ensure that their domestic laws and regulations establish serious criminal offenses sufficient to provide the ability to prosecute and to penalize in a manner duly reflecting the seriousness of the offense:*
>
> *their nationals who travel or attempt to travel to a State other than their States of residence or nationality, and other individuals who travel or attempt to travel from their territories to a State other than their States of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training; ... .*

31 New Zealand has not yet enacted laws that create the offences called for by the Resolution. Proposals to create such offences are currently under consideration.

13.5 Administrative mechanisms for reducing risk

32 The two mechanisms identified at the beginning of the chapter (withdrawing travel documents and control orders) have been provided for in respect of foreign terrorist fighters. The withdrawal of travel documents is designed to prevent travel out of New Zealand by prospective foreign terrorist fighters. The control orders regime is intended to mitigate the risks posed by returning foreign terrorist fighters.

33 Sections 27GA–27GF of the Passports Act 1992 provide for refusals to issue, and suspension and cancellation of, New Zealand travel documents. These mechanisms were first introduced in 2014 and enable disruption of attempts to travel overseas for terrorist purposes. This is not a fail-safe system (for instance, in respect of people who have more than one passport) but, as we have noted, New Zealand has not yet criminalised preparation for such travel.

34 The offence of participation in terrorist groups created by section 13 has effect outside New Zealand. So a New Zealander who has participated in a terrorist group overseas and returns to New Zealand can be prosecuted under section 13.

35 The Terrorism Suppression (Control Orders) Act 2019 provides for control orders in respect of people who have returned from overseas and who, by reason of their actions in a foreign country, pose real risks of "engaging in terrorism-related activities". Once made, these control orders impose prohibitions or restrictions on the activities of such people in New Zealand.

36 The narrow scope of this regime means that it is not an appropriate substitute for the creation of precursor terrorism offences.

13.6 Legislative stewardship

37 Departmental chief executives are responsible for maintaining the currency of any legislation administered by their departments.[177] This means those chief executives should be providing free and frank advice regarding whether that legislation is fit for purpose.

38 The Terrorism Suppression Act is jointly administered by the Ministry of Foreign Affairs and Trade and the Ministry of Justice. Section 70 of the Act required a one-off review of certain provisions of the Act, which was completed in 2005. Amendments were made to the Act in 2005 and 2007. These provided further offences (partly in response to international obligations) and made changes to the designation of terrorist entities. But the Act's content and workability have never been the subject of a fitness for purpose review.

39 The workability of the Terrorism Suppression Act was called into question in 2008 after the then Solicitor-General declined to give permission to lay charges under the Act following Operation Eight (see Part 8, chapter 2). He said that the relevant provisions were "unnecessarily complex, incoherent and as a result it is almost impossible to apply [in the circumstances of that case]".

40 The Terrorism Suppression Act was referred to the Law Commission for review but the review was not progressed. It was initially put on hold pending the trial of the remaining Operation Eight defendants, and then in 2012 was removed from the Law Commission's work programme by Hon Judith Collins, then Minister of Justice. The Law Commission later listed "Criminal Offences in the Terrorism Suppression Act" as part of its programme for 2013–2014 but the then Minister again removed it. Hon Judith Collins said that "the initial concerns arising from the Urewera case have been addressed by the passage of the Search and Surveillance Act 2012, and there does not appear to be any substantial or urgent concerns arising from the operation of the Act".[178]

[177] Public Service Act 2020, section 52(1)(d)(ii).

[178] Adam Dudding "Review of terror laws stopped" *Sunday Star Times* (New Zealand, 15 September 2013) http://www.stuff.co.nz/national/politics/9166763/Review-of-terror-laws-stopped.

41 In 2014, New Zealand Police drew attention to gaps in the legislative framework. While New Zealand Police did not consider that these gaps affected their ability to manage a particular risk presenting at that time, they considered that the gaps might become problematic if the situation evolved. A 2015 Cabinet paper noted potential areas for legislative review and reform, but none of this work was progressed at that time. New Zealand Police expressed increasing concern about the possible inadequacy of the legislation over this period. The New Zealand Security Intelligence Service shared these concerns.

42 In November 2017, the Department of the Prime Minister and Cabinet advised the Prime Minister, Rt Hon Jacinda Ardern, that it was unclear if New Zealand's counter-terrorism legislation was fit for purpose and that it intended to discuss these issues with the relevant Public sector agencies. In May 2018, the Director-General of Security and the Commissioner of Police briefed the Prime Minister, Rt Hon Jacinda Ardern, and the Minister Responsible for the New Zealand Security Intelligence Service, Hon Andrew Little, on the evolving terrorism threatscape and related counter-terrorism legislative challenges. At that time, Ministers sought advice on the counter-terrorism legislative settings. Advice from the Department of the Prime Minister and Cabinet and the Ministry of Justice was provided to Rt Hon Jacinda Ardern, Minister for National Security and Intelligence and Hon Andrew Little, Minister of Justice, in August 2018.

43 The two Ministers subsequently directed the Department of the Prime Minister and Cabinet and the Ministry of Justice to undertake further policy work on:

a) the workability of the Terrorism Suppression Act;

b) new offences that might facilitate earlier intervention by law enforcement;

c) consideration of criminalising travel by foreign terrorist fighters; and

d) consideration of control orders for people who pose a terrorism risk.

44 Ministers noted that this did not necessarily mean that any resulting policy proposals would be accepted by government and emphasised that they wanted to "proceed with caution".

45 As at 15 March 2019, officials were considering the issues but no advice had been provided to Ministers. Advice on priorities was subsequently provided to Hon Andrew Little, Minister of Justice, which led to some counter-terrorism policy work on, for example, control orders and financing of terrorism, being expedited at the expense of other policy projects on, for example, organised crime.

46 Since that time, the government has passed the Terrorism Suppression (Control Orders) Act 2019, creating a civil control order regime that applies to individuals who have engaged in terrorist activity overseas. Work is continuing on possible new terrorism related offences and the workability of the definition of "terrorism" in the Terrorism Suppression Act. A separate but related piece of work will respond to the Law Commission's report on the use of national security information in court proceedings.[179]

47 As this discussion illustrates, the issues discussed in this chapter have been recognised for some time but the 2014 amendments to the Passports Act and the creation of a limited control orders regime in 2019 have been the only tangible progress.

13.7 Should there be precursor terrorism offences?

48 The creation of precursor terrorism offences would require analysis of policy issues. These are explored in a recent article in the Criminal Law Review that criticises the ways in which precursor terrorist offences have been defined and prosecuted in England and Wales.[180] The precursor offences primarily discussed are preparing acts of terrorism, disseminating terrorist publications and collecting information that is likely to be useful to a terrorist. They are "among the most frequently prosecuted terrorism offences".[181] There are issues with the preparation offence. It can catch a person's preliminary behaviour (for example, research into possible methods and targets) even if their intention to engage in acts of terrorism was only conditional (for instance, as depending on future circumstances) and thus not necessarily very likely to be carried out.

49 For these and other reasons reviewed in the article, there is at least a debate to be had before simply expressed precursor terrorism offences (including planning and preparation offences) are created. This is not to seek to pre-empt the result of such a debate, as simply expressed preparation offences exist both in Australia and also in the United Kingdom. Also material to such debate are New Zealand's international obligations.

50 We see much less scope for debate on the appropriateness of criminalising conduct that is connected to the intended act of terrorism, for instance acquiring weapons, terrorist training or preparation in relation to an identifiable potential target (such as hostile reconnaissance or specific internet research).

[179] New Zealand Law Commission *The Crown in Court: A Review of the Crown Proceedings Act and National Security Information in Proceedings Report* 135 (Wellington, December 2015).

[180] Andrew Conford "Terrorist Precursor Offences: Evaluating the Law in Practice" (2020) *Criminal Law Review* at page 663.

[181] Andrew Conford, footnote 180 above at page 664.

13.8 Concluding comments

51 There has been no complete review of whether the Terrorism Suppression Act and its amendments are fit for purpose.

52 Extending the reach of the criminal law (such as by creating precursor terrorism offences, which would criminalise planning and preparation for terrorism and perhaps other activities) would be controversial. So too are preventative measures that do not depend upon conviction for a criminal offence (such as withdrawing travel documents or imposing control orders). We discuss this further in *Part 10: Recommendations*.

53 Our primary concern is with the absence of precursor terrorism offences. We accept that there is scope for legitimate concerns about the risks of over-criminalisation and discrimination against Muslim communities and other potential target communities. The concerns can be mitigated by careful drafting. As well, there are what we see as countervailing factors, particularly our current non-compliance with international obligations and the broader context of the practical difficulties of dealing with potential terrorists and the associated risks to public safety.

Chapter 14: The Intelligence and Security Act 2017

14.1 Overview

1 The Intelligence and Security Act 2017 was enacted following the 2016 Cullen-Reddy Report and gives effect to many of its recommendations.[182] The Act governs the operations of the New Zealand Security Intelligence Service (see Part 8, chapter 5) and the Government Communications Security Bureau (see Part 8, chapter 7), which are defined in the Act as the "intelligence and security agencies".[183]

2 In this chapter, we review the way the Intelligence and Security Act operates in respect of the counter-terrorism effort. The purpose of this exercise is to identify the legal boundaries within which the intelligence and security agencies must operate. We do this by reference to:

a) the objectives and functions of the agencies;

b) oversight of the agencies;

c) the overarching constraints on the agencies;

d) the provisions of the Act dealing with the collection of intelligence;

e) the limited statutory mandate of the Department of the Prime Minister and Cabinet;

f) the extent to which the Act contemplates bulk collection and acquisition of data; and

g) the relationships between the Inspector-General of Intelligence and Security and the agencies.

3 We conclude the chapter with a discussion of other issues, including difficulties and uncertainties with the operation of the Act.

14.2 Objectives and functions of the agencies

4 The objectives of the intelligence and security agencies are provided for by section 9:

> **9 Objectives of intelligence and security agencies**
>
> The principal objectives of the intelligence and security agencies are to contribute to—
>
> (a) the protection of New Zealand's national security; and
>
> (b) the international relations and well-being of New Zealand; and
>
> (c) the economic well-being of New Zealand.

[182] Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM, footnote 38 above.

[183] Intelligence and Security Act 2017, section 4.

5 Countering terrorism falls naturally within the section 9(a) objective.

6 The functions of the agencies are identified in sections 10 to 15 and include:

> **10 Intelligence collection and analysis**
>
> (1) It is a function of an intelligence and security agency to—
>
> (a) collect and analyse intelligence in accordance with the New Zealand Government's priorities; and
>
> (b) provide any intelligence collected and any analysis of that intelligence to 1 or more of the following:
>
> (i) the Minister:
>
> (ii) the Chief Executive of the Department of the Prime Minister and Cabinet:
>
> (iii) any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis of that intelligence.

7 The statutory objectives and functions of the agencies are the same, despite their very different capabilities.

8 Government priorities for intelligence and security are set out primarily in the National Security and Intelligence Priorities (see Part 8, chapter 3). For the purposes of section 10(1)(a) they specify the topics on which the agencies may collect and analyse intelligence. It remains open to the government to identify priorities (and thus authorise collection and analysis) in other ways. What is important is that the agencies are not entitled to self-task. They may only collect and analyse intelligence to the extent authorised by priorities set by the government.

9 Section 13(1) and (2) authorise cooperation between the agencies. It also provides for cooperation between the agencies and the New Zealand Defence Force and New Zealand Police.

10 The Act also sets out functions that do not fall within the agencies' mandate. In particular, section 16 provides that it "is not the function of [the agencies] to enforce measures for national security" except in very limited circumstances. So, it is open to the agencies to collect and analyse intelligence in accordance with priorities set by the government, but they cannot use this intelligence for enforcement purposes. Where enforcement is appropriate, this must be carried out by another Public sector agency, such as New Zealand Police (see Part 8, chapters 6 and 12).

14.3 Oversight of the agencies

11 Oversight of the intelligence and security agencies and their activities is provided for in a number of ways:

a) They are subject to ministerial oversight. The minister responsible for the intelligence and security agencies has functions in relation to the issue of warrants, the approval of business records directions and permission to access restricted information (see 14.6 The provisions of the Act dealing with the collection of intelligence). As well, the agencies are required to have regard to Ministerial Policy Statements issued under section 206 (see 14.5 Overarching constraints on the agencies).

b) The approval of a Commissioner of Intelligence Warrants (who must previously have held office as a High Court judge) and the relevant minister is required for the issue of business records directions and certain warrants. Permission from the Chief Commissioner of Intelligence Warrants is also required for access to certain restricted information.

c) The Intelligence and Security Committee is a statutorily recognised (by section 192) Parliamentary committee that has oversight functions provided for in section 193.

d) There is an Inspector-General of Intelligence and Security who has extensive oversight functions.

e) The agencies are subject to judicial supervision through court proceedings.[184]

f) The agencies are subject to Privacy Commissioner and Ombudsman oversight.

12 In this chapter, we focus on the roles of the Intelligence and Security Committee and the Inspector-General of Intelligence and Security.

The role of the Parliamentary Intelligence and Security Committee

13 The functions and membership of the Parliamentary Intelligence and Security Committee are provided for in the Act. Its members must be drawn from the parties in government and those in opposition.

14 Under section 193, the Intelligence and Security Committee's functions include examining the policy, administration and expenditure of the agencies, receiving their annual reports and conducting annual reviews. There are, however, constraints. While the Intelligence and Security Committee can consider any matter with intelligence or security implications referred to the committee by the prime minister, this does not extend to matters "relating directly to activities of an" agency.[185] As well, section 193(2)(b) provides that the functions do not include:

[184] Intelligence and Security Act 2017, section 162.

[185] Intelligence and Security Act 2017, section 193(1)(f).

> … inquiring into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods, or sources of information … .

15 Sections 202–205 and 224 address the provision of "sensitive information" to the Intelligence and Security Committee and how such information is to be dealt with if provided. Sensitive information is information that, if disclosed, would be likely to prejudice national security, prejudice the maintenance of the law or endanger anyone. Under section 203(1)–(3), whether sensitive information is disclosed depends on the assessment of the Director-General of the relevant agency or the direction of the prime minister.

16 There is an Intelligence and Security Committee of the United Kingdom Parliament. It can, and does, inquire into the operations and activities of the intelligence and security agencies in the United Kingdom.

17 A more extensive and public role for New Zealand's Intelligence and Security Committee would be desirable. It would provide further transparency and general assurance to the public as to the activities of the agencies and thus improve their social licence. Such a role for the Intelligence and Security Committee would require reasonably high levels of cross-party political consensus and trust. In the current environment, we would like to think that such consensus and trust can be achieved.

The role of the Inspector-General of Intelligence and Security

18 The functions of the Inspector-General of Intelligence and Security are specified in section 158. They include:

a) conducting inquiries into:

   i) an agency's compliance with the law;

   ii) whether a New Zealander has been adversely affected by an agency's action, omission, policy or procedure; and

   iii) the propriety (appropriateness) of an agency's actions;

b) dealing with complaints made under section 171 of the Act, which provides for complaints by employees of the agencies or any New Zealander who claims to have been "adversely affected" by an agency's actions, inaction, policies or procedures; and

c) conducting annual reviews and unscheduled audits on warrants (including their issue), compliance systems and the carrying out of any authorised activity.

19 The last two Inspectors-General of Intelligence and Security made a practice of reviewing every warrant obtained by the agencies (see 14.6 The provisions of the Act dealing with the collection of intelligence). At the time the Act was under consideration by Parliament, this scrutiny was described as a component – along with requirements for approval of warrants by the responsible minister and a Commissioner of Intelligence Warrants – of the "triple-lock" protection for New Zealanders from surveillance.

20 Section 163 provides that a conclusion by the Inspector-General of Intelligence and Security that the issue of a warrant or conduct carried out under the warrant was irregular does not invalidate the warrant or render the activity illegal.

14.5 Overarching constraints on the agencies

21 The agencies have a duty to act in accordance with New Zealand law and "all human rights obligations recognised in New Zealand law". They must also act independently and impartially, with integrity and professionalism and in a manner that facilitates democratic supervision.[186]

22 The obligation of the agencies to act appropriately is reinforced by the section 158(1)(c) power of the Inspector-General of Intelligence and Security to conduct an "inquiry into the propriety of particular activities of an intelligence and security agency".

23 There may be scope for debate as to what is unlawful and thus would be a breach of the agencies' obligation to act in accordance with New Zealand law. Unlawful activities must include the commission of criminal offences (whether under the Crimes Act 1961 or otherwise) and behaviour that is contrary to statute (for example, the Privacy Act 1993 and the New Zealand Bill of Rights Act 1990). But whether it also encompasses civil wrongs (for example, trespass or a breach of contract) is unclear. Activities that would otherwise be unlawful can be authorised by warrant (see 14.6 The provisions of the Act dealing with the collection of intelligence).

24 In performing their functions, agencies are required by section 209 "to have regard to Ministerial Policy Statements" issued under section 206. These cover a wide range of lawful activities, including the collection of information, conducting surveillance in public places, obtaining and using publicly available information and requesting information from third parties. The Ministerial Policy Statements impose requirements on the agencies to act only in ways that are both necessary for the agency to pursue its functions and proportionate to the national security purpose on which the agencies rely. They also impose associated restrictions (such as using the least intrusive mechanism possible) and reinforce restrictions imposed by the Act and other statutes.

[186] Intelligence and Security Act 2017, sections 17(a)–(d).

25 The summary at the start of the Ministerial Policy Statement on obtaining and using publicly available information provides an indication of its contents and how Ministerial Policy Statements generally are expressed:

> *It is lawful for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) to obtain and use publicly available information. This ministerial policy statement (MPS) provides guidance on the conduct of this activity. In making decisions related to obtaining and using publicly available information, GCSB and NZSIS must have regard to the following principles: respect for privacy, necessity, proportionality, least intrusive means, respect for freedom of expression, including the right to advocate, protest or dissent, legality and oversight. This MPS also specifies certain matters to be included in internal policies and procedures.*[187]

26 Under section 18(b) of the Act, there is a requirement to ensure that:

> ... any co-operation with foreign jurisdictions and international organisations in the performance of any of the agency's functions is in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

27 The practical implications of this section are fleshed out in a Ministerial Policy Statement.

28 Under section 19, the exercise of the right of freedom of expression (including "the right to advocate, protest or dissent") "does not of itself justify an intelligence and security agency taking any action". A broadly similar version of the provision was first introduced in the New Zealand Security Intelligence Service Act 1969 in 1977.[188] The scope and meaning of the provision has never been subject to judicial explanation.[189] We discuss the implication of this section in relation to target discovery below (see 14.10 Other issues, difficulties and uncertainties with the Act).

29 Subject to these constraints, the agencies can carry out any lawful activity, providing it is carried out in the performance or exercise of any function, duty or power.[190]

[187] Christopher Finlayson *Obtaining and using publicly available information* (September 2017) at page 1.

[188] See the New Zealand Security Intelligence Service Amendment Act 1977, section 3.

[189] Section 3 of the 1977 Act was mentioned in *Choudry v Attorney-General* HC Christchurch CP15/98, 19 August 1998 at page 31. See also Andrew Geddis and Elana Geddis "Addressing terrorism in New Zealand's low threatscape" in I Cram (ed) *Extremism, Free Speech and Counter-Terrorism Law and Policy* (Routledge, Abindgon: UK, 2019) 190 at page 204, which was finalised before 15 March 2019.

[190] Intelligence and Security Act 2017, section 48.

14.6 The provisions of the Act dealing with the collection of intelligence

30 As discussed above, the Intelligence and Security Act imposes a number of limitations on agencies' activities that are not illegal. It also, however, confers powers on agencies which are specific to them, in particular:

a) the use of assumed identities;

b) requests for information;

c) direct access to certain databases held by other Public sector agencies;

d) access to restricted information;

e) business records directions; and

f) collection of intelligence as authorised by warrant.

The use of assumed identities

31 Sections 21–45 authorise and regulate the adoption of assumed identities by agency employees[191] and the use of entities to enable an agency to conduct transactions while maintaining secrecy.[192]

Requests for information

32 Section 121 provides for requests for information by the Directors-General of the intelligence and security agencies to "any other agency".[193] Such a request can be made where the Director-General of one of the agencies believes, on reasonable grounds, that the information is necessary to perform its functions.

33 Section 122 applies to the agency that holds the information requested. An agency can provide the information requested if it chooses to and it believes, on reasonable grounds, that the disclosure of the information is necessary for the intelligence and security agency to perform its functions. To assist with the requested agency's decision, the Director-General of an intelligence and security agency can certify that the disclosure of the information is necessary for the agency to perform its functions.[194]

[191] Intelligence and Security Act 2017, sections 21–32.

[192] Intelligence and Security Act 2017, sections 33–44.

[193] Agency means "any person, whether in the public sector or the private sector" and "includes a department and an interdepartmental venture". See Intelligence and Security Act 2017, section 118.

[194] Intelligence and Security Act 2017, section 122(3).

34 A request and certificate do not override any legal impediment to disclosure (such as contractual obligation).[195] And compliance with these requests is voluntary. So even in the absence of a legal impediment, the requested agency is not legally required to provide information to an intelligence and security agency.

Data access

35 Sections 124–133 deal with the provision of direct access to databases storing "specified public sector information". Schedule 2 of the Act sets out which of the two intelligence and security agencies can negotiate direct access agreements with identified holding agencies.

Table 13: Direct access agreements provided for by the Intelligence and Security Act

Intelligence and security agency	Information-holding agency	Information	Does a direct access agreement exist?
Government Communications Security Bureau and New Zealand Security Intelligence Service	Registrar-General who administers the Births, Deaths, Marriages and Relationships Registration Act 1995	Information about births, civil unions, deaths, marriages and name changes	No for Government Communications Security Bureau Yes for New Zealand Security Intelligence Service
Government Communications Security Bureau and New Zealand Security Intelligence Service	Secretary of Internal Affairs (chief executive of the Department of Internal Affairs)	Citizenship information	No
Government Communications Security Bureau and New Zealand Security Intelligence Service	Ministry of Business, Innovation and Employment	Information collected in connection with the performance or exercise of a function, duty or power under the Immigration Act 2009	No for Government Communications Security Bureau Yes (in part) for New Zealand Security Intelligence Service[196]

[195] Intelligence and Security Act 2017, section 122(4).

[196] Under its direct access agreement with the Ministry of Business, Innovation and Employment, the New Zealand Security Intelligence Service has access to Advanced Passenger Processing information. The information allowed to be shared under the Intelligence and Security Act is broader than this.

Intelligence and security agency	Information-holding agency	Information	Does a direct access agreement exist?
Government Communications Security Bureau and New Zealand Security Intelligence Service	New Zealand Customs Service	Information about border-crossing persons, goods and craft that has been collected in connection with the performance or exercise of a duty or power under the Customs and Excise Act 1996	No for Government Communications Security Bureau Yes for New Zealand Security Intelligence Service
Government Communications Security Bureau and New Zealand Security Intelligence Service	New Zealand Police	Financial intelligence information	No
New Zealand Security Intelligence Service	New Zealand Police	Information about people and locations identified as posing a possible physical threat to Government Communications Security Bureau and New Zealand Security Intelligence Service employees	No

36 Direct access agreements are made between the ministers of the relevant intelligence and security agency and the agency that holds the information. Consultation with the Privacy Commissioner and Inspector-General of Intelligence and Security is required (see Part 8, chapter 9). Limited progress has been made in finalising the direct access agreements envisaged in the Act (see 14.10 Other issues, difficulties and uncertainties with the Act).

Access to restricted information

37 Restricted information encompasses confidential tax information, information about national student numbers, adoption information and photographic images used for driver's licences.[197]

38 The Director-General of an intelligence and security agency seeking access to restricted information must have the permission of the responsible minister and the Chief Commissioner of Warrants if the person concerned is a New Zealand citizen or permanent resident. If the person is not a New Zealand citizen or permanent resident, the responsible minister's permission is required.[198] If permission is granted, the agency holding the restricted information must provide it to the relevant Director-General.[199]

Business records directions

39 Sections 143–155 provide for the intelligence and security agencies to obtain business records of telecommunications network operators and financial service providers. Business records include all information generated or received in the course of the organisation's business but excludes the content of communications.[200]

40 Once the Director-General of an agency is granted approval[201] from the responsible minister and a Commissioner of Intelligence Warrants to obtain business records, they can issue a business records direction. A direction issued under section 150 is restricted to specified business records (or a specified class of business records relating to an identifiable person or thing). For these purposes, "thing" includes an address (for example, an IP address).[202] There is a statutory obligation to comply with a business records direction.

Warrants

41 Under section 49(1), an intelligence and security agency needs a warrant to carry out any activity that would otherwise be unlawful, that is, it would be unlawful but for the authorisation.[203] There is a similar requirement that applies if a New Zealand intelligence and security agency asks an international partner to carry out activity outside New Zealand that would be unlawful if it was carried out in New Zealand.[204] This applies even if the activity is lawful in the international partner country's jurisdiction.

[197] Intelligence and Security Act 2017, section 135.

[198] Intelligence and Security Act 2017, section 136.

[199] Intelligence and Security Act 2017, section 141.

[200] See the definition of "business records" in section 144.

[201] An application for approval is made under section 145 and approval is made under section 147.

[202] Intelligence and Security Act 2017, section 150(4)(b).

[203] Intelligence and Security Act 2017, section 49(1).

[204] Intelligence and Security Act 2017, section 49(2).

42 Section 49 complements section 17, which imposes a general obligation on the agencies to act lawfully. An activity that is authorised under the Act is lawful even if it is contrary to other legislation.[205]

43 The Act provides for different types of warrants.[206] The most relevant type are intelligence warrants, which are provided for by sections 52–78 of the Act.[207] Sections 53 and 54 provide for two types of intelligence warrant – Type 1 and Type 2:

> **53 Type 1 intelligence warrant**
>
> A Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to,—
>
> (a) any person who is—
>
> (i) a New Zealand citizen; or
>
> (ii) a permanent resident of New Zealand; or
>
> (b) a class of persons that includes a person who is—
>
> (i) a New Zealand citizen; or
>
> (ii) a permanent resident of New Zealand.
>
> **54 Type 2 intelligence warrant**
>
> A Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required.

44 Type 1 warrants apply to New Zealand citizens and permanent residents. Type 2 warrants apply to people who are not New Zealand citizens or permanent residents. The difference between the two types of warrant was inherited from the Government Communications Security Bureau Act 2003, which was replaced by the Intelligence and Security Act. Section 14 of the Government Communications Security Bureau Act placed restrictions on the interception of communications of New Zealand citizens and permanent residents.

[205] Intelligence and Security Act 2017, section 49(3).

[206] See the definition of "authorisation" in section 47.

[207] Sections 71–76 provide for the urgent issue of warrants and section 78 provides for very urgent authorisations to be granted where there is insufficient time to obtain a warrant.

45 Type 1 warrants are considered and issued by the responsible minister (or ministers) and a Commissioner of Intelligence Warrants. Type 2 warrants are considered by the responsible minister alone.[208] And, as noted above, the current practice of the Inspector-General of Intelligence and Security is to review every warrant obtained by the agencies. This creates "triple-lock" protection for Type 1 warrants and "double-lock" protection for Type 2 warrants.

46 The preconditions to the issue of warrants are provided for in sections 58 and 59 (for Type 1 warrants) and section 60 (for Type 2 warrants). As well, section 61 (for Type 1 and Type 2 warrants) provides:

> **61 Additional criteria for issue of intelligence warrant**
>
> The additional criteria for the issue of an intelligence warrant … are that—
>
> (a) the carrying out of the otherwise unlawful activity (a proposed activity) by an intelligence and security agency is necessary to enable the agency to perform a function under section 10 or 11; and
>
> (b) the proposed activity is proportionate to the purpose for which it is to be carried out; and
>
> (c) the purpose of the warrant cannot reasonably be achieved by a less intrusive means; and
>
> (d) there are satisfactory arrangements in place to ensure that—
>
> (i) nothing will be done in reliance on the intelligence warrant beyond what is necessary and reasonable for the proper performance of the function under section 10 or 11; and
>
> (ii) all reasonably practicable steps will be taken to minimise the impact of the proposed activity on any members of the public; and
>
> (iii) any information obtained in reliance on the intelligence warrant will be retained, used, and disclosed only in accordance with this Act or any other enactment.

47 Section 61, amongst other things, thus creates a necessary and proportionate test that must be satisfied before a warrant can be issued. This test is not detailed further in the statute.

48 Where a Type 1 warrant is sought for counter-terrorism purposes, the agency must establish that the activity "is necessary to contribute to the protection of national security" and "identifies, enables the assessment of, or protects against … terrorism or violent extremism".[209]

[208] Intelligence and Security Act 2017, section 60.

[209] Intelligence and Security Act 2017, section 58(1)(a)(i), (ii) and (2)(a).

49 The preconditions for the issue of a Type 2 warrant appear less exacting. Where such a warrant is sought for counter-terrorism purposes, the applicant need only show that the activity for which authorisation is sought "is necessary to contribute to national security" and the activity is not in respect of a person (or class of persons) for which a Type 1 warrant is required. There is no explicit requirement to show that the activity "identifies, enables the assessment of, or protects against ... terrorism or violent extremism".

50 This may be a distinction without a practical difference in the context of counter-terrorism. The need to show that the activity is "necessary to contribute to the protection of national security"[210] and the necessary and proportionate requirement under section 61 mean that the information required to support an application for a Type 2 warrant is practically the same as for a Type 1 warrant. In respect of counter-terrorism, it is open to question whether there is a continuing need for, or utility in, the distinction between the two types of warrant, at least as to the criteria to be applied.

51 Section 56 provides for the Directors-General of both agencies to apply for a joint intelligence warrant. No such application has ever been made. That said, the agencies cooperate to some extent, using each other's warrants (under section 51 requests to assist) and sharing intelligence.

52 Section 67(1) sets out the actions that can be authorised under an intelligence warrant:

> **67 Authorised activities**
>
> (1) An intelligence warrant may authorise the carrying out of 1 or more of the following activities that would otherwise be unlawful:
>
> (a) conducting surveillance in respect of 1 or more—
>
> (i) persons or classes of persons:
>
> (ii) places or classes of places:
>
> (iii) things or classes of things:
>
> (b) intercepting any private communications or classes of private communications:
>
> (c) searching 1 or more—
>
> (i) places or classes of places:
>
> (ii) things or classes of things:

[210] Intelligence and Security Act 2017, section 60(3)(a)(i).

(d) seizing—

(i) 1 or more communications or classes of communications:

(ii) information or 1 or more classes of information:

(iii) 1 or more things or classes of things:

(e) requesting the government of, or an entity in, another jurisdiction to carry out an activity that, if carried out by an intelligence and security agency, would be an unlawful activity:

(f) taking any action to protect a covert collection capability:

(g) any human intelligence activity to be carried out for the purpose of collecting intelligence, not being an activity that—

(i) involves the use or threat of violence against a person; or

(ii) perverts, or attempts to pervert, the course of justice.

53 Sections 68 and 69 provide for the actions that the agencies can carry out to give effect to an intelligence warrant. They confer powers to:

a) enter any place, vehicle or thing as authorised by the warrant along with associated powers of search;

b) install, use and maintain visual surveillance, tracking and interception devices;

c) access information infrastructures; and

d) conceal activities associated with the exercise of a warrant.

Unauthorised, irrelevant and incidentally obtained information

54 Sections 102–104 deal how information can be used if that information was obtained:

a) outside the scope of an authorisation or authorised activity (called "unauthorised information"); or

b) within the scope of an authorised activity but which is not, or is no longer, required by the agency for the purposes of its functions (called "irrelevant information").

55 Unauthorised information should be destroyed unless a warrant is obtained authorising the collection of the information or the information can be disclosed under section 104 to New Zealand Police, the New Zealand Defence Force or another public authority (in New Zealand or overseas).[211] Information can be disclosed under section 104 to prevent or detect serious crime or mitigate threats to life or the security or defence of New Zealand or any other country.[212]

56 Irrelevant information should be destroyed (see 14.10 Other issues, difficulties and uncertainties with the Act).[213]

14.7 The limited statutory mandate of the Department of the Prime Minister and Cabinet

57 Sections 233 and 234 set out the functions of the Chief Executive of the Department of the Prime Minister and Cabinet in respect of intelligence collection, analysis and assessment. Relevantly, section 233(1) and (2) provide:

> (1) The Chief Executive of the [Department of the Prime Minister and Cabinet] is responsible for the performance of the following functions:
>
> (a) providing intelligence assessments on events and developments of significance to New Zealand's national security, international relations and well-being, and economic well-being to—
>
> (i) Ministers; and
>
> (ii) departments; and
>
> (iii) any other person who the Chief Executive of the [Department of the Prime Minister and Cabinet] considers appropriate; and
>
> (b) advising Ministers on the setting of priorities for intelligence collection and analysis; and
>
> (c) advising departments on best practice in relation to the assessment of intelligence.
>
> (2) However, the Chief Executive of the [Department of the Prime Minister and Cabinet] must not carry out the functions specified in subsection (1)(a) and (c) personally but must designate an employee of the [Department of the Prime Minister and Cabinet] to carry out those functions.

[211] Intelligence and Security Act 2017, section 102(2).

[212] Intelligence and Security Act 2017, section 104(3).

[213] Intelligence and Security Act 2017, section 103.

58 This section provides the legislative underpinning for the operation of the National Assessments Bureau (see Part 8, chapter 4) and the role of the Department of the Prime Minister and Cabinet in the development of National Security and Intelligence Priorities.

59 In relation to the functions prescribed by section 233, the Act imposes a duty under section 234 on the Chief Executive of the Department of the Prime Minister and Cabinet to act independently.

14.8 The extent to which the Act authorises bulk collection and acquisition of data

What is bulk collection and acquisition?

60 In the aftermath of the Snowden revelations (see Part 8, chapter 2), there has been substantial debate, in New Zealand and elsewhere, about the appropriateness of intelligence and security agencies being able to collect directly ("collection") or obtain from third parties ("acquisition") large quantities of data (which may include, but is not confined to, communications). In this context, "bulk" is usually used in contrast to "targeted".

61 The key feature of bulk collection and acquisition is that a large proportion of the data gathered relates to people who are not intelligence targets and is of no intelligence value. At its most narrow, targeted collection and acquisition may be directed at a single individual, but it may also extend to groups of people or organisations who share a common purpose. Such collection and acquisition is sometimes referred to as "thematic".

62 The language of all of this is very imprecise. Thematic collection and acquisition may occur on a scale that results in the capture of data that is predominantly of no or limited intelligence value. Even with far more targeted collection and acquisition there is often a possibility of acquiring irrelevant data. And likewise, bulk collection will always be targeted to some extent.

63 These concepts are discussed in detail by Lord Anderson of Ipswich KBE QC in the 2016 *Report of the Bulk Powers Review* and, in the New Zealand context, in a 2018 report by the Inspector-General of Intelligence and Security, *Complaints arising from reports of the Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009–2015*.[214] As the latter report indicates, the Government Communications Security Bureau does not use the expression "bulk collection". It is likewise a concept that is not referred to specifically in the Act.

[214] David Anderson *Report of the Bulk Powers Review* (August 2016); Office of the Inspector-General of Intelligence and Security *Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009–2015* (July 2018).

64 Bulk data can play an important part in identifying, understanding and averting threats. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower. The *Report of the Bulk Powers Review* notes:

> *[W]hile intelligence agencies in the UK and elsewhere have access to more communications data than ever before, by using focused queries and data filters, intelligence analysts only need to retrieve and analyse a small fraction of the overall dataset. As with Google, having more data improves the quality of your results. Intelligence analysts can get the data they need comparatively quickly and efficiently.*[215]

65 This was not to reject the importance of targeted collection. On the contrary, "analysis of bulk communications data and focused data collection on 'targets of interest' serve different but complementary purposes".[216]

66 Bulk collection may involve, but is not confined to, interception of all communications (including associated metadata) as they pass between certain communication links (or bearers). The communications collected will be filtered so as to remove communications that are unlikely to be of intelligence value, with what is left subject to queries (selectors) producing a body of data that is able to be examined (with the balance discarded). Collection of this kind, in which the data obtained is stored before being filtered, has been referred to within the Government Communications Security Bureau as "full take". A variant of this process involves the use of selectors at the point of, and just after, interception but before storage.

67 Other countries rely heavily on this method of intelligence collection. In the United Kingdom just under half of all Government Communications Headquarters intelligence reporting is based on data obtained under bulk interception warrants. For counter-terrorism intelligence reporting, this figure rises to over half.[217]

68 Intelligence and security agencies may wish to acquire data that has been collected or generated by other agencies, financial service providers and telecommunication network operators. Such acquisition may be in bulk or alternatively targeted at a particular individual or group of individuals.

[215] David Anderson, footnote 214 above at paragraph 3.75, page 67.

[216] David Anderson, footnote 214 above at paragraph 3.75, page 67.

[217] David Anderson, footnote 214 above at paragraph 5.9, page 82.

The Cullen-Reddy Report

69 The 2016 Cullen-Reddy Report recommended the introduction of "purpose-based warrants":

> *While we recommend providing for purpose-based authorisations in appropriate circumstances, the legislation should contain a presumption in favour of targeted authorisations. The Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, would only be able to issue a purpose-based authorisation where satisfied it is necessary and proportionate in the circumstances, and that the outcome sought could not reasonably be achieved through the use of targeted authorisations. The Attorney-General could also impose restrictions and conditions on authorisations. This would help to avoid the proliferation of overly broad authorisations, while still allowing the Agencies sufficient flexibility to perform their functions effectively.*[218]

70 Given the context of the part of the Report in which this recommendation was made (including mention of then proposed United Kingdom legislation providing for bulk collection), this recommendation appears to have contemplated authorisation of similar collection by New Zealand agencies.

The Intelligence and Security Bill (158-1)

71 Clause 64 of the Intelligence and Security Bill (158-1) provided for purpose-based warrants – that is, warrants "for a purpose specified in the warrant and for reasons specified in the warrant" that did not describe "the persons in respect of whom, or the places at which, the activities will be undertaken". This clause, however, did not survive the Parliamentary process. The advice of the Department of the Prime Minister and Cabinet on this clause was in these terms:

> *[The Department of the Prime Minister and Cabinet] has worked with the [Government Communications Security Bureau] and the [New Zealand Security Intelligence Service] to test operational examples. The agencies are of the view that, as the Bill is framed, they can achieve the operational ends sought through regular class-based warrants. As such, there is no operational justification for retaining provision for purpose-based warrants.*
>
> *We note also the submissions which allege purpose-based warrants were a means to "mass surveillance." We remain of the view that purpose-based warrants could not authorise mass surveillance – purpose-based warrants were included on the same basis they were recommended by the independent reviewers.*[219]

[218] Hon Sir Michael Cullen KNZM and Dame Patsy Reddy DNZM, footnote 38 above at page 107.

[219] Department of the Prime Minister and Cabinet *New Zealand Intelligence and Security Bill: Departmental Report to the Foreign Affairs, Defence and Trade Committee from Department of the Prime Minister and Cabinet* (December 2016) at pages 568–569.

72 The rationale for dropping clause 64, as explained by the Select Committee, was:

> *We received advice from officials that Type 1 and Type 2 warrants can meet the agencies' operational needs without the need for purpose-based warrants. The regular warrants also provide more safeguards, greater legal certainty, and more effective oversight. Therefore, we see no operational justification for retaining the provision for purpose-based warrants, and we recommend deleting clause 64.*[220]

Bulk collection under the Act

73 Activities that, under section 67, can be authorised by an intelligence warrant include collection focused on "persons or classes of person," "places or classes of places" and "things or classes of things". If construed literally, this language is sufficiently broad to cover bulk collection. Indeed, one of the reasons why the purpose-based warrant proposal did not proceed was the availability of class warrants.

74 The primary constraint on obtaining warrants authorising bulk collection is the necessary and proportionate requirement, which must be applied in the context of the Act. This context encompasses the absence of explicit bulk collection powers – in contrast to those provided for in the Investigatory Powers Act 2016 (United Kingdom) – and the legislative history that indicates a distinct unwillingness to contemplate anything smacking of mass surveillance. And, as we will explain, the Inspector-General of Intelligence and Security's position has been that "general warrants" are not appropriate.

75 The application of the necessary and proportionate requirement will depend on the intelligence purpose on which the agencies rely. If the purpose is broad, for example to enable an intelligence and security agency to obtain an understanding of a new phenomenon, collection on a broad basis may be necessary and proportionate. If, on the other hand, the purpose is to identify potential terrorists and thus link data and communications to identifiable individuals, broad collection may be more difficult to justify.

Bulk acquisition under the Act

76 On the face of it, the direct access sharing provisions (sections 124–133) appear to contemplate bulk data acquisition. However, the Government Communications Security Bureau uses the direct access agreements primarily to ascertain whether a person is a New Zealander. For the New Zealand Security Intelligence Service, direct access agreements are used to obtain useful information, but not in the form of bulk data acquisition. So, in practice, the direct access agreements do not provide a mechanism for the agencies to engage in bulk acquisition.

[220] Intelligence and Security Bill 2016 (158-2) (select committee report) at page 6.

77 The business records direction regime under sections 143–155 does not provide for bulk acquisition as a business records direction must relate to an identifiable person or thing. Likewise, sections 121–122, which provide for intelligence and security agencies to request other agencies to provide information, do not contemplate bulk collection. That this is so is apparent from the report of the Inspector-General of Intelligence and Security titled *2016–17 Review of NZSIS requests made without warrants to financial service providers: Report*.[221]

14.9 The relationships between the Inspector-General of Intelligence and Security and the agencies

78 We heard that the intelligence and security agencies have cultures of compliance. For instance, an internal operational review of the New Zealand Security Intelligence Service that was substantially completed, but not finalised, before 15 March 2019 noted a "widespread perception" amongst operational staff that "leadership messaging was dominated by the importance of compliance (and the perils of non-compliance), to the exclusion of operational ambition". The report noted that this perception had been tempered by a speech made by the Director-General of Security in February 2019, but went on to say:

> *Operational teams were not confident in their judgements on procedure (or policy, or principles), as they believed that they had reassured oversight on certain compliance matters, but subsequent written reports had painted a bleaker picture of their compliance.*
>
> *These conclusions had been accepted, and not contested by, [the New Zealand Security Intelligence Service], thereby emphasising the sense of uncertainty among operational decision-makers.*

79 It would not have been a productive use of our time to investigate all areas of dispute between the agencies and the Inspector-General of Intelligence and Security with a view to determining whether the leadership teams of the agencies had appropriately pushed back against any adverse views. They certainly did on some occasions. And some issues of contention were referred to the Solicitor-General for determination.

80 The Inspector-General of Intelligence and Security's views are not presumptively authoritative, and the agencies are not obliged to act in accordance with findings and recommendations. The agencies are, however, acutely aware of their limited social licence and take adverse reports (which might detract from that social licence) very seriously.

81 The Inspector-General of Intelligence and Security is the primary oversight body of the agencies. A degree of tension is, therefore, both expected and necessary. The independence of the Inspector-General of Intelligence and Security from the agencies is critical to the social licence (limited as it is) that the agencies currently have. This independence might be compromised by close and proactive engagement with agencies.

[221] Office of the Inspector-General of Intelligence and Security *2016–17 Review of NZSIS requests made without warrants to financial service providers: Report* (November 2018).

82 All of that said, our discussion with the agencies and the current Inspector-General of Intelligence and Security suggests that there are issues – for instance in relation to warrants for target discovery purposes – where misconceptions have arisen that could be resolved by closer engagement. Such engagement would enable points on which there is substantial agreement to be resolved. It would also facilitate issues on which there is disagreement to be identified quickly, rather than more painfully in after-the-fact adverse reports. If necessary, disputes as to such issues could be settled authoritatively and promptly by the Solicitor-General.

14.10 Other issues, difficulties and uncertainties with the Act

83 We have identified further issues with the Act as it affects the counter-terrorism effort:

a) A lack of congruence between the Act and the structure and operation of the New Zealand Intelligence Community.

b) The application of the necessary and proportionate test to actions that do not require authorisation.

c) Direct access agreements having not been put in place as contemplated by Parliament.

d) Specificity requirements for warrants.

e) Type 2 warrants and the incidental collection of information about New Zealand citizens and permanent residents.

f) Absence of a legal requirement to enable activity authorised by a warrant.

g) Searches of existing holdings.

h) Accessing existing holdings of partner agencies.

i) The possible effect of section 19 in limiting target discovery in respect of right-wing extremism.

j) The operation of section 103.

k) The definition of "employee".

A lack of congruence between the Act and the structure and operation of the New Zealand Intelligence Community

84 The Act operates primarily to regulate and authorise the activities of the agencies and a more accurate short title might have been "The Intelligence and Security Agencies Act". It says very little about the Department of the Prime Minister and Cabinet. There is, for instance, no explicit mention of the National Assessments Bureau (albeit that function is covered by section 233(1)(a)) and no substantial underpinning in the Act of the leadership and coordination role of the Department of the Prime and Cabinet (see Part 8, chapter 3).

85 The result of the lack of legislative guidance is that there is a dissonance between the role the Department of the Prime Minister and Cabinet has in the counter-terrorism effort and the very limited role identified in the Act.

The application of the necessary and proportionate test to actions that do not require an authorisation

86 As we have explained, a necessary and proportionate test applies to the issue of warrants. This test is applied when a warrant application is considered and thus ahead of any action taken. Agencies can, therefore, take comfort in the fact that the conduct has already been deemed to be necessary and proportionate. In turn, agencies are not required to turn their minds to this test again (unless they wish to engage in activities that fall outside the scope of the original warrant).

87 By way of contrast, there is no prior approval mechanism for activities that are lawful. Therefore, an operation that relies on (or largely relies on) lawful activities will need to be assessed for necessity and proportionality as it progresses. This is because actions that an agency wishes to carry out which are lawful are practically required to be confined to what may later have to be justified to the Inspector-General of Intelligence and Security as necessary and proportionate. Such a process may prove to be cumbersome, particularly if there are time constraints.

88 We discussed with staff of the counter-terrorism agencies whether and how they would have investigated the Facebook posts made by the individual under the username Barry Harry Tarry, if they had come to their attention (see Part 6, chapter 4). An issue was raised whether inquiries at the individual's gym would have met the necessary and proportionate test. Such inquiries may have resulted in the gym manager and/or other gym members learning that a particular member was a person of national security interest. There were concerns whether, on the material assumed to have been at hand, that consequence could have been justified as proportionate.

Direct access agreements having not been put in place as contemplated by Parliament

89 The New Zealand Security Intelligence Service has entered into only a limited number of the types of direct access agreements that are permitted under the Act.

90 There are considerations of principle and practicability that mean that an agreement between the relevant intelligence and security agency and the other agency is a practical prerequisite to an effective data sharing arrangement. So it is difficult to see any alternative to a structure broadly along the lines of that presently provided for in the Act. That said, progress towards the finalisation of direct access agreements has been limited. There are currently no mechanisms to encourage other agencies to enter into such agreements.

91 Adding a statutory requirement to report on progress might assist with speeding up these processes.

Specificity requirements for warrants

92 The rationale of intelligence warrants is to enable the collection of information that is of utility to the agencies in the performance of their functions under the Intelligence and Security Act. Associated with this, the activities that may be authorised by an intelligence warrant are expressed in section 67 in general terms, for instance surveillance on "persons or classes or persons", "places or classes of places" and "things or classes of things".

93 There is no evidential threshold in the Act comparable to the criminal law concepts of reasonable grounds to suspect or believe, provided for in the Search and Surveillance Act 2012.[222] These usually apply to the investigation of offending that has been, or is being, committed. Instead, under the Intelligence and Security Act, agencies must show that:

a) "the activity is necessary to contribute to the protection of national security" (for Type 1 and 2 warrants);

b) "the activity identifies, enables the assessment of, or protects against … terrorism or violent extremism" (for Type 1 warrants); and

c) the necessary and proportionate test is satisfied.

94 Although some intelligence warrants are about the activity of identified individuals and specific suspicions about their activities (and in these respects have some similarities to warrants under the Search and Surveillance Act), others are thematic in character.

95 The Inspector-General of Intelligence and Security has taken the view that, when a warrant proposes to target a class of people, it "must be tolerably clear who will fall within the class and who will not".[223] What this means in practice is that where a Government Communications Security Bureau warrant authorises an activity that targets a class of people that is "so wide or loose" that it is "impossible to tell with any certainty who falls within it", the Inspector-General of Intelligence and Security will likely find the warrant to be irregular.[224] The Government Communications Security Bureau now sets out in warrant applications, with as much specificity as possible, those who fall within the scope of the proposed activity and therefore can be targeted.[225]

[222] A "reasonable grounds to suspect" criterion does feature in section 59(2) of the Act in relation to warrants relating to the "economic well-being" of New Zealand.

[223] Office of the Inspector-General of Intelligence and Security *Warrants Issued under the Intelligence and Security Act 2017: Report* (December 2018) at page 109.

[224] Office of the Inspector-General of Intelligence and Security, footnote 223 above at page 115.

[225] Office of the Inspector-General of Intelligence and Security, footnote 223 above at pages 117 and 119.

96 There has also been dispute between the Government Communications Security Bureau and the Inspector-General of Intelligence and Security about what approach should be taken to whether a warrant authorising activity directed towards a class of persons authorises collection activity against a particular target. The Government Communications Security Bureau has taken the view that where a warrant authorises activity against a person or class of people, it may target an individual if it reasonably *suspects* that the individual is a member of that class.[226] The Inspector-General of Intelligence and Security is of the view that, in those circumstances, the Government Communications Security Bureau must have a reasonable *belief* that those intended to be targeted are within the class.[227] In individual instances, this dispute must be determined against the definition of the target class in the warrant. And, as the Inspector-General of Intelligence and Security has recognised, a warrant could define a class by reference to reasonable suspicion, that is "persons reasonably suspected of x".

97 In practice, the approach has largely followed the interpretation of the Inspector-General of Intelligence and Security. That is, the targeting of individuals (whether specifically or as members of a class) requires reasonable grounds to believe that they are engaging in relevant conduct (such as terrorism) or – but only if the warrant is expressed so as to allow this specifically – at least reasonable cause to suspect that they are.

98 Despite this issue being largely resolved, another issue has emerged. The agencies told us that the Inspector-General of Intelligence and Security is of the view that – at least for Type 1 warrants issued under section 58 – there is a "strict" necessity threshold requiring positive grounds for suspecting a New Zealander's association with the listed harms, below which the agencies cannot obtain a warrant. The agencies told us that they disagreed with this view. In their opinion, section 58 contemplates an activity that "identifies, enables the assessment of, or protects against" any of the listed harms. That threshold, they said, is all that the Intelligence and Security Act requires in terms of authorising target discovery activities (see Part 8, chapter 10).

99 Our impression is that either the agencies have misunderstood the position of the Inspector-General of Intelligence and Security or it has not been conveyed to them clearly. The Inspector-General of Intelligence and Security accepts that, providing agencies meet the statutory requirements in section 58, there is no impediment to the authorisation of target discovery activities. Misunderstandings would be less likely if there was more direct and proactive engagement – particularly involving operational staff from the agencies – along the lines we have earlier indicated.

[226] Office of the Inspector-General of Intelligence and Security, footnote 223 above at page 144.

[227] Office of the Inspector-General of Intelligence and Security, footnote 223 above at pages 145.

Type 2 warrants and the incidental collection of information about New Zealand citizens and permanent residents

100 There is scope for argument about whether a Type 1 warrant is required where the purpose of a proposed activity is not directed at New Zealand citizens or permanent residents but the collection of information about New Zealand citizens or permanent residents is a likely, probable or inevitable consequence of carrying out the activity.[228]

101 The distinction between Type 1 and Type 2 warrants, in some instances, complicates online intelligence gathering where nationality can be difficult to determine or where the scale of collection makes it inevitable that New Zealanders' information will be collected.

102 One option is for the agencies to apply for a Type 1 warrant where there is a likelihood of information about a New Zealander being collected. Another option is to apply for a Type 2 warrant and, where information is collected about a New Zealander, subsequently apply for a Type 1 warrant. Additionally, in some circumstances, given the different requirements of sections 58–60, agencies may be required to apply for three different warrants to cover the same investigation. Requiring the agencies to apply for multiple different warrants for the same investigation imposes considerable administrative burdens.

103 The current distinction between Type 1 and Type 2 warrants rests on the view that New Zealanders should be afforded greater protection from surveillance by New Zealand agencies than foreign nationals. This is why a Commissioner of Intelligence Warrants must approve Type 1 warrants rather than just the responsible minister (thereby providing an additional "lock"). It does not, however, explain why the criteria for the issue of warrants for counter-terrorism purposes should be differently expressed. Given the practical difficulties that the distinction causes, it may be more straightforward to provide for a single category of warrant, at least for counter-terrorism.

Absence of a legal requirement to enable activity authorised by a warrant

104 Although section 51 provides for an intelligence and security agency to request the assistance of New Zealand Police (or other people) to give effect to an authorisation, there is no legal duty on those affected by a warrant to comply with it (unless the requested agency is a network operator or service provider as they have a duty to assist the agencies under section 24 of the Telecommunications (Interception Capability and Security) Act 2013).

105 This is of limited practical effect when the activity authorised is to be carried out in a covert way. It can, however, be of considerable significance where the activity cannot be carried out without the cooperation of a third party.

[228] See Office of the Inspector-General of Intelligence and Security, footnote 223 above at pages 136–142.

Searches of existing holdings

106 Where information has been collected under a Type 2 warrant, current practice is that it will not be searched for information relating to a New Zealand citizen or permanent resident without a Type 1 warrant being held or obtained.

Accessing existing holdings of partner agencies

107 Section 49(2) provides that an intelligence and security agency requires an authorisation before asking a partner agency to carry out an activity that would be unlawful if carried out directly by the New Zealand agency. What is not clear is whether a warrant is required to access information already collected by a partner agency.

108 It is at least arguable that a warrant is required in these circumstances. A request to a partner agency to search its existing holdings may amount to a search for the purposes of section 21 of the New Zealand Bill of Rights Act 1990.

The possible effect of section 19 in limiting target discovery in respect of right-wing extremism

109 As we noted earlier, section 19 is based on a provision first introduced in 1977 into the New Zealand Security Intelligence Service Act 1969. Clause 22 of the New Zealand Intelligence and Security Bill (158-1) was intended to replicate the gist of this part of the 1969 Act:

> (a) Nothing in this Act limits the right of persons to engage in lawful advocacy, protest, or dissent in respect of any matter.
>
> (b) The exercise of the right in subsection (1) does not, of itself, justify an intelligence and security agency collecting intelligence on any person who is in New Zealand or any class of persons who are in New Zealand.

110 The Inspector-General of Intelligence and Security submitted on clause 22 in this way:

> *Section 2(2) of [the New Zealand Security Intelligence Service Act 1969] provides that the [New Zealand Security Intelligence Service] is not justified in "instituting surveillance", while clause 22 states that the intelligence and security agencies will not be justified in "collecting intelligence". The [Inspector-General of Intelligence and Security] is concerned the protection in clause 22 is narrower because "collecting intelligence" could be construed as being limited to collection of intelligence pursuant to an intelligence warrant, whereas "instituting surveillance" could encompass observation undertaken legally without a warrant. The [Inspector-General of Intelligence and Security] considers that lawful advocacy, protest and dissent do not in themselves justify the agencies taking any action at all, and that the Bill should be reworded to capture this.*

111 The Department of the Prime Minister and Cabinet agreed with the Inspector-General of Intelligence and Security's submission and recommended that the words "collecting intelligence" be replaced with "taking any action". As will be apparent, this change is reflected in the wording of section 19.

112 The wording of section 19 gives rise to some difficulties in terms of target discovery. We can illustrate these difficulties by reference to the possible monitoring of far right websites and forums. Bearing on the appropriateness of such monitoring are fact that:

a) a number of people, including those on the far right, use websites and online forums to spread (or receive) divisive hateful rhetoric; and

b) some of those people may be potential terrorists and analysis of what is said on those websites and forums might enable them to be identified; but

c) very little of what is found on such websites and forums (including the divisive and hateful rhetoric) is contrary to the law.

113 Collection and analysis of what is said on those websites and forums can be regarded as involving agency action directed at a group of people targeted because of their exercise of the right to freedom of expression. It is at least open to argument that such collection and analysis would be in breach of section 19. If so, we would not see the problem as able to be resolved by obtaining a warrant, given what we consider to be the purpose of section 19, its legislative history and the effect of other provisions in the Act.

114 A practical example of the issues that may arise is provided by the IP address lead discussed in *Part 6: What Public sector agencies knew about the terrorist*. A major reason why the lead was generated and pursued is that the person using the internet address had accessed extremist material. It is far from clear that, in doing so, that person committed an offence. If accessing the material did not amount to an offence, it follows that such access was within the scope of the right to freedom of expression (which encompasses seeking out the opinions of others). There were other elements to the internet activity (relating to firearms) that were material to the decision to open and pursue the lead. This probably means that the exercise of the right to freedom of expression – that is, accessing extremist material – was not "of itself" the basis for the action that was taken. On the other hand, upstream collection of intelligence about who is accessing what internet material is an activity in itself and one that could engage section 19.

115 There should be proactive engagement between the agencies and the Inspector-General of Intelligence and Security as to the implications of section 19 on target discovery. But such engagement, while likely to be useful, will not authoritatively resolve the potential for major problems with section 19 in the current environment. Difficult though the issues around section 19 will be to resolve legislatively, we see them as warranting urgent consideration by Parliament.

The operation of section 103

116 Section 103(1) and (2) provides:

> **103 Destruction of irrelevant information**
>
> (1) In this section, irrelevant information means information that—
>
> (a) is obtained by an intelligence and security agency within the scope of an authorised activity; but
>
> (b) is not required, or is no longer required, by the agency for the performance of its functions.
>
> (2) Irrelevant information must be destroyed as soon as practicable.

117 Section 103 assumes that relevance and irrelevance are binary concepts – that intelligence is either relevant to the performance of the agencies' functions (in which case it may be retained) or that is irrelevant (in which case it must be deleted). It also assumes that the agencies are in a position to continuously monitor the relevance of information that they hold. Neither assumption is correct. Relevance is a relative concept. The agencies do not have the practical ability to operate a continuous review of the relevance of all information that they hold. And, even if they did, devoting the limited resources of the agencies to such a task may impact their ability to carry out more important functions, such as identifying potential terrorists.

118 Section 103 should be reviewed.

The definition of "employee"

119 The powers of the agencies to give effect to intelligence warrants may be exercised by authorised employees (see sections 68 and 69). The section 4 definition of "employee" does not encompass officials from other agencies seconded to the agencies (including from another intelligence agency). There are number such persons who, in a practical sense, work for the agencies. There is a work-around (involving the use of section 51) but it would be preferable if the definition of "employee" reflected the way in which the agencies are, in practice, staffed.

Chapter 15: Evaluation of the counter-terrorism effort

Distressing Content

15.1 Overview

1 Three of the questions on which we were required by our Terms of Reference to make findings were applicable to the counter-terrorism effort:

> 4(c) whether relevant [Public] sector agencies failed to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats;
>
> (d) whether any relevant [Public] sector agency failed to meet required standards or was otherwise at fault, whether in whole or in part; and
>
> (e) any other matters relevant to the purpose of the inquiry, to the extent necessary to provide a complete report.

2 Underlying these issues is a concern that the relevant Public sector agencies may have missed opportunities to disrupt the 15 March 2019 terrorist attack by, for instance, looking the wrong way. We interpreted these paragraphs as asking, primarily at least, whether the relevant Public sector agencies were at fault in relation to the terrorist attack.

3 We were required to make recommendations about how the counter-terrorism effort could be improved. These recommendations did not need to be tied to (or based on) findings under our Terms of Reference. On the other hand, we would not recommend improvements unless we had concluded that there is scope for improvement. In the case of the counter-terrorism effort, these conclusions are closely related to, and follow on from, our findings. It is logical therefore to examine in this chapter whether there are elements of the counter-terrorism effort that need improvement.

4 In this chapter we:

a) assess whether relevant Public sector agencies failed to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats;

b) assess whether any relevant Public sector agency failed to meet required standards or was otherwise at fault, whether in whole or in part;

c) consider whether any other findings are necessary to provide a complete report on other matters relevant to the purpose of the inquiry; and

d) describe the elements of the counter-terrorism effort that we consider warrant improvement.

15.2 Did relevant Public sector agencies fail to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources or priorities on other terrorism threats?

The issue on which a finding is required

5 In some respects, the question we must answer is narrow:

a) We were not asked to address whether the resources allocated to the counter-terrorism effort were sufficient. We have not looked at allocations between agency work programmes (such as New Zealand Police's counter-terrorism and, say, family violence prevention efforts). We have focused on the counter-terrorism resources of relevant Public sector agencies as they were at the relevant time.

b) The expression "plan for or anticipate the attack" specifically refers to the terrorist attack carried out on 15 March 2019. Had the relevant Public sector agencies planned for or anticipated that terrorist attack, they would have been able to disrupt it. So we see the question as directed at whether the concentration of counter-terrorism resources was material to the terrorist attack not being disrupted.

6 But although narrow in the respects just mentioned, the question requires assessment of the allocation of resources between competing priorities and necessitates consideration of multiple factors involving different choices across various domains and, for those reasons, is polycentric. To such a question, a simple "yes" or "no" answer may not be possible.

7 We have not treated the "resources" and "priorities" as raising separate issues. Instead, we see them as expressing a single idea. In this chapter we use the terminology of concentration of counter-terrorism resources.

8 We focus primarily, although not exclusively, on the period between 2016 and 15 March 2019. 2016 is a sensible starting point for the following reasons:

a) Up until late 2014 there had been New Zealand Police assessments of the extreme right-wing. Although these assessments primarily focused on threats to public order and offending, they did cover national security concerns. The last of these assessments, in late 2014, noted that the far right in New Zealand was characterised by "discord and discoordination" and that experienced far right activists were unlikely to pose a risk to national security over the next three years.

b) In 2015–2016 there was a sharp increase in far right activity internationally, which we see as relevant to whether the Public sector agencies involved in the counter-terrorism effort should have turned their attention towards the threat of extreme right-wing terrorism.

c) 2016 is when the Strategic Capability and Resourcing Review funding was approved (see Part 8, chapter 2). Before that funding becoming available, the New Zealand Security Intelligence Service's capabilities and capacity had degraded so severely that it would be a pointless exercise for us to review its resource allocation decisions.

9 We address the discussion that follows under the following headings:

a) The available counter-terrorism resources.

b) The concentration of counter-terrorism resources on the threat of Islamist extremist terrorism.

c) The reasons for the concentration of resources on the threat of Islamist extremist terrorism.

d) The risk of right-wing extremist terrorism as discernible before 15 March 2019.

e) What the counter-terrorism effort did about the risk of right-wing extremist terrorism.

f) Did the concentration of resources on the threat of Islamist extremist terrorism materially increase the overall risk of terrorism?

g) Was the concentration of resources on the threat of Islamist terrorism a considered decision following an appropriate process?

h) Would any plausible alternative allocation of counter-terrorism resources have resulted in anticipation or planning for the terrorist attack?

i) Our conclusions.

The available counter-terrorism resources

10 As discussed in this Part, a number of Public sector agencies contribute to the counter-terrorism effort.

11 For the purposes of this exercise, we leave the following to one side:

a) The Government Communications Security Bureau. It had only four staff in 2016, two in 2017 and seven in 2018 who were assigned to domestic counter-terrorism. It engaged in counter-terrorism only when specifically tasked by another agency to do so, and had not received any tasking relevant to the issue. It therefore had comparatively little to do with the allocation of counter-terrorism resources.

b) The counter-terrorism unit in New Zealand Customs Service and Immigration New Zealand. The individual did not present as a threat at the border and there is no reason to think that any different focus of counter-terrorism resources at the border would have resulted in disruption of his planning.

c) The Specialist Coordinator and other staff in the National Security Group of the Department of the Prime Minister and Cabinet.

12 Recognising, as we do, that precise delineation of relevant counter-terrorism resources is a little artificial, we think that what is most relevant for the purposes of our finding are the counter-terrorism investigative resources within the New Zealand Security Intelligence Service's Counter-Terrorism Unit and New Zealand Police's National Security Investigation Team. These resources were scarce. As of 2016, the resources of the New Zealand Security Intelligence Service were insufficient to provide for more than partial monitoring of its investigative prioritisation (watch) list targets (see Part 8, chapter 5). The specialist counter-terrorism staff of New Zealand Police were also under pressure. A 2016 budget bid for an increase in New Zealand Police's counter-terrorism funding had been rejected.

13 The numbers of specialised counter-terrorism staff in the New Zealand Security Intelligence Service and New Zealand Police were supplemented by their supervisors. As well, the Counter-Terrorism Unit in the New Zealand Security Intelligence Service could call on the assistance of other staff (for instance collections staff). New Zealand Police's National Security Investigation Team could call on the broader resources of New Zealand Police, including the Security Intelligence and Threats Group, as and when required (and as the priorities of those other staff allowed) although members of that Team were also sometimes called upon for other New Zealand Police purposes.

14 Also relevant, but in a different way, are the National Assessments Bureau and the Combined Threat Assessment Group. The way these assessment agencies viewed their respective roles, and the focus of their efforts, influenced the allocation of domestic counter-terrorism resources within the counter-terrorism agencies.

The concentration of counter-terrorism resources on the threat of Islamist extremist terrorism

15 Counter-terrorism resources were primarily concentrated on the threat of Islamist extremist terrorism. This can be demonstrated by the New Zealand Security Intelligence Service's priority investigation (watch) list. As at 11 March 2019, it included 25 counter-terrorism investigations involving 32 subjects of investigation. All these subjects were under investigation due to their assessed affiliation with Islamist extremism, primarily inspired by Dā'ish.

The reasons for the concentration of resources on the threat of Islamist terrorism

16 There are several interconnected reasons why counter-terrorism resources were concentrated on the threat of Islamist extremist terrorism:

a) Assessments of the Combined Threat Assessment Group and the National Assessments Bureau were primarily focused on Islamist extremist terrorism threats.

b) Before 2015, New Zealand Police had produced assessments on far right individuals and groups in New Zealand but from 2015 the New Zealand Police intelligence function had degraded to the point that it was not producing assessments on the far right.

c) International partner reporting and leads were overwhelmingly focused on Islamist extremism.

d) Islamist extremist terrorism was seen as the presenting threat.

e) There was Limited availability of counter-terrorism resources.

We discuss each of these in turn.

17 From 2010–2019 the intelligence assessments of the National Assessments Bureau and the Combined Threat Assessment Group considered the terrorist threat to New Zealand and New Zealanders as coming largely from Islamist extremism. For example, in July 2015 the Combined Threat Assessment Group assessed that the primary domestic terrorism threat was from "individuals and groups, based in New Zealand but with inspiration from abroad, who subscribe to extreme Islamist ideologies". It did not explicitly mention the threat of terrorism from the extreme right-wing.

18 From 2016 onwards, assessments continued to evaluate Islamist extremism as the primary terrorist threat to New Zealand and New Zealanders. For example:

a) In 2016, a New Zealand Police intelligence report, *New Zealand's Islamist Extremist Landscape,* stated that more New Zealanders are vulnerable to extremist messaging due to the pervasive nature of Dā'ish's propaganda, which had proven more effective at attracting disaffected young males than other extremist groups.

b) The Combined Threat Assessment Group's 2018 assessment of the New Zealand terrorism environment stated that "in spite of ongoing losses in Syria and Iraq, [Dā'ish] will continue to exert itself as a terrorist and insurgent group with international influence and reach … the overall level of support for [Dā'ish] among New Zealand-based Islamist extremists does not seem to have changed markedly … though the manifestation of support for radical Islam continues to evolve".

c) The New Zealand Security Intelligence Service similarly concluded in 2018 that "[Dā'ish's] territorial decline has not had any marked impact on the New Zealand extremist environment".

d) Two papers produced by the National Assessments Bureau in 2018 discussed the "persistent threat from Jihadist terrorism".

19 As of 2016, New Zealand Police's national intelligence function had degraded and no longer produced strategic assessments on the domestic threatscape (see Part 8, chapter 6).

20 International partner reporting was overwhelmingly focused on Islamist extremism. The Government Communications Security Bureau informed us that in the second quarter of the 2018–2019 financial year, it received 7,526 intelligence reports from international partners about terrorism and violent extremism. None of those reports related to right-wing extremism. While international partners do not direct or dictate that New Zealand agencies pursue particular leads or ideologies, partner reporting and partner-supplied leads necessarily informed the development of New Zealand threat assessments and affected the allocation of resources, certainly by the counter-terrorism agencies.

21 Leads received from within New Zealand by counter-terrorism agencies were predominantly about possible Islamist extremist terrorism. A New Zealand Security Intelligence Service report of 5 September 2018 noted an absence of indications of terrorist threats from non-Islamist extremist sources. In part this may have resulted from the leads-based investigative model employed by New Zealand Security Intelligence Service which, because of its focus on Islamist extremism, was not calibrated so as to generate leads associated with other ideologies (see Part 8, chapter 10).

22 There were many tangible leads and a substantial number of persons of interest with an Islamist extremist outlook. As well, there were numerous active domestic investigations and operations focused on Islamist extremist activity that posed real threats to public safety in New Zealand. We have seen evidence that New Zealand Police and the New Zealand Security Intelligence Service achieved some success in mitigating such threats. For example, between August 2015 and January 2018, eight passports were cancelled, and New Zealand Police arrested 17 individuals of national security interest for a variety of offences and issued 40–50 warnings for extremism-related objectionable material.

23 The primary explanation given by the counter-terrorism agencies for not making earlier efforts to understand the threat of extreme right-wing terrorism is that their limited resources were substantially tied up dealing with the presenting threat of Islamist extremist terrorism.

24 From at least early 2016, it was appreciated by the New Zealand Security Intelligence Service there was a potential for terrorism from non-Islamist extremist sources and that it was largely unsighted to the nature and extent of such threats. This is referred to in a February 2016 Strategic Capability and Resourcing Review Cabinet paper, which identified the expected capacity increase in relation to countering violent extremism:

> *The capability increases from a current state where partial monitoring of watch-list targets is possible and there is minimal coverage outside Auckland, to a future where there is a New Zealand-wide baseline threat picture.*

25 Baselining emerging terrorist threats was ranked as the third goal in the New Zealand Security Intelligence Service's 2016 *10-Year Operational Strategy*,[229] but its ranking meant that work on it was deferred. As events turned out, the New Zealand Security Intelligence Service did not have enough counter-terrorism staff to start its baselining project until May 2018.

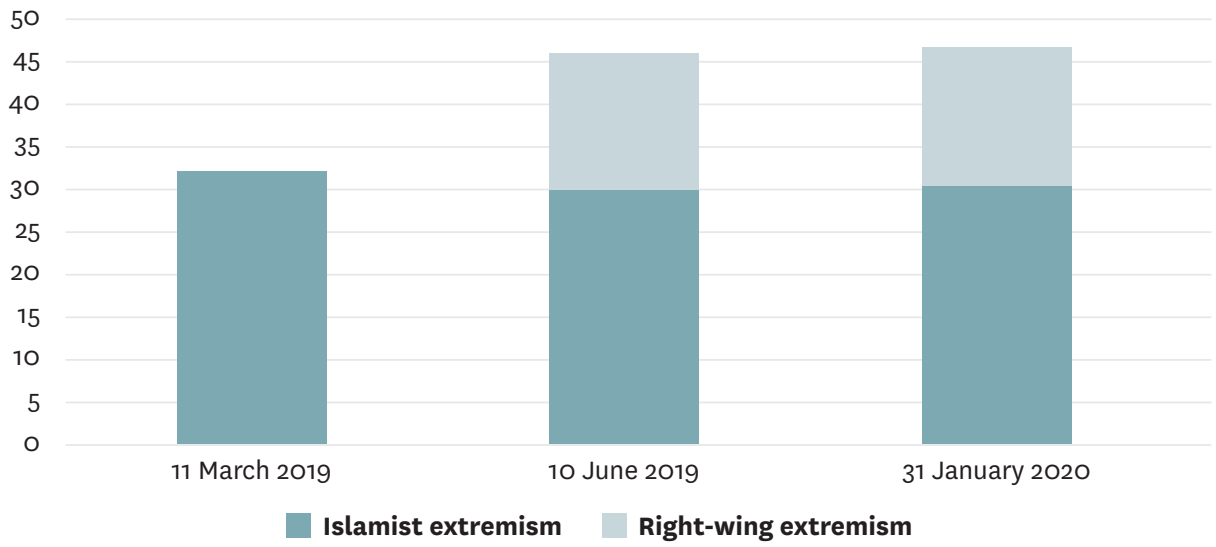
The threat of right-wing extremist terrorism as discernible before 15 March 2019

26 What has become apparent after the terrorist attack has shown that, before 15 March 2019, there were national security threats from right-wing extremists, at least some of which would have been be likely to have come to light if the concentration of counter-terrorism resources had been different. We know this because some of the new extreme right-wing leads that were opened after 15 March 2019 (as a result of the counter-terrorism agencies reviewing their existing holdings and through public or partner reporting) met the threshold for investigation. This deserves a brief explanation.

27 On 10 June 2019, the New Zealand Security Intelligence Service's watch list included 28 counter-terrorism investigations involving 46 subjects of interest. Twenty-four of the investigations (involving 30 subjects of interest) related to Islamist extremism. The remaining four investigations (involving 16 subjects of interest) involved right-wing extremism. On 31 January 2020 the watch list included 34 counter-terrorism investigations, comprising 47 subjects of investigation. Of these, 20 investigations (involving 31 subjects of interest) related to Islamist extremism, while 14 investigations (involving 16 subjects of interest) involved right-wing extremism. These can be compared to the corresponding figures at 11 March 2019, discussed above and shown in the figure below.

[229] New Zealand Security Intelligence Service, footnote 55 above.

Figure 47: Number of subjects of interest in New Zealand Security Intelligence Service counter-terrorism investigations, by associated ideology (March 2019–January 2020)



28 What all this means is that, before 15 March 2019, there was activity in New Zealand involving individuals with extreme right-wing ideologies who were of national security interest. This is not surprising.

29 Before 15 March 2019, there had been many extreme right-wing terrorist attacks in Canada, the United Kingdom and the United States of America, which showed that ideological thinking along the lines of the Great Replacement had the capacity to motivate some people to extreme violence. Right-wing extremist terrorism was exemplified by the Oslo terrorist's attack in 2011, several mass shootings at places of worship in Europe and North America between 2012–2018 and a planned extreme right-wing attack in Australia that was disrupted in 2016 (see Part 8, chapter 2). In short, global events showed that right-wing extremism was a known phenomenon, with substantial potential lethality, was not confined to a single jurisdiction, had been around for a number of years and fed off a number of drivers to which New Zealand could not claim to be immune (including racism, Islamophobia, poverty, growing inequality, the radicalising role of the internet and immigration).

30 The Australian Security Intelligence Organisation recently confirmed that right-wing violence now occupies 30 to 40 percent of its counter-terrorism cases, up from 10 to 15 percent in 2016.[230]

[230] Maani Truu "Threats from far-right extremists take up between 30 per cent and 40 per cent of ASIO's resources, up from only 15 per cent half a decade ago" *SBS News* (Australia 22 September 2020) https://www.sbs.com.au/news/threats-from-far-right-extremists-have-skyrocketed-in-australia-with-asio-comparing-tactics-to-is.

31 Right-wing groups have been active in New Zealand for many decades. Associated with this have been at least three hate crime murders (committed by members of the Fourth Reich, a right-wing gang). And while other right-wing groups have been seen primarily as posing threats to public order, the underlying thinking of their supporters meant that they would be receptive to the ethno-nationalist ideas (see Part 2, chapter 5), that were starting to achieve considerable global currency by 2015–2016.

32 Although cultural controversies involving immigration have not been as acute in New Zealand as in some other Western countries, there were several issues in New Zealand that had the potential to galvanise those on the extreme right-wing. These included provocative statements made by some in public life about race relations, Te Tiriti o Waitangi and the nature of Islam. As well, as survey data shows, New Zealanders generally feel "less warmth" towards Muslim communities than other groups.[231]

33 Members of Muslim communities were concerned about risks of right-wing extremist terrorism. We have discussed the detail of this in *Part 3: What communities told us* and *Part 9: Social cohesion and embracing diversity.* As expressed, these concerns tended to be closely associated with worries about discrimination, Islamophobia, hate speech and hate crime and often did not clearly relate to national security. Nonetheless they reflected community concerns that warranted attention and reassurance from counter-terrorism agencies, or other relevant Public sector agencies, if that could be provided legitimately.

34 The easy availability of firearms of high lethality was recognised in the 1997 Thorp Report.[232] In 2011 the Combined Threat Assessment Group concluded that a terrorist could legally acquire firearms for use in an attack (see Part 8, chapter 4). In 2014, a New Zealand Police assessment commented on the propensity of the extreme right-wing to acquire and use firearms.

The counter-terrorism effort and right-wing extremist terrorism

35 The threat posed by the extreme right-wing in New Zealand was briefly mentioned in some assessments (see Part 8, chapter 4).

36 Before 2015, New Zealand Police had produced assessments on far right individuals and groups in New Zealand. Although these were primarily about threats these individuals posed to public order or general offending, national security concerns were addressed in two assessments in 2014. One of these assessments noted that right-wing extremists were unlikely to pose a risk to national security over the next three years.

[231] Chris G Sibley, M Usman Afzali, Nicole Satherley, Anastasia Ejova, Samantha Stronge, Kumar Yogeeswaran, Michael Grimshaw, Diala Hawi, Zahra Mirnajafi, Fiona Kate Barlow, Petar Milojev, Lara M Greaves, Sarah Kapeli, Elena Zubielevitch, Logan Hamley, Maria C Basabas, Marvin H Wu, Chloe Howard, Carol HJ Lee, Yanshu Huang, Christopher Lockhart, Joaquín Bahamondes, Sam Manuela, Taciano L Milfont, Ryan Perry, Nikhil K Sengupta, Nickola C Overall, John H Shaver, Geoffrey Troughton, Danny Osborne and Joseph Bulbulia *Prejudice toward Muslims in New Zealand: Insights from the New Zealand Attitudes and Values Study* (July 2020).

[232] Sir Thomas Thorp KNZM *Review of Firearms Control in New Zealand: Report of an Independent Inquiry Commissioned by the Minister of Police* (Thorp Report) (Government Printer, June 1997).

37 In January 2018 the Combined Threat Assessment Group's *New Zealand Terrorism Threatscape* noted that:

> *Open source reporting indicates the popularity of far right ideology has risen in the West since the early 2000s. Since 2014, the 'new' right-wing movements have been strengthened by opposition to refugee settlements and Islamist extremist attacks in the West, especially in Europe and Scandinavia.*
>
> *[The Combined Threat Assessment Group] has not sighted any reporting to indicate [established New Zealand far right groups have] the intent or capability to promote their ideology by an act of terrorism. As has been evidenced in similar jurisdictions to New Zealand, an extreme right-wing lone actor attack remains a possibility, albeit a remote one.*
>
> ...
>
> *We also note that Islamist extremist attacks in other Western countries have provoked retaliatory attacks from individuals with other ideologies, such as extreme right-wing groups. [The Combined Threat Assessment Group] assesses that this could occur in New Zealand following any terrorism incident.*

38 During the first half of 2018 (before the New Zealand Security Intelligence Service started its project to establish a baseline picture of emerging domestic terrorism threats), there were several Combined Threat Assessment Group briefing notes that referred to the threat of extreme right-wing terrorism in similar but more limited terms.

39 The National Assessments Bureau's first comment on the terrorist threat from the extreme right-wing in New Zealand was in September 2018 in its *Global Terrorism Update*. In an annex to the main assessment is a small section on "extreme right terrorism" in which the National Assessments Bureau observed that "between 12 September 2001 and 31 December 2016 in the United States of America, there were more extreme-right incidents than Islamist terrorist incidents resulting in fatalities". It concluded that there had been an emerging global threat from extreme right-wing terrorism for some time, but groups were fragmented with limited international coordination. The assessment went on to note that:

> *Extreme-right-wing groups are present in New Zealand and have an online presence, but have not been active. Extreme-right groups differ from far right groups in the fact that the extreme-right is willing to use terrorism to further their aims. There has been no evidence to suggest New Zealand-based far right groups have the intent or capability to promote their ideology by an act of terrorism.*

40 We have seen a few reports and assessments prepared by Public sector agencies including the Department of Corrections and New Zealand Customs Service that refer to the extreme right-wing as a possible (but unsighted) domestic threat, with the potential for violence. A New Zealand Police national security situation update in May 2018 specifically noted that Muslim communities in New Zealand could be the target of such threats.

41 Leads on the extreme right-wing were received occasionally and, when received, were pursued. These include the IP address lead, which we have discussed in some detail in Part 6, chapter 3.

42 New Zealand Customs Service and New Zealand Police had developed some limited training material for front-line staff that was focused on the extreme right-wing (see chapter 17 of this Part).

43 The New Zealand Security Intelligence Service produced one report in 2011 that referred to the national security threat from the extreme right-wing. It produced several more such reports in 2018. No reports were published in the intervening period (2012–2017).

44 New Zealand Police and the New Zealand Security Intelligence Service held a tabletop exercise in October 2018 to increase understanding of their respective processes and procedures in Response to a counter-terrorism incident. One of the scenarios drew on the Finsbury Park Mosque terrorist attack. The scenario played out the Response that Public sector agencies would take to a report of a lone actor vehicle terrorist attack on worshippers leaving the Masjid an-Nur in Christchurch (see Part 8, chapter 4).

45 Although we have recorded what may appear to be a good deal of activity, the reality is that counter-terrorism resources were primarily concentrated on the threat of Islamist extremist terrorism.

46 The 2019 Arotake Review noted:

> *[The New Zealand Security Intelligence Service's] work on the extreme-right-wing in New Zealand remained at its early stages at the time of the 15 March 2019 attacks. After a long period without focus on this complex area, [the New Zealand Security Intelligence Service] was seeking to develop an understanding of the key ideologies, groups, individuals involved, their propensity to violence, and operational techniques, despite being only able to devote limited resources committed to the task.*

47 We agree with this judgement. As far as the New Zealand Security Intelligence Service was concerned, there was a developing but still limited understanding of the threat of right-wing extremism in New Zealand as at 15 March 2019. Broadly similar considerations apply to New Zealand Police, whose work on right-wing extremism had only just started by 15 March 2019.

Did the concentration of resources on the threat of Islamist extremist terrorism materially increase the overall risk of terrorism?

48 An increased concentration of counter-terrorism resources on the extreme right-wing was not likely to have materially increased the likelihood of the individual's preparation being disrupted. We explain why later in this chapter.

49 If the counter-terrorism agencies' scarce counter-terrorism resources had, earlier than May 2018, been diverted away from the presenting threat of Islamist extremist terrorism towards, say, developing a better understanding of emerging threats from other ideologies, there are a range of possible outcomes. It may have led to an increase in the risks associated with Islamist extremist terrorism, due to a reduction in the effort to mitigate those risks. It may also have led to a decrease in the risks of extreme right-wing terrorism, due to a better understanding and mitigation of the threat. Neither side of that equation can be precisely assessed.

50 It is not possible to determine with confidence whether the overall risk of domestic terrorism would have been increased or decreased had counter-terrorism resources been allocated earlier to the threat of right-wing extremist terrorism. An attempt at such determination would have required detailed consideration of each of the investigation prioritisation (watch) list targets and the threats they presented and the extent to which diversion of effort would have increased the risk they posed. Also required would have been a comparable assessment of the extent to which the risk of extreme right-wing might have been mitigated by an earlier diversion of effort.

51 This exercise would at best produce a very speculative conclusion, though this is not to say a risk management framework is not required for prospective allocation of scarce resources, a point which we will come back to shortly. But more significantly the exercise would have turned the focus of our inquiry away from the actions of Public sector agencies to one which includes surveillance targets within our communities. We do not see this as consistent with our Terms of Reference.

Was the concentration of resources a considered decision following an appropriate process?

52 Another way to assess the appropriateness of the concentration of counter-terrorism resources is to consider the process undertaken in relation to the allocation of counter-terrorism resources. In this approach, the concentration of counter-terrorism resources on threats of Islamist extremist terrorism to the substantial exclusion of other threats could be justified only on the basis of either:

a) an informed assessment of the threats of terrorism associated with other ideologies; or

b) a system-wide decision that, despite the absence of such an assessment, counter-terrorism resources should continue to be allocated almost exclusively to the threat of Islamist extremist terrorism.

53 In the period between 2016 and May 2018 there was not an informed assessment of the threats of terrorism associated with ideologies other than Islamist extremism. The only relevant assessments are the Combined Threat Assessment Group assessments of July 2015 and January 2018, the relevant parts of which we have set out above.

54 The Combined Threat Assessment Group's July 2015 *New Zealand Terrorism Threatscape* assessment that Islamist extremist terrorism was the primary terrorist threat could be taken to imply that other threats had been assessed. As far as we can tell, this was not the case. And the January 2018 assessment, while accurate as far as it went (in its reference to not having sighted reporting), could be taken to imply more in the way of an evidence-based assessment than had actually been carried out. This is particularly so in relation to the comment that the possibility of an attack by an extreme right-wing lone actor was "remote".

55 The National Assessments Bureau's *Global Terrorism Update* of September 2018 stated, "[t]here has been no evidence to suggest New Zealand-based far right groups have the intent or capability to promote their ideology by an act of terrorism". This was literally true as there was, at the time, no such evidence. The statement, however, could be taken to imply that there had been more effort to look for such evidence than had been the case.

56 It is of interest to compare these assessments with the December 2018 *New Zealand Terrorism Update* issued by the New Zealand Security Intelligence Service (see Part 8, chapter 4). We reproduce the key passage of the report here for ease of reference:

> *Non-Islamist terrorist threats from extreme political, religious and issues-motivated groups are plausible in New Zealand, especially given heightened political partisanship internationally and the spread of disinformation online. Various radical groups are present in New Zealand, some of which have extreme elements that could plausibly turn violent; however, terrorist acts by them are currently not expected.*
>
> ...
>
> *The spread of highly partisan political content online, especially over social media, has almost certainly contributed to acts of non-Islamist extremist violence in Western countries. Several attempted and realised attacks in the United States in 2018 were linked to extreme right-wing, conspiratorial, or racist agitation in social and other media, judging from press reporting.*

57 The more general problem, as we see it, is that the two key assessment agencies were not well situated to provide assessments of emerging threats. In the case of the National Assessments Bureau, this was a result of its customer focus and its limited resources. In the case of the Combined Threat Assessment Group this was due to both its short term and tactical focus and also the negative reaction from other agencies to its

reporting on the 2011 Oslo terrorist's attack and its firearms assessment of 2011 due to a perception it was stepping outside of its mandate. This firearms assessment had judged that a terrorist could legally acquire firearms (including military style semi-automatic firearms) for an attack and that the firearms licence vetting process would be unlikely to reliably identify a terrorist posing as a legitimate firearms applicant (see Part 8, chapter 4).

58 The concentration of counter-terrorism resources on the threat of Islamist extremist terrorism was not therefore based on an informed assessment of the threats of terrorism from other ideologies. We now turn to consider whether there was a system-wide decision that, despite the absence of such an assessment, counter-terrorism resources should continue to be allocated almost exclusively to the threat of Islamist extremist terrorism.

59 The position of the New Zealand Security Intelligence Service is that before May 2018, a combination of the presenting threat of Islamist extremist terrorism and its limited capacity meant that it did not have the resources to devote to developing an understanding of other threats. It also pointed out that Islamist extremism and right-wing extremism are not the only ideologies that can, and have, led to acts of terrorism. The New Zealand Security Intelligence Service suggests that a requirement to assess all possible sources of terrorism before allocating counter-terrorism resources would be impractical. Furthermore, and importantly, the way in which the New Zealand Security Intelligence Service allocated its resources was considered. It was foreshadowed in the February 2016 Strategic Capability and Resourcing Review Cabinet paper in a way that indicates government acceptance of the appropriateness of deferring baselining. It was also consistent with the priorities identified in the New Zealand Security Intelligence Service's 2016 *10-Year Operational Strategy*. And when it had the capacity to do so in May 2018, the New Zealand Security Intelligence Service commenced its baselining project.

60 There is some substance in these arguments. But:

a) An informed assessment of the threat might have been based on an exercise less substantial than the baselining project that the New Zealand Security Intelligence Service commenced in May 2018 (itself a deliberate allocation of counter-terrorism resources) and permitted an informed decision as to the relative priorities of those threats. As it happens there was no such assessment and indeed no continuing or dynamic review of the threats or the priorities identified in the 2016 *10-Year Operational Strategy*.

b) Our appreciation of the situation in, say, 2017 is that the threat of extreme right-wing terrorism and risk associated with the recognised ease with which a potential terrorist could obtain weapons of high lethality were more than theoretical and at least warranted some attention.

c) Most importantly, we consider that a deliberate decision on the part of the New Zealand Security Intelligence Service to devote its counter-terrorism resources almost exclusively to the threat of Islamist extremist terrorism despite the absence of an assessment of other threats is not a substitute for a system-wide decision.

61 In the minutes of the Security and Intelligence Board and the Counter-Terrorism Coordination Committee, the inter-agency groups primarily responsible for coordinating New Zealand's counter-terrorism efforts, there is a striking absence of specific discussion about the threat of right-wing extremist terrorism. There is no record that these groups explicitly recognised that there was a domestic terrorist threat from the extreme right-wing and that this threat was not well understood.

62 There is a reasonable case to be made for the view that, despite the absence of explicit discussion, members of the Security and Intelligence Board either did know, or should have known, that there was a threat of right-wing extremist terrorism that the counter-terrorism agencies did not understand:

a) The Strategic Capability and Resourcing Review set out capacity and capability constraints affecting the New Zealand Security Intelligence Service, and the implementation programme that followed broadly indicated how these capacity and capability constraints would be addressed over time. That there were threats that were not understood, and that no systematic effort to understand them would start until resources allowed, followed logically from a close reading of the associated documents.

b) Reporting of right-wing extremist activity in other Western countries was widely distributed amongst the agencies represented on the Security and Intelligence Board. As well, its members' knowledge of global events would likely have included the right-wing extremist terrorist activity that was occurring in other Western countries.

c) It was implicit in what was said (and not said) at meetings of the Security and Intelligence Board and the Counter-Terrorism Coordination Committee that the focus of the counter-terrorism effort was on Islamist extremist terrorism and that there was no reference to work being carried out on any other terrorist threats.

63 It may well have been stating the obvious if the New Zealand Security Intelligence Service or New Zealand Police had explicitly told the Security and Intelligence Board or Counter-Terrorism Coordination Committee that their understanding of the non-Islamist extremist domestic terrorist threat was very limited. As well:

a) There were financial constraints. The Cabinet papers associated with the Strategic Capability and Resourcing Review programme indicated a clear government expectation that, in the absence of a significant change of circumstances, the agencies were not expected to seek further funding before 2019. A New Zealand Police budget bid in 2016 for additional counter-terrorism resources had been rejected.

b) The options for the counter-terrorism effort were limited. As we have explained, it was not obvious that reallocating scarce counter-terrorism resources away from the presenting threat to start the baselining project earlier would have resulted in an overall reduction in risk. Bringing additional counter-terrorism staff into the system was already underway and increasing the pace of this would have presented challenges, even if additional funding became available (see Part 8, chapter 5).

64 All of that said, we are of the view that there was a systemic failure to recognise that there was a threat of extreme right-wing domestic terrorism that was not understood. It follows that the allocation of counter-terrorism resources almost completely to Islamist extremist terrorism was not the result of a considered system-wide decision.

65 New Zealand, as a small country, cannot achieve capacity and capability to operate across the full spectrum of risks and threats it faces. This means that assessment (and continual reassessment) of risks and threats to national security, and allocation of resources to match those risks and threats, are critical to a well-functioning national security system. One of the mechanisms that underpins the "all hazards, all risks" framework is that resources across the system will be allocated to the highest priority risks and threats. If there are capacity or capability limitations that prevent particular risks or threats being understood, the core organising principle of New Zealand's national security system – the "all hazards, all risks" approach – requires those limitations to be identified.

66 In 2010, Barry Charles Ezell and others in *Probabilistic Risk Analysis and Terrorism Risk* wrote that:

> *… considerable efforts have been made to estimate the risks of terrorism and the cost effectiveness of security policies to reduce these risks. [The Department of Homeland Security], industry, and the academic risk analysis communities have all invested heavily in the development of tools and approaches that can assist decisionmakers in effectively allocating limited resources across the vast array of potential investments that could mitigate risks from terrorism and other threats.*[233]

This is relevant to New Zealand's counter-terrorism effort. Although we have not been prepared to engage in a retrospective risk analysis of the concentration of resources on Islamist extremist terrorism, such analysis is required for effective resource allocation decisions in the future. Identification of capability and capacity limitations that may be preventing risks and threats being understood should be explicit.

67 The members of the Security and Intelligence Board and the Counter-Terrorism Coordination Committee could not be expected to have had the Cabinet papers relating to the Strategic Capability and Resourcing Review in the forefront of their minds. And despite what may have been implicit in what was said (and not said), explicit recognition at meetings of the fact that there was a threat that was not understood would presumably have prompted discussion.

[233] BC Ezell, SP Bennett, D von Winterfeldt, J Sokolowski and AJ Collins "Probabilistic Risk Analysis and Terrorism Risk" (2010) 30(4) *Risk Analysis* https://www.dhs.gov/xlibrary/assets/rma-risk-assessment-technical-publication.pdf.

68 Given the known capacity and capability constraints of the New Zealand Security Intelligence Service and its plan to remedy its poor understanding of emerging threats, such discussions may have led nowhere. It would, however, have been possible to ask for more money. Additional resources from within the New Zealand Security Intelligence Service or New Zealand Police might have been allocated to counter-terrorism. And the focus of the National Assessments Bureau and the Combined Threat Assessment Group may have been reconsidered.

69 Across the counter-terrorism effort there remains a lack of clarity as to who holds the responsibility for looking across the collective effort to identify risks and gaps. As a result, we found it difficult to understand how the *collective* responsibility to detect and mitigate future terrorist threats could be fully exercised.

70 Finally, despite what should or may have been apparent to members of the Security and Intelligence Board and the Counter-Terrorism Coordination Committee, ministers could not be expected to infer from the material they received that there was a threat of extreme right-wing terrorism that was not understood by the counter-terrorism agencies. And this was something that they were entitled to be told.

71 Had they been advised of this, and of the unmitigated risk to New Zealand's national security that the system was carrying, ministers would have been able to decide whether that was a risk they were willing to accept. Because they were not informed of this risk, they were not given the opportunity to act.

72 The following factors contributed to this systemic failure of the counter-terrorism effort:

a) The limited resources in the overall counter-terrorism effort.

b) The focus of the National Assessments Bureau and the Combined Threat Assessment Group.

c) The New Zealand Security Intelligence Service not highlighting with the Security and Intelligence Board and Counter-Terrorism Coordination Committee the risk implications of its operational strategy (in particular, the timing of the growth of capability and capacity, and deferral of the baselining project until sufficient resources were available).

d) The members of the Security and Intelligence Board and Counter-Terrorism Coordination Committee not exploring what was implicit in what they had been told (and not told) – that the right-wing extremist threat was not well understood.

e) New Zealand Police not highlighting with the Security and Intelligence Board and Counter-Terrorism Coordination Committee that their intelligence function had been run down, they were no longer producing assessments on the extreme right-wing and strategic assessments on domestic extremism, and the residual risk this carried.

f) The reality that the system did not force or at least encourage Public sector agencies to discuss their individual strategies and any residual risk they were carrying and thus identify gaps in the system.

Would any plausible allocation of counter-terrorism resources have resulted in anticipation or planning for the terrorist attack?

73 We have reviewed at length the individual's background and his planning and preparation for the terrorist attack (see *Part 4: The terrorist*). The indicators of his planning and preparation that might have been noticed by the public or by the counter-terrorism agencies were limited. The strongest indicator was his flying a drone over Masjid an-Nur. As well, his internet activity using the Barry Harry Tarry username, his Trade Me username "Kiwi14words" and his shooting style at the Bruce Rifle Club could be seen, individually, as indicators, though not particularly strong ones. Further, if there had been different health reporting arrangements that had enabled his steroid and testosterone use and firearms injury to be linked to his status as the holder of a firearms licence, his fitness to hold that licence might, conceivably, have come into question. As it turns out, however, none of these indicators came to the notice of the counter-terrorism agencies.

74 Had there been a threat agnostic public facing counter-terrorism strategy that incorporated a "see something, say something" policy, there would have been an increased chance of such signals being reported, perhaps the drone flying incident and possibly his shooting style or his use of the "Kiwi14words" username. The absence of such a public-facing counter-terrorism strategy, however, is unrelated to the general concentration of counter-terrorism resources on Islamist extremist terrorism.

75 Based on the counter-terrorism effort operating as it did before 15 March 2019, the individual's detection by the counter-terrorism agencies depended on chance – that is, the individual deviating from his attempts at operational security, and this coming to the attention of relevant Public sector agencies such as New Zealand Police. We are of the view that detecting the individual would have depended on chance even if there had been a very substantial focus on right-wing extremism by the counter-terrorism agencies.

76 In the absence of a "see something, say something" policy, such increased focus on right-wing extremism by the New Zealand counter-terrorism agencies would not have increased the likelihood of public reporting. It is unlikely that the counter-terrorism agencies would have monitored what was discussed in a private Facebook group associated with an Australian group. Similarly, the counter-terrorism agencies did not have the capability or probably the legal authority to monitor social media activity on the scale necessary to pick up possibly significant usernames such as "Kiwi14words". Even if they had they done so, it is not easy to see how discovering that someone was using that username would have justified collecting the additional information that would have been needed to identify the individual as a national security threat. We have in mind the restrictions created by section 19 of the Intelligence and Security Act 2017 and the necessary and proportionate test (see Part 8, chapter 14).

77 Therefore, we do not see the substantial concentration of counter-terrorism resources on Islamist extremist terrorism in the years leading up to 15 March 2019 as having contributed to the individual's planning and preparation for the terrorist attack going undetected.

Conclusion

78 We conclude that the concentration of counter-terrorism resources on the threat of Islamist extremist terrorism before the New Zealand Security Intelligence Service's baselining project began in May 2018 was:

a) not based on an informed assessment of the threats of terrorism associated with other ideologies; and

b) did not result from a system-wide decision that, despite the absence of such an assessment, counter-terrorism resources should continue to be allocated almost exclusively to the threat of Islamist extremist terrorism.

It was therefore inappropriate. But we also conclude the concentration of resources on the threat of Islamist extremist terrorism did not contribute to the individual's planning and preparation not being detected.

15.3 Did any relevant Public sector agency fail to meet required standards or was otherwise at fault?

79 Other than in the systemic sense just identified, we see no failure to meet required standards in respect of the counter-terrorism effort.

80 The systemic failure to recognise that there was a threat of extreme right-wing domestic terrorism which was not understood did not contribute to the fact that the individual's planning and preparation was not detected. This is for essentially the same reasons as discussed above. For this reason, we do not make a finding of failure or fault against any of the relevant Public sector agencies in respect of the counter-terrorism effort.

15.4 Whether other findings are necessary to provide a complete report on other matters relevant to the purpose of the inquiry?

81 As we have observed, we interpreted the questions in our Terms of Reference on which findings were required as primarily directed to whether the relevant Public sector agencies were at fault in relation to the terrorist attack. Recommendations that we make must be based on factual assessments but these assessments do not need to be premised on formal findings. There is thus no requirement for further formal findings.

15.5 Elements of the counter-terrorism effort that need improvement

A preliminary comment

82 The counter-terrorism effort in New Zealand has achieved successes, as we have described. In doing so, the counter-terrorism agencies have shown considerable flexibility, looking to achieve good outcomes in ways that do not necessarily involve prosecution. This success has been achieved despite the limited counter-terrorism resources available and the absence of precursor terrorism offences in the Terrorism Suppression Act 2002 (see Part 8, chapter 13), which in some instances may have enabled investigations to be closed earlier than they were.

83 The people engaged in the counter-terrorism effort are professional and dedicated. They deal with unpredictable people and are required to make decisions based on incomplete information. And if they get those decisions wrong, the consequences may be catastrophic.

84 The concerns we have about the counter-terrorism effort are not about the professionalism of those working in the operational agencies. They are, rather, systemic in character. In this section, we set out our principal conclusions on the parts of the counter-terrorism effort that need improvement, on which we base our recommendations (see *Part 10: Recommendations*).

85 We approach the discussion that follows under the following headings:

a) Political and public engagement.

b) Leadership and coordination.

c) Strategic intelligence assessments.

d) Role of the Government Communications Security Bureau.

e) Information sharing.

f) Interagency cooperation.

g) Online capability.

h) Legislative stewardship.

86 These conclusions reflect the environment after 15 March 2019. In this environment lessons learned from the 15 March 2019 terrorist attack and subsequent appraisals of the counter-terrorism effort, including this report, can be applied. As well, constraints that previously limited the lines of activity that could be pursued are less significant than they were previously.

Political and public engagement

87 The current Directors-General of the intelligence and security agencies have been more proactive with the public than their predecessors. The New Zealand Security Intelligence Service has an active community engagement programme, which, for example, resulted in more than 100 interactions between the New Zealand Security Intelligence Service staff and community representatives in 2018 and 2019.

88 All of that said, and recognising the hard work that has been carried out, there has been little informed public debate about the counter-terrorism effort beyond that stimulated by identification of errors or embarrassment for the intelligence and security agencies or New Zealand Police or controversies involving proposed legislative changes. There are few public-facing documents explaining to New Zealanders what is done on their behalf by those involved in the counter-terrorism effort. Stories of counter-terrorism successes have not been told publicly. More generally, there has been little or no recognition of the need for, and efforts of, the agencies that contribute to New Zealand's counter-terrorism effort and keeping New Zealanders safe.

89 The events and controversies to which we referred in Part 8, chapter 2 led to an environment surrounding the intelligence and security agencies that was sufficiently toxic as to leave limited scope for useful political engagement. As well, in the situation as it was before 15 March 2019, politically-led discussion and debate about counter-terrorism was likely to result in further stigmatisation of Muslim communities, along the lines of what had occurred following the "Jihadi brides" controversy. There was also a political desire not to be alarmist about the terrorism threat.

90 The ability of the counter-terrorism agencies to talk about their successes has been severely constrained. In the absence of terrorist attacks, the lack of precursor terrorism offences meant that there were no terrorism prosecutions. This is despite the possibility that there may have been some prosecutions if New Zealand had legislation in place similar to that of the United Kingdom and Australia. The successful resolution of some investigations may have been jeopardised by publicity. Further, pervasive secrecy requirements are in themselves a serious limit on what can be said publicly. All of this has meant that there is at best limited public understanding of the threat of terrorism and the work that the counter-terrorism agencies carry out.

91 The lack of informed public debate has had consequences:

a) The social licence for the Public sector agencies involved in the counter-terrorism effort is limited.

b) The public, local government, private sector and civil society do not know what contribution they can make to the counter-terrorism effort.

c) Successive governments' budget decisions have not been informed by a deep political or public appreciation of counter-terrorism threats and risks and the value that the relevant Public sector agencies do, and could, provide to public safety and national security.

92 These consequences are not theoretical. Two examples will suffice:

a) Despite the individual's attempts at operational security, there were a few occasions when he acted in ways that were noticed by the public. Primarily relevant are the individual flying a drone over Masjid an-Nur, and his shooting style, which was noted as odd by some members of the Bruce Rifle Club. If the public was more aware of the risk and they knew how they could contribute to the counter-terrorism effort, people might have reported the individual's actions to the counter-terrorism agencies. We cannot know what difference such reports might have made, but the chance of the individual's activities being detected would have increased.

b) A public facing counter-terrorism strategy would include risk mitigation measures relating to target-hardening and managing crowded spaces. If implemented before 15 March 2019 such measures may well have reduced the loss of life resulting from the terrorist attack.

93 In the post-15 March 2019 environment, there should be substantially increased scope for informed public debate.

94 The terrorist attack of 15 March 2019 changed the public perception of terrorism in New Zealand. It also reinforced the reality that the terrorist threat comes from a number of groups and ideologies. This is clear from not only the terrorist attack of 15 March 2019 but also what has come to light since. In this environment, a threat agnostic counter-terrorism strategy should be able to be presented in a way that does not stigmatise particular communities or unduly alarm the public.

95 As we have already noted, a high-level *Countering terrorism and violent extremism national strategy overview* was published on the website of the Department of the Prime Minister and Cabinet in February 2020.[234] This mode of publication meant that it attracted little public attention and it has not been promoted as an opportunity to stimulate debate. We have been told that the Government has been awaiting our report before implementing more activities in the national strategy overview's proposed *Public information action plan*, including public messaging on how to stay safe during a terrorist attack and media engagement. We note that part of this, a crowded places strategy, was made public with a press release by New Zealand Police in September 2020 (and included on the websites of New Zealand Police, the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and other Public sector agencies).[235]

[234] Department of the Prime Minister and Cabinet, footnote 48 above.

[235] New Zealand Police press release *Working together to keep crowded places safe* (17 September 2020) https://www.police.govt.nz/news/release/working-together-keep-crowded-places-safe; New Zealand Police website *Crowded places strategy* https://www.police.govt.nz/advice-services/protecting-crowded-places-attack/crowded-places-strategy; Department of the Prime Minister and Cabinet website *Counter-terrorism* https://dpmc.govt.nz/our-programmes/national-security-and-intelligence/counter-terrorism; New Zealand Security Intelligence Service website *Protecting our Crowded places* (18 September 2020) https://www.nzsis.govt.nz/news/protecting-our-crowded-places/.

96 We consider that the development of a countering violent extremism and terrorism strategy should prompt public debate, as we hope will be the case with this report.

Leadership and coordination

97 As part of the national security system, the counter-terrorism effort is organised on a decentralised coordinated model (see Part 8, chapter 3). It is decentralised in that no single agency has overall responsibility for policy and operational effort and the counter-terrorism effort is spread across multiple agencies. It is coordinated, in that the agencies within the system proactively work together under the coordinating leadership of the Department of the Prime Minister and Cabinet. That leadership is not directive. The chief executives of the intelligence and security and law enforcement agencies have statutory responsibility for the performance of their individual agencies and are not under the direction or control of the Department of the Prime Minister and Cabinet. There is, however, a collective responsibility regarding national security through the Security and Intelligence Board.

98 There are significant disadvantages or risks associated with this decentralised model, including lack of engagement, miscommunication, slow or incomplete information exchange, duplication of effort and the absence of a single point of accountability. There are also potential advantages, including absence of capture by a single agency, flexibility to innovate, nimbleness of individual agencies, different perspectives able to be brought to the table and competing ideas exposed for debate.

99 Maximising the advantages and minimising the disadvantages requires leadership that:

a) ensures that the individual agencies are interacting effectively with each other (sharing information, coordinating efforts, undertaking joint operations and collaborating on strategy) and not operating individually and in parallel; and

b) sets an agenda that identifies and addresses gaps in the system that individual agencies might not see from the vantage points of their own positions within the system.

100 This is a demanding leadership role, particularly for an agency such as the Department of the Prime Minister and Cabinet, which has little operational experience and limited resources.

101 Where a work programme involves contributions from multiple agencies, it is usual Public sector management practice in New Zealand for a strategy document to be put in place to guide and coordinate each agency's contribution. A good strategy document enables role and terminology clarification, identifies common purpose, allocates accountability and enables proper resource allocation. However, no such strategy was in place to guide the counter-terrorism effort.

102 Between 2014 and March 2019, the counter-terrorism effort had made some progress:

a) A new ministerial portfolio for national security and intelligence was created in 2014.

b) The Specialist Coordinator for the counter-terrorism effort was appointed in 2016.

c) The Intelligence and Security Act was passed in 2017, which reformed the intelligence and security agencies' authorising environment.

d) A National Risk Register was developed in 2018. While the Register has not yet been approved and published by the Government, the risk profiles are being used by officials to support a more strategic and proactive approach to risk management.

e) A more clearly defined interagency counter-terrorism work programme was progressed by the Security and Intelligence Board in 2018 (largely driven by the Specialist Coordinator).

f) The Security and Intelligence Board approved the *Counter-Terrorism Strategic Framework* and the *High-Level Framework for the Prevention of Violent Extremism* in 2018.

103 Some work streams that did not produce tangible public outcomes were affected by political considerations, most particularly the proposed public facing counter-terrorism strategy and the National Risk Report, which would have had a terrorism component. In the post-15 March 2019 environment, the constraints that influenced these political considerations may have less relevance.

104 There was little progress in areas that needed coordination. This is illustrated by:

a) the absence of a mature risk management framework or mechanism that would have resulted in system-wide recognition of potential threats to New Zealand and what actions would be taken to mitigate them;

b) a lack of common understanding about leadership of the counter-terrorism effort;

c) the delay in New Zealand Police and the New Zealand Security Intelligence Service cooperating on understanding the threat posed by right-wing extremism leading to confusion between the counter-terrorism agencies of their respective individual and collective roles as to right-wing extremism;

d) the limited coordination of building online capability and capacity; and

e) the absence of system performance standards and accepted best practice in the New Zealand context against which to monitor performance and measure the effectiveness of the system.

105 The overarching benefit of a functioning system is the development of whole-of-system insights on which to implement joint effort. This appears lacking. Our impression of the material we have seen is that the agencies represented on the Security and Intelligence Board were not working together to understand and provide advice on the collective insights from assessments or to identify and respond to gaps in the system.

106 It is apparent that the counter-terrorism effort was not functioning as a national security system should. It was functioning as a collection of agencies, operating largely in parallel, with some elements of coordination but little shared direction.

Strategic intelligence assessments

107 Strategic assessments enable the counter-terrorism effort to scan the horizon to look for new and emerging threats. They lift the focus from today's presenting threat and remind operational agencies of the need to anticipate future threats. It is an important tool for the effective allocation of resources, particularly where capacity or capability are limited. In New Zealand the Combined Threat Assessment Group and the National Assessments Bureau are the two agencies with responsibility for strategic assessments that support the counter-terrorism effort (see Part 8, chapter 4).

108 As is apparent, we are of the view that the orientations of these two assessment agencies meant that they did not focus on emerging threats of domestic terrorism. This was contributed to by resource constraints. As well, there was no national assessments programme to coordinate the strategic assessment activities of those two agencies.

109 Despite recognition since at least 2003, when the Auditor-General reported that an "over the horizon" function was critical to New Zealand's national security system,[236] such a capability has not been developed. The counter-terrorism effort would be strengthened if the assessment agencies had a dedicated horizon scanning function.

Role of the Government Communications Security Bureau

110 As we have explained, the domestic counter-terrorism role of the Government Communications Security Bureau was very limited (see Part 8, chapter 7). Leaving aside its cyber security role, it operates primarily as a foreign intelligence agency and it engages in domestic counter-terrorism activity only when tasked by another agency. There are a number of reasons for this, including legacy effects of the legislative settings before the Intelligence and Security Act, its capabilities and its assessment as to where those capabilities are best directed.

111 The domestic counter-terrorism effort would be strengthened if the Government Communications Security Bureau took a more proactive role.

[236] Office of the Controller and Auditor-General, footnote 8 at pages 39-40.

Information sharing

112 In New Zealand's decentralised counter-terrorism effort, sharing of information between Public sector agencies is critical to the effectiveness of the system (see Part 8, chapter 9). Well-functioning information sharing practices are particularly critical to enabling Public sector agencies to detect lone actor threats because, on the whole, it is less likely that lone actors will give detectable signals than terrorists operating within a cell or network.

113 Information sharing issues are not confined to highly classified information. Public sector agencies are not using current legislation to the fullest extent possible to provide for the sharing of information that is not subject to secrecy constraints. The Intelligence and Security Act permits direct access agreements to be established between the intelligence and security agencies and other specified Public sector agencies, but few have been entered into. While we accept that some effort and resource is required to conclude these agreements, our sense is that not all agencies are prioritising this work. The Department of the Prime Minister and Cabinet, as sector leader, should drive this area of effort.

114 There are also issues relating to highly classified information:

a) Sharing highly classified information between intelligence and security agencies (such as the New Zealand Security Intelligence Service) and law enforcement agencies (such as New Zealand Police) is a problem in many international jurisdictions. While New Zealand Police and the New Zealand Security Intelligence Service have improved their information sharing practices over the last five years by, for example, developing an information sharing protocol and co-locating teams in Auckland, there are continuing concerns amongst operational staff, particularly in New Zealand Police.

b) We have seen many examples of documents being over-classified. The more highly classified a document, the fewer people can see it. As we have noted, the volume of highly classified information produced by the New Zealand Security Intelligence Service and the Government Communications Security Bureau on domestic terrorism threats is relatively small. This small scale makes it possible for agencies to spend more time than we think they currently do on classification decisions or tearline reports. Tearlines are portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification.[237]

c) The "need to know" principle could be used as an opportunity for Public sector agencies to think through who would benefit from receiving information, rather than as a reason for not sharing information.

[237] Office of the Director of National Intelligence *Intelligence Community Directive 209: Tearline Production and Dissemination* (6 September 2012) https://fas.org/irp/dni/icd/icd-209.pdf.

d) Strategic intelligence assessments about terrorism threats in New Zealand are the culmination of a great deal of investment. They should present the most authoritative and complete picture of the threatscape possible. Ideally they should be classified at a level that permits sufficiently wide distribution to enable them to inform government decisions and activity.

115 Other than developing practical enablers, such as improved secure information technology, we have not seen a coordinated effort led by the Department of the Prime Minister and Cabinet and the Security and Intelligence Board to focus attention on information sharing and to overcome barriers to sharing highly classified information with all the Public sector agencies whose work would benefit from receiving it.

Interagency cooperation

116 The decentralised, coordinated model that the counter-terrorism effort employs relies for its effectiveness on the quality of interagency cooperation.

117 In the course of our inquiries we have been able to observe the level of cooperation between the Public sector agencies involved in the counter-terrorism effort. Our primary focus was the relationship between New Zealand Police and the New Zealand Security Intelligence Service (see Part 8, chapter 12).

118 Since 2015 there has been a significant improvement in the level of cooperation between the counter-terrorism agencies. The two agencies have created formal interagency groups and committees designed to facilitate cooperation at different levels of their organisations. Some co-location has been piloted and found to be of value to the working relationship.

119 The general philosophy has been to allow cooperation to develop organically. This involves relying on individuals to cooperate. Although we acknowledge significant improvement, this approach means that much depends on the informal understandings and arrangements between individuals. The system benefits could be lost with changes in personnel or a shift in focus. This is not a recipe for enduring success.

120 We have earlier identified some issues where cooperation has not been ideal and where the counter-terrorism agencies have operated in parallel. We are left with the view that, for the future, a more structured approach to cooperation would produce better results.

Online capability

121 A significant element of New Zealand's counter-terrorism effort needs to be online, because the internet is widely recognised as having become a key platform for terrorist radicalisation and recruitment. Our report shows that it was on the internet that the individual developed and shared his extreme right-wing views, received inspiration and probably obtained operational information, researched firearms capability and undertook some of his reconnaissance. It was also the internet that enabled him to reach a worldwide audience with his GoPro livestream and manifesto (see *Part 4: The terrorist*).

122 Before 15 March 2019 the online capability of New Zealand's counter-terrorism effort was limited (see Part 8, chapter 11). In the aftermath of the terrorist attack, the New Zealand Security Intelligence Service's online capability was assessed as "fragile". The same was true of the capability of New Zealand Police. The Government Communications Security Bureau was not substantially involved in the counter-terrorism effort.

123 In mid-2018 the Specialist Coordinator commissioned a stocktake of agencies' online activity to counter extremism. This found that although there were some relevant work streams underway, there was not a common approach and the level of coordination between agencies was questionable. The stocktake was provided to the Counter-Terrorism Coordination Committee but no further progress had been made by 15 March 2019.

124 Given the commonalities of effort between New Zealand Police and the New Zealand Security Intelligence Service and the complementary or additional roles and capabilities of the Government Communications Security Bureau and Department of Internal Affairs (in relation to objectionable material), coordination of the development of online capability is plainly sensible. Such coordination was not evident in relation to new funding approved for one agency to develop online capability in the 2019 Budget.

Legislative stewardship

125 Legislation is an important tool in any counter-terrorism effort. In our enquiries we focused on two principal statutes, the Terrorism Suppression Act (see Part 8, chapter 13) and the Intelligence and Security Act (see Part 8, chapter 14).

126 The Terrorism Suppression Act, among other things, sets the framework for criminalising various types of terrorist activity. It therefore sets the point at which New Zealand Police can disrupt terrorist activity by arrest and prosecution. The Intelligence and Security Act regulates intelligence gathering by the New Zealand Security Intelligence Service and the Government Communications Security Bureau. For the counter-terrorism effort to be effective, both pieces of legislation need to keep up to date with evolving patterns of terrorist activity, emerging technologies, operational challenges and public expectations about the balance between public safety and human rights.

127 The Terrorism Suppression Act does not provide the counter-terrorism agencies with assistance in dealing with potential terrorists who are operating in what we have called the pre-criminal space – that is, they are planning and preparing for a terrorist attack but have not committed any offences. This issue has been addressed in the United Kingdom and Australia by the creation of precursor terrorist offences, which include but are not confined to planning and preparation for acts of terrorism. The lack of such offences in New Zealand has limited the ability of New Zealand Police to disrupt terrorist planning and preparation by arrest. As well, it imposes at least potential limitations on the ability of New Zealand Police to exercise powers under the Search and Surveillance Act 2012. The lack of precursor terrorist offences also contributed to the New Zealand Security Intelligence Service's focus on monitoring known terrorist threats. Rebecca Kitteridge, Director-General of Security, told us that this was unsatisfactory, as it tied up resources that should be actively seeking out unknown threats.

128 More generally, the effectiveness of the Terrorism Suppression Act has been affected by the lack of a review of whether it is fit for purpose. A holistic assessment of the nature of the risk presented by potential terrorists in the pre-criminal space is required. That assessment should consider the best way the risk can be mitigated with the resources that New Zealand is prepared to allocate to the counter-terrorism effort.

129 The Intelligence and Security Act has been useful in modernising and unifying the legal framework within which the New Zealand Security Intelligence Service and the Government Communications Security Bureau operate. It will be the subject of a mandatory review in 2022.

130 We consider that some of the difficulties with the operation of the Intelligence and Security Act may be able to be resolved by a different style of engagement between the intelligence and security agencies and the Inspector-General of Intelligence and Security (see Part 8, chapter 14). We have in mind here issues associated with the threshold for intelligence warrants on the risk of terrorism. This is particularly relevant to target discovery (Part 8, chapter 10).

131 There are other difficulties that warrant attention in the 2022 review of the Intelligence and Security Act as we set out in chapter 14. We are, however, of the view that urgent attention should be given to section 19.

Chapter 16: Findings

1 We conclude that the concentration of counter-terrorism resources on the threat of Islamist extremist terrorism before the New Zealand Security Intelligence Service's baselining project began in 2018 was:

a) not based on an informed assessment of the threats of terrorism associated with other ideologies; and

b) did not result from a system-wide decision that, despite the absence of such an assessment, counter-terrorism resources should continue to be allocated almost exclusively to the threat of Islamist extremist terrorism.

It was therefore inappropriate.

2 We find that the inappropriate concentration of resources on the threat of Islamist extremist terrorism did not contribute to the individual's planning and preparation for his terrorist attack not being detected. And for that reason, the Public sector agencies involved in the counter-terrorism effort did not fail to anticipate or plan for the terrorist attack due to an inappropriate concentration of counter-terrorism resources.

3 We find no Public sector agency involved in the counter-terrorism effort failed to meet required standards or was otherwise at fault in respects that were material to the individual's planning and preparation for his terrorist attack not being detected.

Chapter 17: Questions asked by the community

17.1 Right-wing extremism

Before 15 March 2019, were Public sector agencies sufficiently aware of the threat posed by white supremacist and other right-wing extremist non-state actors and movements? If so, what did they do in response to the threat?

Public sector agencies had some awareness of the terrorist threat posed by the extreme right-wing (see Part 8, chapter 4). This awareness was limited:

- The primary focus of intelligence assessments was international terrorism (particularly the threat to New Zealanders overseas). Those assessments on international terrorism primarily focused on Islamist extremist terrorism.
- In the five years or so leading up to 2018, there were few strategic assessments about terrorism threats in New Zealand, and practically none on threats other than Islamist extremism.
- The New Zealand Security Intelligence Service started its baselining project in May 2018. Following a meeting in December 2018 New Zealand Police took preliminary steps to undertake their own exercise on the extreme right-wing. As at 15 March 2019, the awareness of the threat posed by the extreme right-wing was developing but was still limited.

In response to the threat, the counter-terrorism agencies:

- investigated leads relating to the extreme right-wing as and when received;
- in 2018 began work to better understand the threat, most relevantly the New Zealand Security Intelligence Service baselining project on domestic right-wing extremism; and
- conducted a tabletop counter-terrorism Response exercise in October 2018 based on a scenario of an assumed motor vehicle attack on worshippers outside Masjid an-Nur.

What intelligence did agencies receive from Five Eyes partners regarding white supremacy and right-wing extremism before 15 March 2019?

Very little international partner reporting related to right-wing extremism (see Part 8, chapter 4). For example, in the second quarter of the 2018–2019 financial year, the Government Communications Security Bureau received 7,526 intelligence reports from international partners about terrorism and violent extremism, none of which related to right-wing extremism.

Reporting that was received included:

- Intelligence from an international partner that assessed the potential – in terms of the availability of firearms – of a "Norwegian-style attack" occurring in that country.
- Intelligence received from an international partner in 2013 about the extreme right-wing in their country.
- Intelligence received from an international partner about an extreme right-wing group member possibly planning a violent act. This was cited in a March 2017 Combined Threat Assessment Group assessment, which observed that "an increase in anti-Semitic and anti-Muslim hatred is a concern for [the international partner's] authorities".
- Intelligence cited in a May 2017 Combined Threat Assessment Group assessment addressed implications for New Zealand of the Manchester Arena terrorist attack.

Public sector agencies involved in the counter-terrorism effort participated in some meetings and training opportunities with international partners that addressed, among other things, the extreme right-wing.

Given the upward trend in white supremacist and other right-wing extremist acts of violence (actual and prevented) in the decade prior, why was there no concern of this happening in New Zealand until mid-2018?

There was some concern about the threat from the extreme right-wing (see Part 8, chapter 4). The reasons why counter-terrorism resources were largely concentrated on the threat of Islamist extremist terrorism are discussed in the same chapter. They largely come down to Islamist extremism being seen as the presenting threat and resource limitations.

Was any assessment done regarding danger to Muslim communities? If so, what was the result?

Strategic and tactical intelligence assessments primarily focus on the threat posed, and who poses the threat, rather than the risk to particular communities. Intelligence assessments can relate specifically to the risk to events or locations (for example, threat associated with the hosting of the Rugby World Cup 2011).

We have seen one New Zealand Police intelligence assessment produced before 15 March 2019 that specifically refers to the risk to Muslim communities. A May 2018 report, *National Security Situation Update: Ramadan 2018*, which was provided to New Zealand Police Assistant Commissioners and District Commanders, noted that Dā'ish had issued calls for terrorist attacks during Ramadan for the previous three years and could again. It advised that Ramadan was also a time of increased risk to the Muslim community and noted:

> *The Muslim community in New Zealand has experienced sporadic incidents of vandalism and abuse. While not frequent, incidents do create widespread concern among the community when they do occur, as well as attention from the media.*

Other assessments that referred more generally to the threat of right-wing extremism are discussed in chapter 4.

17.2 National Security and Intelligence Priorities

How are the National Security and Intelligence Priorities developed?

The Department of the Prime Minister and Cabinet's National Security Group leads the development of the National Security and Intelligence Priorities (see Part 8, chapter 3), following this process:

- The National Assessments Bureau produces a strategic intelligence assessment on the national security threats facing New Zealand.
- Priorities are developed, informed by the strategic assessment, and current government, sector and agency policy priorities and, since 2018, the National Risk Register.
- Relevant Public sector agencies are consulted on the draft Priorities.
- The Security and Intelligence Board endorses the Priorities.
- Cabinet approves the Priorities.

Which agencies influence the setting of the National Security and Intelligence Priorities, and how?

The Government Communications Security Bureau, Immigration New Zealand, New Zealand Customs Service, New Zealand Police, the New Zealand Security Intelligence Service and other Public sector agencies contribute to the setting of National Security and Intelligence Priorities (see Part 8, chapter 3). For example, for the terrorism Priority the relevant Public sector agencies are:

- consulted on the drafting of the strategic assessment prepared by the National Assessments Bureau that informs the development of the Priority;
- consulted on the draft Priority individually, and in cross-agency workshops;
- consulted on the Department of the Prime Minister and Cabinet's policy papers that recommend changes to the Priorities; and
- represented at the Security and Intelligence Board, which endorses the Priorities to be sent to the Cabinet committee.

Were white supremacy and right-wing extremism included in the current National Security and Intelligence Priorities as areas of focus for counter-terrorism?

Not specifically. The 16 National Security and Intelligence Priorities approved by Cabinet in December 2018 included a terrorism priority (see Part 8, chapter 3). It includes domestic as well as international terrorism threats but does not refer to particular ideologies.

The domestic terrorism threats were described as "those that may arise in and against New Zealand or be carried out by New Zealanders overseas ... [and the] scope includes emerging trends and characteristics associated with overseas terrorist networks' links to New Zealand". The international terrorism threats were described as "threats against New Zealand's interests overseas in areas which have the greatest exposure for New Zealanders, and the trends and characteristics of emerging regional and global terrorism threats" that may impact on New Zealand. An unclassified version of the National Security and Intelligence Priorities was initially published in the Department of the Prime Minister and Cabinet's 2019 Annual Report.[238] In September 2020 the Department of the Prime Minister and Cabinet updated its website to include the unclassified version of the National Security and Intelligence Priorities,[239] which included:

> *Terrorism. Threats to New Zealand, New Zealanders and New Zealand's interests from terrorism (ideologically, politically or religiously motivated violence) at home and abroad.*

Did the National Assessments Bureau or the New Zealand Security Intelligence Service raise the issue of white supremacy and right-wing extremism in the drafting of previous or the current National Security and Intelligence Priorities?

National Assessments Bureau

Four strategic assessments produced by the National Assessments Bureau (see Part 8, chapter 4) have informed the development of the National Security and Intelligence Priorities in 2012, 2015, 2016 and 2018 (see Part 8, chapter 3):

- The strategic assessment that informed the 2012 Priorities noted the resurgence of neo-Nazi and extreme right-wing groups in Europe and the United States of America espousing hard-line nationalist and anti-immigration rhetoric. It assessed that:
    - such groups may come to prominence in New Zealand in response to the effects of the global economic crisis; and
    - economic and immigration policies could stir such groups in New Zealand to protest against perceived increasing inequalities, and this could lead to the adoption of more violent methods to effect political change.

[238] Department of the Prime Minister and Cabinet, footnote 46 above at page 85.

[239] Department of the Prime Minister and Cabinet, footnote 47 above.

- The strategic assessment that informed the 2015 Priorities did not mention white supremacy or right-wing extremism.
- The strategic assessment that informed the 2016 Priorities noted that the recovery from the Global Financial Crisis has left governments under pressure from disgruntled citizens, who are looking for alternatives on the political right and left, with unpredictable consequences.
- The strategic assessment that informed the 2018 Priorities did not mention white supremacy or right-wing extremism.

New Zealand Security Intelligence Service

The New Zealand Security Intelligence Service was consulted during the development of the National Assessments Bureau assessments that informed the development of the Priorities in 2012, 2015 and 2016.

The New Zealand Security Intelligence Service (with New Zealand Police and the Department of the Prime Minister and Cabinet) is the owner of the terrorism risk profile in the National Risk Register (see Part 8, chapter 3), which informed the development of the National Security and Intelligence Priorities in 2018.

The first terrorism risk profile (in January 2018) noted:

- the global rise of a new far right ideology, which had been strengthened by opposition to refugee settlements and Islamist extremist attacks in the West;
- that there was no indication that far right groups in New Zealand have the intent and capability to promote their ideology by an act of terrorism; and
- that an extreme right-wing lone actor attack in New Zealand remained a possibility, albeit a remote one.

Do trends in terrorist attacks (actual or prevented) on Five Eyes and other western countries inform the development of the National Security and Intelligence Priorities? If so, how?

Yes. Strategic intelligence assessments produced by the National Assessments Bureau (see Part 8, chapter 4) inform the development of the National Security and Intelligence Priorities. These draw on all sources of intelligence, both secret and open-source. This includes intelligence and reports from Five Eyes and other international partners, as well as other Public sector agencies involved in the counter-terrorism effort, such as the Combined Threat Assessment Group, the Government Communications Security Bureau, New Zealand Police and the New Zealand Security Intelligence Service.

Did the Government Communications Security Bureau or the New Zealand Security Intelligence Service withhold any information from the Department of the Prime Minister and Cabinet, and Cabinet, relating to the global trends in white supremacy and right-wing extremism during each of the previous National Intelligence Priorities cycles since they were introduced?

We have no indication, or evidence, that this occurred.

17.3 Intelligence investigations

Before 15 March 2019, how many national security investigations have been carried out on Muslim individuals, associations or institutions?

The New Zealand Security Intelligence Service told us that their investigations focus on individuals, not associations or institutions (see Part 8, chapter 5). Approximately 30–40 individuals were on the investigative prioritisation (watch) list being investigated by the New Zealand Security Intelligence Service at any given time in recent years. Most of these individuals were assessed by the New Zealand Security Intelligence Service as supporters of Dā'ish.

New Zealand Police told us that, before 15 March 2019, most of their counter-terrorism investigations were focused on the threat of Islamist extremism (see Part 8, chapter 6). The limitations of New Zealand Police's recording practices mean that exact numbers are not available. There was no centralised information system for recording national security leads, the actions taken, outcomes of investigation and characteristics of complainants, victims or offenders (such as religion).

Before 15 March 2019, how many national security investigations have been carried out on white supremacist or right-wing extremist individuals, associations or institutions?

The New Zealand Security Intelligence Service's baselining project on domestic right-wing extremism, which started in mid-2018, generated ten leads relevant to right-wing extremism (see Part 8, chapter 5). These leads were treated according to the New Zealand Security Intelligence Service's leads management process. Some of these leads remained open as at 15 March 2019.

While we have seen evidence that New Zealand Police had conducted national security investigations into activities of suspected white supremacists or right-wing extremists before 15 March 2019 (see Part 8, chapter 6), the limitations of New Zealand Police's recording practices mean that exact numbers are not available.

After 15 March 2019, New Zealand Police compiled a list of 1,700 individuals who had potential right-wing extremist characteristics from a review of their intelligence holdings. They told us that they had never attempted to do this before 15 March 2019. New Zealand Police told us that the accuracy and reliability of the information used to compile the list was variable and required further assessment. New Zealand Police collaborated with the New Zealand Security Intelligence Service and New Zealand Customs Service after 15 March 2019 to refine and prioritise the agencies' leads on right-wing extremist individuals and groups in New Zealand.

17.4 National Assessments Bureau

Did the National Assessments Bureau produce any assessments on global developments and events related to white supremacy and right-wing extremism?

Yes. The National Assessments Bureau produced two intelligence assessments related to right-wing extremism between 2010 and 15 March 2019 (see Part 8, chapter 4):

- A 2013 assessment, titled *Far Right Rising: A Dangerous Myth*, focused on the changing political landscape in Europe. The assessment noted that far right movements stepped up their anti-immigrant and anti-Muslim rhetoric during the European debt crisis (2009 onwards) but did not cover terrorism and/or violent extremism implications.
- A September 2018 assessment, titled *Global Terrorism Update,* included a small section on "extreme right terrorism". It noted that "between 12 September 2001 and 31 December 2016 in the United States of America, there were more extreme-right incidents than Islamist terrorist incidents resulting in fatalities". It concluded that there had been an emerging threat of extreme right-wing terrorism for some time, but groups were fragmented with limited international coordination.

Was the National Assessments Bureau dissatisfied with the intelligence gathering practices or products of the New Zealand Security Intelligence Service or the Government Communications Security Bureau in relation to white supremacy and right-wing extremism?

We have no indication, or evidence, that this is the case.

17.5 The New Zealand Security Intelligence Service

What level of awareness did the New Zealand Security Intelligence Service have of right-wing extremism before 15 March 2019? What information informed this awareness, including from internal analysis and/or international partners?

Before 15 March 2019, the New Zealand Security Intelligence Service had:

- received a few reports and assessments from international partners that included intelligence about extreme right-wing activity; and
- only a limited understanding of the right-wing extremist threatscape in New Zealand. This was due to a range of factors, including resourcing.

Up until mid-2018, the New Zealand Security Intelligence Service's counter-terrorism resources were focused on monitoring and investigating the presenting threat – supporters of Dā'ish seeking to participate in hostilities abroad or to mount, encourage or support terrorist attacks, or undertake activities in support of terrorism, in New Zealand (see Part 8, chapters 4 and 5).

Why did the New Zealand Security Intelligence Service undertake a baselining project on right-wing extremism in 2018? Why then?

From at least early 2016, it was appreciated by the New Zealand Security Intelligence Service there was a potential for terrorism from non-Islamist extremist sources and that it was largely unsighted to the nature and extent of such threats (see Part 8, chapter 5). This is referred to in a February 2016 Strategic Capability and Resourcing Review Cabinet paper, which identified the expected capacity increase in relation to countering violent extremism:

> *The capability increases from a current state where partial monitoring of watch-list targets is possible and there is minimal coverage outside Auckland, to a future where there is a New Zealand-wide baseline threat picture.*

Baselining emerging terrorism threats was identified as the third goal in the New Zealand Security Intelligence Service's 2016 *10-Year Operational Strategy*,[240] but its ranking meant that work on it was deferred. The New Zealand Security Intelligence Service did not have enough counter-terrorism resources until May 2018 to start its baselining project.

[240] New Zealand Security Intelligence Service, footnote 55 above.

Has the extreme right-wing baselining project been completed? If so, what were the findings? If not, has the scope, timeframe or resourcing changed as a result of the 15 March 2019 attack?

The baselining project resulted in a Security Intelligence Report on extreme right-wing online activity in New Zealand in July 2019. The report examined the online activity of a number of far right and extreme right-wing groups, forums and individuals in New Zealand. The report noted that within New Zealand there were a growing number of individuals espousing violent extreme right-wing rhetoric online. Despite this, as at July 2019, they did not identify any New Zealand-based groups that openly advocated the use of violence, and did not identify any indication that individuals or groups associated with the extreme right-wing in New Zealand were mobilising to conduct an ideologically-motivated act of violence. The report acknowledged that this could be, in part, because these groups were avoiding publicly using violent rhetoric so as to attract a wider audience and avoid detection by law enforcement and security agencies.

After 15 March 2019, the New Zealand Security Intelligence Service collaborated with New Zealand Police and New Zealand Customs Service to update and enhance the agencies' collective understanding of the post-attack domestic right-wing extremist threatscape, including refining and prioritising leads. This project concluded in June 2020.

After 15 March 2019, the New Zealand Security Intelligence Service directed more resources towards building a picture of emerging threats (see Part 8, chapter 5). It established a dedicated target discovery team within the Counter-Terrorism Unit, which has been scoping and re-scoping a number of discovery projects.

Did the extreme right-wing baselining project influence any intelligence activities relating to white supremacy or right-wing extremism before 15 March 2019?

Yes. The domestic right-wing extremism baselining project generated ten leads relevant to right-wing extremism. These leads were treated according to the New Zealand Security Intelligence Service's leads management process, and some remained open at 15 March 2019. In addition, the New Zealand Security Intelligence Service's online operations team began to look at right-wing forums (see Part 8, chapter 5).[241]

[241] New Zealand Security Intelligence Service, footnote 57 above at page 96.

What evidence informed Rebecca Kitteridge's claim regarding the "slow, but concerning, rise of right-wing extremism internationally" in her opening statement before Parliament's Security and Intelligence Committee on 20 February 2019? Was it informed by the baselining project?

The Director-General of Security's comments were informed by a few reports and assessments the New Zealand Security Intelligence Service had been receiving from international partners, including about extreme right-wing activity.

The comments were also informed by the work that had been completed up to that date on the extreme right-wing baselining project, which had started in May 2018 and was due for completion in June 2019 (see Part 8, chapter 5).

17.6 New Zealand Police

Do New Zealand Police keep a formal or informal list of Muslim individuals? Do they have any units that are predominantly focussed on Muslim individuals or communities?

Religious faith is rarely recorded in police data holdings and New Zealand Police systems do not allow the automatic or easy collation of a list of people based on their religion. New Zealand Police therefore do not keep a list of Muslim individuals.

New Zealand Police do not have any units whose purpose is to focus on Muslim individuals and communities. One of the responsibilities of ethnic liaison officers is to develop relationships with communities, including Muslim communities, but they do not work exclusively with any one ethnic or religious community. The National Security Investigation Team have primarily focused on Islamist extremism (see Part 8, chapter 6).

What records do New Zealand Police have of complaints of anti-Muslim or threatening behaviour against Muslim individuals and Muslim institutions, in Christchurch and nationally?

The limitations of New Zealand Police's recording practices means that exact numbers are not available. There was no centralised information system for recording national security leads, the actions taken, outcomes of investigations, and characteristics of complainants, victims or offenders (such as religion).

New Zealand Police provided us with a list of recorded interactions with Muslim individuals from 2010 to 14 March 2019. This list included approximately 45 reports of threatening behaviour against Muslim individuals and institutions, of which six were in the Canterbury region. The list was created after 15 March 2019 by asking Districts and specialist units to search their various databases, and collating the information provided (see Part 8, chapter 6).

We discuss recording of hate-motivated offending in Part 9, chapter 4.

Do New Zealand Police collect information on threats or attacks against places of worship or religious institutions in New Zealand? If so, how many such incidents have occurred since 1990?

The limitations of New Zealand Police's recording practices mean that this information is not available. There was no centralised information system for recording national security leads, the actions taken, outcomes of investigation, characteristics of complainants, victims or offenders (such as religion), or locations such as places of worship or religious institutions.

What, if any, partnerships have been built with international partner agencies to build capability for policing the perceived threat of white nationalism and right-wing extremism and the perceived threat of Islamist extremism?

New Zealand Police have partnerships with international law enforcement agencies and groups, including the Five Eyes Law Enforcement Group. One of the purposes of these partnerships is to build capability across a range of ideological threats.

New Zealand Police are a member of the Australia New Zealand Counter-Terrorism Committee. The Committee provides specialist training, which New Zealand Police staff have attended. Right-wing extremism has been a training focus on occasion.

New Zealand Police have adopted prioritisation and risk assessment tools developed by the Committee, such as the Operational Threat Assessment Guideline and the Counter-Terrorism Persons of Interest Prioritisation Tool Guideline. These contain generic indicators of threat and capability relevant to both Islamist extremist and right-wing extremist threats (see Part 8, chapter 6).

The leads triage process New Zealand Police adopted in the immediate aftermath of the 15 March 2019 terrorist attack was developed in consultation with specialist staff from international partner agencies.

New Zealand Police are currently increasing the number of staff based in other countries.

Do New Zealand Police respond differently to reports of suspicious or threatening behaviour related to violent extremism or terrorism when the complaint is made against a Muslim individual compared to when the complaint is made against a non-Muslim individual?

The limitations of New Zealand Police's recording practices mean that it is not possible to undertake a comparative analysis of how similar threats against Muslim individuals and non-Muslim individuals were actioned by New Zealand Police.

Many Muslim communities told us they felt that New Zealand Police did not always take reports about suspicious or threatening behaviour seriously (see *Part 3: What communities told us*). When we put this to New Zealand Police, they told us they are "threat agnostic" – meaning that when they receive a lead they use the same assessment criteria regardless of the ideological source of the threat.

New Zealand Police lacked a sophisticated understanding of the new iterations of the extreme right-wing that emerged from about 2016. Many frontline staff lacked an understanding of the risks and threats of terrorism, including how to recognise such risks and threats and what to do about them. While the National Security Investigations Team comprised capable investigators, they had limited knowledge of, and experience in investigating, right-wing extremists (see Part 8, chapter 6).

What are the policies and practices of New Zealand Police in relation to passing on complaints or information about suspected extremists to the New Zealand Security Intelligence Service?

New Zealand Police and the New Zealand Security Intelligence Service jointly manage counter-terrorism leads in accordance with an agreed joint leads process (see Part 8, chapter 12). The New Zealand Security Intelligence Service hosts a fortnightly Joint Leads Meeting attended by the Department of Corrections, Immigration New Zealand, New Zealand Customs Service, New Zealand Police and (since September 2019) the Government Communications Security Bureau. This forum is where agencies share leads and intelligence. In addition, the counter-terrorism agencies regularly share information on leads in real time, on an informal basis and as investigations progress.

What policies and procedures do New Zealand Police follow regarding the financing of international terrorism by individuals residing in New Zealand?

The Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 requires the financial sector to report suspicious financial activities to New Zealand Police's Financial Intelligence Unit through the Prescribed Transaction Reporting regime.

Reporting entities such as financial institutions and casinos have to submit all international fund transfers over $1,000 and all cash transactions over $10,000 to the Financial Intelligence Unit. This information is used for modelling and detecting suspicious criminal activity, which is referred to New Zealand Police investigation teams. The Financial Intelligence Unit produces a quarterly report which, among other things:

- examines money laundering and terrorist financing methods used in New Zealand and overseas; and
- provides indicators of money laundering and terrorist financing techniques.

17.7 Government Communications Security Bureau

Did the Government Communications Security Bureau take any action in relation to right-wing extremist threats, including actual or planned acts of terrorism within New Zealand, before 15 March 2019?

No. Before 15 March 2019, the Government Communications Security Bureau was not tasked by any agency to conduct signals intelligence activities in relation to right-wing extremism.

Since 2016, all of the Government Communications Security Bureau's counter-terrorism activities have been in response to being tasked by another agency (usually the New Zealand Security Intelligence Service). In accordance with this customer-led approach, the Government Communications Security Bureau does not "unilaterally undertake domestic counter-terrorism investigations" and does not "self-task or identify its own intelligence questions" for any counter-terrorism activity, domestic or international (see Part 8, chapter 7).

Did the Government Communications Security Bureau seek to have any extreme right-wing content removed from social media before 15 March 2019?

No. The Government Communications Security Bureau does not play a role in the reporting, filtering and removing extremist content online. This is because the identification, reporting and removal of extremist content from social media platforms is not an intelligence activity.

The removal of extremist content from social media is undertaken by the Department of Internal Affairs, organisations such as Netsafe or by social media organisations themselves.

Are social media accounts of people posting weaponry tracked?

No. Posting images of weaponry on social media is not an illegal activity.

The Government Communications Security Bureau told us it does "not monitor all of New Zealand's social media activity or internet traffic" because it does not have the legal authority, technical means or resources to do so. No Public sector agency monitors all of New Zealand's social media activity or other internet activity.

17.8 The border agencies

Why was the individual not picked up as a threat at the border?

The information available to the border agencies about the individual was limited (see Part 6, chapter 6). Between them the border agencies held information on:

- the individual's passport information (name, gender, date of birth, birthplace, citizenship, etc);
- the dates, times, arrival and destination locations of flights he took in and out of New Zealand from 1999 onwards;
- information indicating that he travelled with gaming friend from New Zealand to Japan and back in 2018;
- information that he otherwise travelled alone on flights in and out of New Zealand from August 2017 onwards;
- his arrival and departure cards for the last two international flights he took in 2018; and
- Advanced Passenger Processing and Passenger Name Record data in relation to the individual about his arrivals into New Zealand from March 2013 onwards and departures from New Zealand from 28 September 2017.

The border agencies did not hold information about the individual's full travel history. Both border agencies ran the information they had about the individual through their automated screening systems, and these processes did not identify any risks or issues. No agency raised a border alert on the individual and the individual was never subject to secondary processing at the border. On each arrival into New Zealand, his presentation at the border appears to have been unremarkable.

In summary, the individual was not picked up at the border as he did not present as a threat.

What policies and procedures are used by border agencies to identify which individuals to stop and search or interview? Is there a specific policy or procedure relating to non-Islamist terrorist threats?

Immigration New Zealand and New Zealand Customs Service each have their own processes for identifying terrorism threats (Part 8, chapter 8).

Immigration New Zealand identify terrorism threats through their Risk Targeting Programme and the Advanced Passenger Process. They use risk indictors and target advice on terrorism to identify who may pose a threat. The targeting rules are mostly built around clusters of individual risk factors that, when present in a single travel record, indicate that the person may be a potential security risk. Where a risk is identified, Immigration New Zealand will

instruct the airline not to allow the person to board the plane. If the risk is identified too late to allow this to happen, an alert will be placed in New Zealand Customs Service's database and it will be addressed when the passenger arrives at the border.

New Zealand Customs Service run their own rules-based targeting programme across the Passenger Name Record, passport and flight data to identify people who may pose a risk and require intervention at the border. The rules-based targeting applies across the various issues New Zealand Customs Service tackle, such as drug smuggling, money laundering, objectionable material and terrorism. To identify terrorism risks New Zealand Customs Service use a terrorism risk profile developed by their intelligence team. The terrorism risk profile sets out a list of singular terrorism risks, which when combined into a rules-based targeting system can identify people of interest.

Before 15 March 2019, the border agencies, targeting rules and indicators for identifying potential terrorist threats at the border were primarily targeted at identifying Islamist extremist terrorist threats.

Immigration New Zealand had no specific targeting rule in place for electronically screening for extreme right-wing terrorism threats (such as travel history, age or sex).

New Zealand Customs Service had one indicator (which was added in 2013) relating to white supremacy and right-wing extremism to its counter-terrorism profile to assist frontline staff.

Do the border agencies know what countries a person entering New Zealand has travelled to?

Not always. It is not always feasible to obtain a person's full travel records. Technical and data sharing difficulties mean Immigration New Zealand generally do not hold the full travel history for an individual. The border agencies will, where necessary from time to time, request further travel information from overseas. However, getting detailed travel information may be a long process and involve international agreements (see Part 8, chapter 8).

Which countries a person has travelled to would raise red flags for entry into New Zealand, and why?

The national security instructions include a list of countries or territories of possible security concern including those known for extremism (see Part 8, chapter 8). This list is primarily focused on people who have connections with African, Asian and Middle Eastern countries.

Is it statistically likely for a person with the travel history of the individual to be stopped and searched or interviewed by New Zealand Customs Service?

This question assumes that the border agencies will know what countries a person has travelled to. This is not always the case. As set out in our answer to a previous question, it is not always feasible to obtain a person's full travel records. As discussed in *Part 6: What Public sector agencies knew about the terrorist*, the border agencies had limited information about the individual's travel history.

Do border agencies' processes vary depending on the country of citizenship or origin? If so, how?

Yes. Immigration New Zealand applies differing scrutiny to different travellers (see Part 8, chapter 8). The groups below are listed in order of the increasing scrutiny they receive:

- Australian citizens.
- Citizens from visa-waiver countries.
- Citizens from countries requiring visas to travel to New Zealand.
- People with connections to the countries in the national security instructions.

How many people were denied entry into New Zealand because they were determined to pose a risk to security, a threat to public order, or a threat to public interest in 2015–2019 by country of origin and ethnicity?

Immigration New Zealand do not record to this level of detail the reasons for declining entry permission. They do not record information on people who are refused entry to New Zealand based on security grounds, including their ethnicity and country of origin.

How do border agencies ensure that those entering New Zealand have never publicly made a racist statement or been a member of a racist group?

They do not. The Immigration Act does not state that a person must be excluded or denied entry permission from New Zealand for being a racist or a member of a racist group (unless that group is a designated terrorist entity). A person may be excluded or denied entry permission if they are likely to be a risk to security, public order or the public interest or on character grounds (see Part 8, chapter 8).

How many speakers with extremist (Islamist and non-Islamist) views were prevented from entering New Zealand before 15 March 2019? On what basis?

Immigration New Zealand's records cannot be searched using the criteria of their occupation (whether they are a speaker), their views or their religion.

In what instances has New Zealand Customs Service received complaints about racial or religious profiling?

Between 1 July 2019 and 30 June 2020, New Zealand Customs Service received 47 complaints, of which six complaints included allegations of potential discrimination based on racial or religious bias. This is similar to the number of complaints about racial or religious bias received in previous years. There were five allegations of racial and religious bias between 1 July 2017 and 30 June 2018 and again between 1 July 2018 and 30 June 2019. The complaints came from people spanning a range of ethnicities and nationalities. The complaints of racial or religious bias were investigated by New Zealand Customs Service, and none were found to be substantiated.

Is there a culture or institutionalisation of anti-Muslim bias at New Zealand Customs Service?

New Zealand Customs Service's risk identification rules are designed to identify people of terrorism concern. Before 15 March 2019, New Zealand Customs Service's targeting rules and indicators were primarily targeted at identifying Islamist extremist terrorism threats. While New Zealand Customs Service maintain that they do not deliberately target people based on their religious beliefs, the way that the risk identification rules and indicators operate mean that Muslim individuals are particularly susceptible to being stopped, questioned and searched at the border (see Part 8, chapter 8).

17.9 Experience of staff

How many full-time equivalent staff were dedicated to white supremacy and right-wing extremism compared to Islamist extremism in the 10 years before 15 March 2019?

No individual staff or teams across the counter-terrorism effort were solely focused on understanding and responding to the threat of right-wing extremism – they were also focused on Islamist extremist threats or other non-Islamist extremist threats.

Combined Threat Assessment Group

Before 15 March 2019 the Combined Threat Assessment Group generally had a full-time equivalent staff of five to seven analysts, each of whom worked on a range of terrorism threats. No analyst worked exclusively on the threat of right-wing extremism.

Government Communications Security Bureau

Approximate intelligence staff numbers (including graduates) dedicated to domestic counter-terrorism at the Government Communications Security Bureau[242] in recent years were two in 2015, four in 2016 (increased by graduates), two in 2017 and seven in 2018 (see Part 8, chapter 7). None of these staff worked solely on right-wing extremism.

Since 2016, all of the Government Communications Security Bureau's counter-terrorism activities have been in response to being tasked by another agency. Before 15 March 2019, the Government Communications Security Bureau was not tasked by any agency to conduct signals intelligence activities in relation to right-wing extremism.

Immigration New Zealand

Immigration New Zealand do not have a dedicated counter-terrorism team and therefore do not have any staff dedicated solely to counter-terrorism.

National Assessments Bureau

The National Assessments Bureau did not have a dedicated terrorism analyst until 2018, when one full-time terrorism analyst position was established. This analyst had responsibility across all terrorist ideologies.

New Zealand Customs Service

New Zealand Customs Service have a counter-terrorism intelligence team. Staff work across a range of threats, and therefore no staff are dedicated solely to the threat of right-wing extremism.

New Zealand Police

There were no staff dedicated solely to right-wing extremism within New Zealand Police. Staff in the National Security Investigations Team and Security and Intelligence Threats Group worked across all national security threats. Some of their time was spent investigating leads related right-wing extremism, however, the majority of staff time was dedicated to Islamist extremism.

[242] This number does not include staff in other areas of the Government Communications Security Bureau whose work may contribute in part to its counter-terrorism activity.

New Zealand Security Intelligence Service

As at May 2018, there were three investigative teams in the Counter-Terrorism Unit in the New Zealand Security Intelligence Service, comprising three team managers and 16 investigators. Each of the three teams had responsibility for Islamist extremist threats, and one team also had responsibility for non-Islamist threats. Twenty percent of investigator time was allocated to the baselining and discovery work programme, which included a project on domestic right-wing extremism.

In the years before mid-2018, the Counter-Terrorism Unit resources, as well as those of the collection group (such as surveillance, technical operations and human intelligence), were focused on the presenting threat of Islamist extremist terrorism.

What is the demographic breakdown of New Zealand Security Intelligence Service staff working on countering different forms of terrorism? Please provide available information on numbers of staff assigned (whether on a full-time or percentage basis), ethnic, religious and gender identities, capabilities and qualifications, and seniority.

The New Zealand Security Intelligence Service does not hold demographic statistics by directorate. This means the demographic breakdown of staff in the Counter-Terrorism Unit is not available.

As at June 2020, 12.1 percent of the New Zealand Security Intelligence Service workforce had an ethnically diverse background,[243] compared to 10.8 percent in June 2019. The New Zealand Security Intelligence Service had a target of having 13 percent of its workforce from ethnically diverse backgrounds by 30 June 2020, which it did not meet primarily because of a high turnover rate among ethnically diverse staff.[244]

The 2019 Arotake Review found that, although there had been a substantial increase in the number of investigators in the New Zealand Security Intelligence Service in 2018, half of the investigators had less than one year's experience at the time of the 15 March 2019 terrorist attack.[245] The Counter-Terrorism Unit was, however, led by experienced staff.

[243] This includes people of Māori, Asian, Pacific Island, Middle Eastern, Latin American and African descent.

[244] The figures here were provided to the Royal Commission. These figures are different to those listed in *Part 9: Social cohesion and embracing diversity,* which are sourced from the New Zealand Security Intelligence Service's and the Government Communications Security Bureau's annual reports. This is because they use different methodologies. The figures in agency annual reports are calculated using the Public Service Commission methodology, which uses the number of people who identify as being a certain ethnic group divided by the number who have provided an ethnic group. Conversely, the figures referenced above are calculated using the number of people who identify as being a certain ethnic group divided by the number of all staff (regardless of whether they list their ethnicity). We use the figures provided to the Royal Commission to answer the question above so that we are able to report on the New Zealand Security Intelligence Service's progress towards their ethnic diversity target.

[245] New Zealand Security Intelligence Service, footnote 57 above at page 59.

Did agency staff receive specialist training on white supremacy and right-wing extremism before 15 March 2019?

Government Communications Security Bureau

No. As the Government Communications Security Bureau was not tasked to undertake any work on right-wing extremism before 15 March 2019, staff did not receive any training on this subject matter and their focus remained on Islamist extremism.

New Zealand Customs Service

Yes. Since 2013, frontline New Zealand Customs Service staff have been provided with guidance on recognising the indicators of white supremacy and extremism while processing people at the border. This includes information on New Zealand and international groups of right-wing extremist interest, and information on indicators. In 2018 material on right-wing extremism was added to New Zealand Customs Services training material for frontline staff.

New Zealand Police

Yes. The type of training New Zealand Police staff received on white supremacy or right-wing extremism included the following:

- All staff had access to an awareness raising video on counter-terrorism which was available from 19 April 2018. This included material related to right-wing extremism.
- In 2018, a session on the counter-terrorism environment, issues and challenges was delivered to staff that attended the Serious Crime Course. It included a section on right-wing extremism.
- In 2018, a presentation titled *Extremist Threatscape* was delivered to the Advanced Police Negotiators Training course. It focused predominantly on Islamist extremism, but also referred to right-wing extremism including in New Zealand.
- Specialist national security staff received training primarily through the Australia New Zealand Counter-Terrorism Committee, including on right-wing extremism.

New Zealand Security Intelligence Service

No. The New Zealand Security Intelligence Service told us it does not run or commission training exclusively on white supremacy and right-wing extremism.

Since the commencement of the baselining and discovery work programme in mid-2018, New Zealand Security Intelligence Service staff have engaged with international and domestic partners in relation to a range of extreme ideologies, including right-wing extremism, and indicators of mobilisation to violence.

Have the National Assessments Bureau analysts with regional expertise developed adequate knowledge of nationalist and populist movements including their extremist fringes?

The National Assessments Bureau did not have a dedicated terrorism analyst until 2018, when one full-time terrorism analyst position was established. This analyst had responsibility across all terrorist ideologies.

The National Assessments Bureau produced two intelligence assessments related to right-wing extremism between 2010 and 15 March 2019 – one in 2013, and one in 2018.

Glossary

Term	Definition
Al Qaeda	An Islamist extremist terrorist organisation, which was responsible for the 11 September 2001 terrorist attacks on the United States of America.
assessment agencies	The Combined Threat Assessment Group (hosted by the New Zealand Security Intelligence Service) and the National Assessments Bureau (in the Department of the Prime Minister and Cabinet).
authorising environment	The environment that provides authority for a Public sector agency to operate effectively. Formal sources of authority include legislation, Cabinet decisions and budget approvals. Informal sources of authority include ministers, the central agencies, other Public sector agencies, stakeholders, communities, civil society and the private sector.
capacity and capability	Capacity describes whether there is enough of something (for example, staff) to achieve a certain outcome. Capability describes the ability to achieve a certain outcome, for example, whether people have the right knowledge, skills and technical tools.
central agencies	The Department of the Prime Minister and Cabinet, Te Kawa Mataaho Public Service Commission (formerly the State Services Commission) and the Treasury.
classical model of investigation	A model of counter-terrorism investigation that begins with lead information that is then investigated.
Combined Counter-Terrorism Investigations and Leads Meeting (Joint Leads Meeting)	A fortnightly meeting hosted by the New Zealand Security Intelligence Service and attended by the Department of Corrections, Immigration New Zealand, New Zealand Customs Service, New Zealand Police and (since September 2019) the Government Communications Security Bureau. Agencies bring leads they have and the other agencies can look across their own data holdings to provide further intelligence on the lead.
communications intelligence (COMINT)	Information derived from communications. The primary component of signals intelligence (SIGINT).
control orders	Court-imposed civil orders that place conditions or restrictions – such as curfews and electronic monitoring – on individuals who are seen to be at high risk of engaging in terrorism.

Term	Definition
counter-terrorism agencies	New Zealand Police and the New Zealand Security Intelligence Service.
counter-terrorism effort	Counter-terrorism activities undertaken by relevant Public sector agencies to detect terrorists and disrupt their organisation, planning, preparation and attacks.
counter-terrorism strategy	A framework used to guide the activities of the Public sector agencies involved in the wider counter-terrorism effort.
Dā'ish	Arabic acronym for the Islamic State of Iraq and the Levant (ISIL), also known as the Islamic State of Iraq and Syria (ISIS). An Islamist extremist terrorist organisation.
dark web	Part of the internet that is not visible to search engines and requires the use of specialist anonymising software to access.
deconfliction	A process that enables agencies to be aware of each other's activities where they are investigating the same subject of interest.
directive leadership	Involves a leader setting clear directions, objectives and expectations.
Director-General of the Government Communications Security Bureau	The chief executive of the Government Communications Security Bureau. This is a statutory title defined in the Intelligence and Security Act 2017.
Director-General of Security	The chief executive of the New Zealand Security Intelligence Service. This is a statutory title defined in the Intelligence and Security Act 2017.
domestic terrorism	Terrorism or terrorist activity that occurs in New Zealand. We note that this may differ from definitions used by others, including New Zealand's counter-terrorism agencies.

Term	Definition
far right	A range of views and ideologies that are underpinned by a strong form of nationalism that holds that Western civilisation and its values are under threat form non-native people (particularly immigrants) and ideas (such as multiculturalism). Both the radical right and the extreme right-wing fit under the broad umbrella of the far right. We do not use a hyphen for far right even when it is being used as an adjective.
Five Eyes	The intelligence sharing partnership between Australia, Canada, New Zealand, the United Kingdom and the United States of America.
"full take" collection	A phrase used by the Government Communications Security Bureau meaning collection and storage of all communications data collected from a communications link, before irrelevant or unwanted information has been filtered out.
human intelligence (HUMINT)	Information derived from covert human sources, private individuals who volunteer information, face-to-face meetings with individuals, community engagement and communications.
intelligence and security agencies	The Government Communications Security Bureau and the New Zealand Security Intelligence Service. This is a statutory term under the Intelligence and Security Act 2017.
international terrorism	Terrorism or terrorist activity that occurs outside New Zealand. We note that this may differ from definitions used by others, including New Zealand's counter-terrorism agencies.
Internet Protocol address (IP address)	A unique number linked to each device connected to a computer network that uses the Internet Protocol for communication.
lone actor terrorist	A single person operating alone to plan and carry out a terrorist attack.
metadata	Information about other data, such as the date the data was created, who created it, and who can access it.

Term	Definition
mobilisation	The process by which a radicalised person moves from an extremist intent to preparatory steps to engage in terrorist activity, such as researching potential targets, training or increased use of concealment behaviour.
New Zealand Intelligence Community	The Government Communications Security Bureau, the New Zealand Security Intelligence Service and the National Security Group of the Department of the Prime Minister and Cabinet (including the National Assessments Bureau).
Officials' Committee for Domestic and External Security Coordination (ODESC)	The primary governance board overseeing New Zealand's national security and resilience. Its main role is the identification and governance of national security risk. It is chaired by the Chief Executive of the Department of the Prime Minister and Cabinet.
operational security	Awareness and minimisation of behaviours that might attract attention from Public sector agencies.
Performance Improvement Framework	A tool, developed by the central agencies, for Public sector agencies and their chief executives to improve the performance of a Public sector agency.
Performance Improvement Framework review	A review of a Public sector agency completed by independent reviewers using the Performance Improvement Framework.
Public sector agency	In general, an organisation that works for the government of New Zealand. In this report, "Public sector agencies" means the 217 organisations listed in the appendix.
Public sector agencies involved in the counter-terrorism effort	The Department of the Prime Minister and Cabinet, the Government Communications Security Bureau, Immigration New Zealand, New Zealand Customs Service, New Zealand Police and the New Zealand Security Intelligence Service.
radicalisation	The process through which people develop commitment to a particular extremist ideology. People can radicalise to violence when they come to see violence as a feasible tool to address their grievances.

Term	Definition
radical right	Ideologies and beliefs that form part of the far right. Those on the radical right generally use democratic means to achieve their aims and do not openly endorse the use of violence as a legitimate tool to achieve their aims.
right-wing extremism	Ideologies and beliefs that form part of the far right. Those in the extreme right-wing often believe that democracy should be replaced, and they see non-democratic means, such as violence, as legitimate tools to achieve their aims. We use a hyphen for right-wing even when it is not being used as an adjective.
risk	The likelihood that a threat will occur, and the seriousness of consequences if it does. The more likely the threat and the more severe the likely consequences, the greater the risk.
sanitisation	Removing sensitive information (often by rewording the language) from a document so that it can be more widely distributed.
sensitive information	Information that, if disclosed, would be likely to cause damage to the security or defence of New Zealand, or to the New Zealand government's international relations, or prejudice the maintenance of the law or endanger the safety of a person.
signals intelligence (SIGINT)	Information derived from electronic communications ("signals" such as phone calls and emails), the primary component of which is communications intelligence (COMINT).
social licence	The ability of a business, organisation or government to do its work because it has the ongoing approval or acceptance of society to do so.
target hardening	A term used by law enforcement, security and military personnel to refer to the strengthening of a building or installation in order to protect it in the event of an attack. This can include security measures like installing closed-circuit television (CCTV) and alarms.
terrorist cell	A small semi-independent or entirely separate unit of a larger terrorist organisation.
threat	A source of potential damage or danger.

Term	Definition
threatscape	The threat environment.
Tor browser	Software that allows users to surf the web anonymously by concealing the user's location as well as what they are looking at online. It can also be used to access the dark web.
tradecraft	Operational (often secret) practices.
Virtual Private Network (VPN)	Software that allows the user to create a secure connection to another server over the internet. Once connected, the user can browse the internet using that server. In doing so, the user is provided with an Internet Protocol (IP) address associated with the different server, which hides the user's location.
wider counter-terrorism effort	Public sector agencies that contribute to or support the counter-terrorism effort, including: – the agencies involved in the counter-terrorism effort (the Department of the Prime Minister and Cabinet, the Government Communications Security Bureau, Immigration New Zealand, New Zealand Customs Service, New Zealand Police and the New Zealand Security Intelligence Service); and – agencies who can play a role in supporting counter-terrorism activities where it overlaps with their functions, including Public sector agencies (such as the Department of Internal Affairs, the Ministry of Education and the Ministry of Foreign Affairs and Trade).
wider New Zealand Intelligence Community	The group of Public sector agencies that collect, assess or otherwise use intelligence and those agencies that collect and/or use intelligence for external or domestic policy and operations. This includes agencies in the New Zealand Intelligence Community (the National Security Group of the Department of the Prime Minister and Cabinet, the Government Communications Security Bureau and the New Zealand Security Intelligence Service) and other agencies such as the Department of Corrections, Immigration New Zealand, the Ministry for Primary Industries, New Zealand Customs Service, the New Zealand Defence Force and New Zealand Police.