Assessing Terrorism Threats to New Zealand: The Role of the Combined Threat Assessment Group

Author/s: Combined Threat Assessment Group (CTAG)
With Foreword by Rebecca Kitteridge

ASSESSING TERRORISM THREATS TO NEW ZEALAND: THE ROLE OF THE COMBINED THREAT ASSESSMENT GROUP

with Foreword by Rebecca Kitteridge[1]

This article has been produced by the Combined Threat Assessment Group (CTAG). It provides in detail, and publicly for the first time, a genuinely informed explanation for the origins and function of CTAG. It covers the nature and challenge of threat assessment, the methodology applied as well various iterations of the threat assessments that are undertaken. This leads on to an explanation of how New Zealand's National Terrorism Threat Level is set. Overall, this article provides an informative and well-rounded explanation of the components that comprise the National Terrorism Threat Level and makes for essential reading for wider public service, academic, and security conscious public and private institutions across the country.

Keywords: Combined Threat Assessment Group (CTAG), Threat Assessment, National Terrorism Threat Level, National Security System.

Foreword

The Combined Threat Assessment Group has been playing a vital role in New Zealand's national security system for the last 16 years, so I am delighted that the *National Security Journal* has given the team the opportunity to tell its story; to shed some light on its inner workings and maybe even dispel a few myths.

I have read countless CTAG assessments since I become Director-General of Security, and while a customer in previous roles. I am consistently impressed with the rigour of their analysis and appreciative of the insight they are able to offer key decision makers across government.

---

1   The identities of this article's authors have necessarily been withheld due to the nature of their roles within CTAG. Rebecca Kitteridge is Director General of Security.

The work of CTAG is also well regarded by our partners overseas. The Group boxes well above its weight in comparison to its counterparts overseas, which have much bigger teams and can draw upon significantly more resources. CTAG has become expert at tapping those resources adeptly to build its understanding on the evolving drivers of terrorism and violent extremism in New Zealand and abroad.

Conducting threat assessments is not an easy task. It is a complex job and a big responsibility, especially considering there is no exact science to fall back upon and that assessments rely on incomplete or ambiguous information. I hope this article begins to raise the level of understanding about the likelihoods and probabilities the members of CTAG have to weigh up every day. It is critical work, carried out with dedication to the mission of keeping New Zealanders safe.

Introduction

Periodically, the New Zealand terrorism threat level, and the inter-agency unit responsible for assessing it, hits the headlines. Unfortunately, this coverage tends to coincide with a revelation to the New Zealand public of dangers to our safety and national security; little information has been available for the media or the public to understand the significance of threat levels, how they are assessed and by whom. It is unsurprising then that the role of the Combined Threat Assessment Group (CTAG) and the specific purpose of threat assessment is overlooked or misunderstood.

In the absence of information, misinterpretations can carry undue weight. In February 2020, a media article incorrectly reported that CTAG "detectives" were "investigating" an individual and speaking with their family and close associates.[1] This was not the case, nor did the article accurately describe CTAG's responsibilities. The article did, however, highlight the need for CTAG to more proactively inform and educate the New Zealand public about CTAG and correct past misunderstandings. This article offers an overview of CTAG's role and functions, methodologies and our place in New Zealand's national security system, particularly in relation to assessing and setting the National Terrorism Threat Level.

CTAG Overview

CTAG's creation was confirmed by Cabinet in February 2004, following a recommendation from the Officials Committee for Domestic and External Security Coordination (ODESC) that a 'combined agency group' be responsible for the provision of threat assessments and the evaluation of threat warning intelligence and information. CTAG's creation followed a pattern among close international partners in Australia, Canada, the United Kingdom and the United States of establishing multi-agency

terrorism analysis and threat assessment centres after the 11 September 2001 terrorist attacks in the United States and, particularly for New Zealand and Australia, the 2002 Bali bombings in Indonesia. The threat assessment centres brought together a range of national security, intelligence and law enforcement agencies to facilitate and ensure information sharing and collaborative analysis in order to provide their governments with all-source, authoritative threat assessments.

CTAG is specifically charged with providing government with "timely and accurate assessment of […] threats to New Zealanders and New Zealand interests". CTAG does not assess all potential security threats, but is mandated to primarily focus on terrorism (including violent extremism in advance of any terrorist acts), as well as threats from violent protest and violent crime (the last, only abroad).

CTAG is a multi-agency unit with staff seconded from a range of state sector agencies, which has evolved over time. Today, CTAG is staffed by secondees from the Civil Aviation Authority, Department of Corrections, Government Communications Security Bureau (GCSB), New Zealand Defence Force (NZDF), New Zealand Police, and New Zealand Security Intelligence Service (NZSIS). In addition to these agencies' contributions, funding is also provided by the New Zealand Customs Service (NZCS) and the Ministry of Foreign Affairs and Trade (MFAT). In addition, the National Assessments Bureau (NAB) within the Department of Prime Minister and Cabinet (DPMC) is an associate member of CTAG, providing specialist contributions to and regular peer review of CTAG reporting.

CTAG has been subject to two organisational reviews since its creation, and has been described as "in and of" NZSIS, which provides CTAG administrative, technical and logistical support. However, CTAG retains analytical independence to minimise 'capture' or undue influence by any one of the contributing agencies. CTAG is recognised as one of the New Zealand government's primary assessment agencies and, as such, relies on information and intelligence gathered or generated by contributing agencies and open source. CTAG cannot enforce measures for national security or acquire an intelligence warrant under the *Intelligence and Security Act 2017*, and does not have any investigative powers afforded to the contributing agencies, despite media reporting to the contrary.

Threat Assessment Overview

New Zealand is exposed to a range of national security risks, managed by multiple government agencies and coordinated by DPMC.[2] Dependent on their origins, these risks are either classified as 'hazards' or 'threats' – with the former being natural (such as earthquakes) and the latter requiring human agency (such as terrorism).

---

2   For further information, refer DPMC's National Security System Handbook, August 2016.

Risk: assessing likelihood and consequence of an event

Within the risk management process, threat assessment is distinct from risk assessment. To adequately assess risk, risk assessors require an understanding of the likelihood of an event occurring, and the range of consequences if the event were to manifest. These 'likelihood' and 'consequence' assessments provide a clear understanding of the exposure to that risk, and assist with identifying any mitigation or management efforts required to reduce the likelihood of that risk causing harm.

Figure 1: Contributing factors in threat and risk assessments
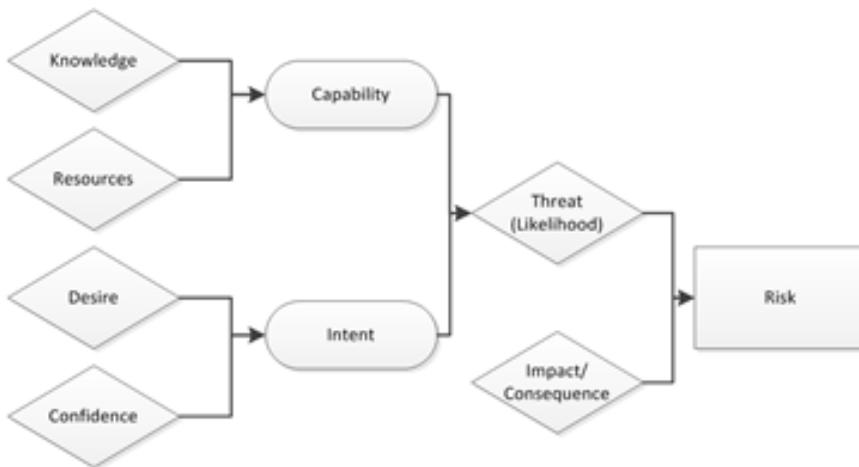
The primary purpose of the threat assessment process is to inform risk appreciation, mitigation and management (refer Figure 1 above). Threat assessment is not an end in itself, nor should it be confused with a conclusive statement of the vulnerability of New Zealand or New Zealand interests to harm. State sector agencies are responsible for their own risk management, which is informed by a range of government policies, including health and safety obligations and the Protective Security Requirements (PSR) framework.

Threat: assessing the intent and capability of an actor

Threat assessment is the analytical process focused on assessing the likelihood of a threat, or human-driven event, manifesting. The primary purpose of threat assessment is to inform the 'likelihood' component of a risk assessment framework. When assessing the likelihood of a threat manifesting, two core elements are considered: the actors' intent (i.e. the desire to inflict harm, coupled with the confidence to do so), and whether they possess the capability (i.e. the access to knowledge and resources required to conduct harm) to do so.

Assessment of intent and capability has been the common approach towards threat assessment since David Singer formalised the practice within academic literature in his 1958 analysis of the armament-tensions dilemma[2]. Singer identified that states perceive the extent of a threat through the assessment of their adversaries estimated intent and estimated capability. Since Singer's intent-capability threat assessment matrix was developed, academics and security practitioners have applied and integrated this approach to a range of industries, from psychology to law enforcement.[3] While there have been different threat assessment frameworks to address specific threats, the core focus of these remain on understanding the intent and capability of actors to better assess the likelihood of the threat manifesting.

Communicating the likelihood of an event manifesting

When assessing the likelihood of a terrorist attack occurring, threat analysts make predictions about whether a future event will or will not occur. Future predictions involve an inevitable degree of uncertainty due to the range of alternative events that could also occur. When making anticipatory judgements, such as threat assessments, analysts use probabilistic language – a set of qualitative terms that express estimations of likelihood. Probabilistic language aids with communicating the degree of uncertainty within assessments, acknowledging how alternative scenarios compare and are supported by the information currently available. In general terms, the more likely an event is assessed to occur, the less likely the alternative scenarios are.

Figure 2: guidance on what probabilistic, qualitative terms can mean

Almost Certain	A scenario that has only a remote chance of not occurring or not being currently accurate. In such cases, alternative scenarios are highly unlikely.
Highly Likely	A scenario that has only a small chance of not occurring or not being currently accurate. Alternative unlikely scenarios will remain, but the highly likely scenario is dominant (alternatively, very likely, highly probable, or very probable).
Likely	A scenario that is more likely than not to occur or be currently accurate (alternatively, probable). In such cases, alternative scenarios remain, but do not outweigh the likely scenario (alternatively, probable, or could well occur).
Possible	A scenario that has a realistic chance of occurring or being currently accurate, but which does not outweigh all other alternative possibilities (alternatively, realistic possibility).
Unlikely	A scenario that is plausible, but which has only a small chance of occurring or being currently accurate (alternatively, improbable).
Highly unlikely	A scenario that only has a remote chance of occurring or being currently accurate. In such cases, alternative scenarios are highly likely (alternatively, remote)

Figure 3: How the probabilistic, qualitative terms relate to each other

<< Lower likelihood			Even chance		Higher likelihood>>	
Highly unlikely	Unlikely	Possibly Possible Realistic possibility	Likely Probable Probably		Highly likely	Almost certain

When used in risk assessment frameworks, the likelihood assessment is often represented by a threat level. For the National Security System risk assessment framework, CTAG conveys its assessment of the likelihood of a terrorist attack occurring on a scale from VERY LOW to EXTREME (see Figure 4 below). This follows a change in methodology from a six to a five-tiered threat level framework with effect from 1 July 2020. Although the level descriptors were updated to better reflect probabilistic language, the descriptor for MEDIUM has remained as "feasible and could well occur", placing it in the mid-range for probabilistic language spectrum. Importantly, the parameters of the levels themselves have not changed (with the exception of VERY LOW, which expanded to include former NEGLIGIBLE assessments). Accordingly, aside from the now defunct 'negligible' level, all threat levels set before 1 July 2020 did not require adjustment, including the National Terrorism Threat Level.

Figure 4: Past and current CTAG threat levels

Previous Threat Levels		Threat Levels from 1 July 2020	
Likelihood Statement	**Level**	**Likelihood Statement**	**Level**
Terrorist attack, violent protest activity or violent criminal behaviour is expected imminently	**EXTREME**	Terrorist attack, or violent protest, or violent crime is expected	**EXTREME**
Terrorist attack, violent protest activity or violent criminal behaviour is assessed as very likely	**HIGH**	Terrorist attack, or violent protest, or violent crime is assessed as highly likely	**HIGH**
Terrorist attack, violent protest activity or violent criminal behaviour is assessed as feasible and could well occur	**MEDIUM**	Terrorist attack, or violent protest, or violent crime is assessed as feasible and could well occur	**MEDIUM**
Terrorist attack, violent protest activity or violent criminal behaviour is assessed as possible but not expected	**LOW**	Terrorist attack, or violent protest, or violent crime is assessed as a realistic possibility	**LOW**
Terrorist attack, violent protest activity or violent criminal behaviour is assessed as unlikely	**VERY LOW**	Terrorist attack, or violent protest, or violent crime is assessed as unlikely	**VERY LOW**
Terrorist attack, violent protest activity or violent criminal behaviour is assessed as very unlikely	**NEGLIGIBLE**		

CTAG's Threat Assessment Methodology

CTAG analysts assess the likelihood of the threat of physical harm from terrorism, violent protest or violent crime (abroad) occurring in a specific environment, targeting a specific entity, or emanating from a specific individual or group by assessing the intent and capability of relevant threat actors and considering broader environmental factors. Methodologies have been adapted to meet New Zealand National Security System requirements and are intended as analytical guides to provide analysts with greater confidence during assessment development. Robust analysis is achieved through application of structured analytical techniques and logical reasoning techniques, which draw upon well-regarded international academic and institutional research, as well as analyst training in the identification and mitigation of conscious and unconscious bias.

The process of using multiple analytical and logical reasoning techniques helps analysts understand incomplete data sets and test different hypotheses. The assessment of the likelihood of a threat manifesting is therefore a product of robust and thorough intelligence analysis of the factors constituting the threat (intent and capability). Techniques used include, but are not limited to, the Inference Development Model (IDM) and Pattern and Trend Analysis (PTA):

- The IDM encourages strong logical reasoning by using identified indicators to develop premises, which together form an inference or explanation of what available information means or could mean.

- PTA employs an analyst's understanding of the environment's past or current patterns or trends (subject matter expertise), and requires the analyst to recognise and articulate assumptions that a past pattern of activity will repeat or current trends will hold true.

The final likelihood assessment is reliant on analytical judgements specific to the particular environment. These judgements are clearly articulated and recorded. Similarly, intelligence gaps hindering analytical confidence in assessments are clearly articulated. CTAG acknowledges, for example, that the threat of the unknown actor will always be present and is unavoidable in intelligence analysis. Use of structured analytical techniques and logical reasoning techniques therefore also assist in developing an understanding of the likelihood of individuals being present in the environment with the intent and capability to cause harm *who are unknown to authorities*.

A brief overview of the three types of Threat Assessment produced by CTAG, based on the above methodologies, is provided below.

Environmental Threat Assessment

CTAG analysts assess the general likelihood of a threat of physical harm (from terrorism, violent protest or violent crime) occurring in a particular environment, usually a specified country. This likelihood assessment, represented by a threat level, is the baseline assessment for the environment. An overview of the process, using the example of assessing the likelihood of a terrorist attack, is as follows:

1. Assessment of the likelihood there are individuals in the environment with intent to conduct an attack. For example, *there are **likely** individuals in the environment with the current intent to conduct an attack*.

2. Assessment of the likelihood of individuals in the environment assessed as having current intent and who have, or could acquire, capability to conduct an attack. For example, *it is **likely** individuals in the environment assessed to have current intentions to conduct an attack have, or could acquire, the capability to conduct the intended attack*.

3. Assessment of the likelihood of physical harm occurring in the environment, and identification of the appropriate threat level. For example, CTAG assesses the terrorism threat level in Country X is **MEDIUM**; *terrorist attack is assessed as feasible and could well occur*.

Specifically Targeting Threat Assessment

An assessed environmental threat level does not necessarily dictate the assessed threat level for a New Zealand Interest, Major Event, or Travel of Internationally Protected Persons (IPP) present or occurring in that environment. Rather, an assessment pertaining to one of these interests can be conducted by way of a Specifically Targeting Threat Assessment (STTA). The same process used for an Environmental Threat Assessment is applied, but focuses on the likelihood of a terrorist attack (for example) targeting a New Zealand Interest, Major Event or IPP within the context of the relevant environment. An example of a resulting threat level assessment is as follows:

> CTAG assesses the threat of terrorism specific to [Major Event A] is
> **LOW**; *terrorist attack is assessed as a realistic possibility*.

An STTA threat level will almost always be consistent with, or lower than, the assessed environmental threat level. A Threat Stream Threat Assessment may result in a temporary exception to an Environmental Threat Assessment or STTA.

Threat Stream Threat Assessment

A particular threat emanating from a specific group or individual within an environment is referred to by CTAG as a Threat Stream. Threat Stream Threat Assessments (TSTAs) therefore assist with determining if a Threat Stream is consistent with the assessed

Environmental Threat Level. If a Threat Stream is assessed at a level higher than the Environmental Threat Level, a reassessment of the Environmental Threat Level, and any Specifically Targeting Threat Levels if applicable, takes place. Threat Stream Threat Levels are not necessarily published, but aid analysts in articulating workings behind a TSTA, and its impact on the environment.

A change to an Environmental Threat Level based on a Threat Stream is clearly articulated using Threat Stream Caveats, which detail information on locality, coordination and sophistication. This differentiates Threat Stream change from a change to the threat level due to the broader threat environment. This nuance is designed to assist customers with adequately and proportionately responding to any change in Threat Level. A Threat Level change due to a specific Threat Stream also remains under constant review and is revised in due course.

Setting of the National Terrorism Threat Level and Informing the National Security System

In September 2019, the External Relations and Security (ERS) Cabinet sub-committee acknowledged CTAG would in the future produce an annual national terrorism threat assessment, including a formal review of the National Terrorism Threat Level. Despite these annual reviews, CTAG continuously monitors the threat environment and can revise the National Terrorism Threat Level at any time. This was evidenced immediately after the 15 March 2019 Christchurch terrorist attack when the National Terrorism Threat Level was raised from LOW to HIGH, and then revised to MEDIUM on 17 April 2019.

CTAG's threat assessments, including the National Terrorism Threat Level, inform wider government agencies of the physical threat to New Zealand and New Zealanders from terrorism, but do not recommend actions to mitigate these threats. For example, following the lowering of the threat level from HIGH to MEDIUM in April 2019, New Zealand Police made the operational decision to end routine arming of frontline officers, which had been implemented following the raising of the threat level from LOW to HIGH on 15 March 2019.

CTAG assessments undergo rigorous multi-agency peer review before CTAG finalise the National Terrorism Threat Level recommendation. Given the significance of the threat level to government risk management responses, ERS vested the Director-General of Security (the Chief Executive of NZSIS) with responsibility for setting the level. The Director-General of Security then informs the Chair of ODESC of all national threat level decisions. When the Director-General of Security changes the threat level on CTAG's advice, ODESC considers the appropriate response and makes recommendations to Ministers and the Prime Minister.

In addition to informing agency security settings, CTAG's reporting is intended to support systematic consideration of counter-terrorism system priorities, and provide the basis for any public statements on the threat environment. Government agencies also draw on CTAG threat assessments to support risk assessment and risk management activities offshore, such as informing travel advisories and security planning for major events.

Despite attracting national prominence, CTAG threat levels are not intended as a public messaging tool, and a change in threat level does not necessarily require a specific response from the general public. As such, the decision to publicise the national threat level lies with the Government of the day. Any messaging to the public regarding forewarning of a terrorist attack should be part of a risk management strategy, informed by a threat assessment.

Concluding remarks

The threat assessments CTAG produces are an important part of the national security and risk management mechanisms of the New Zealand government in response to terrorism, as well as violent protest and violent crime (abroad). These assessments intentionally focus on actors who mean to physically harm New Zealand and New Zealand interests, and evaluate the nature of their hostile intent and capability to conduct their desired attack. This requires a combination of science and art; a clear methodology with a depth of subject-matter understanding and intuition. Despite their system-level value, threat assessments and their associated threat levels should not be misinterpreted as a conclusive statement about the vulnerability of New Zealand or its people and interests abroad. They describe a start point, not an end state.

This paper has focussed on CTAG's role in the national security system and its threat assessment methodology. The assessment of specific threats remains CTAG's core function, but CTAG and New Zealand's intelligence services must remain alert to the emergence of new forms of violent extremism. In recognition of its analysts' understanding of the diverse drivers of terrorism and violent extremism in New Zealand and abroad, from 1 July 2020 CTAG expanded its focus towards identifying and analysing emerging violent extremist threats. These horizon-scanning 'Insight' reports are designed to support government agencies to consider responses and possible mitigations at the earliest opportunity.

---

1   Kerr, D., & Manch, T. (2020). Counter-terror investigation into soldier. *The Dominion Post*. 1 February 2020.

2   Singer, D. (1958). Threat-Perception and the Armament-Tension Dilemma. *The Journal of Conflict Resolution, 2* (1), 90-105.

3   Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). *Behavioural Sciences and the Law*, 17, 323-337; also see:

Campbell, J. C., Glass, N. E., Sharps, P. W., Laughon, K., & Bloom, T. *(2007) Intimate Partner Homicide: Review and Implications for Research and Policy. Violence, Trauma and Abuse, 8, 246-269;*

Cole, J., Alison, E., Cole, B., Alison, L. *(2009). Guidance for Identifying People Vulnerable to Recruitment into Violent Extremism. University of Liverpool: School of Psychology.*

Davis, P. K., Perry, W. J., Hollywood, J. S., & Manheim, D. (2016). *Uncertainty-Sensitive Heterogenous Information Fusion: Assessing Threat with Soft, Uncertain, and Conflicting Evidence.* Santa Monica, CA: RAND Corporation.

Fein, R., Vossekuil, B., (2000). *Protective Intelligence and Threat Assessment Investigations: A Guide for Local Law Enforcement Officials.* Washington, D.C.: United States Department of Justice;

Harding, D. (2014). Threat Management: The Coordinated Focus on the Threat Actor, their Intentions, and Attack Cycle. *Journal of Applied Security Research, 9,* 478-494.

James, D. V., Kerrigan, T., Forfar, R., Farnham, F., & Preston, L. (2010). The Fixated Threat Assessment Centre: preventing harm and facilitating care. *Journal of Forensic Psychiatry and Psychology, 21,* 521-536.

Koçak, M. (2012). Threat Assessment of Terrorist Organisations: the Application of Q Methodology. *Journal of Risk Research, 15* (1), 85-105;

Malone, R. (2015). Protective Intelligence: Applying the Intelligence Cycle Model to Threat Assessment. *Journal of Threat Assessment and Management, 2* (1), 53-62.

McKenna, B. G., Poole, S. J., Smith, N. A., Coverdale, J. H., & Gale, C. K. (2003) A survey of threats and violent behaviour by patients against registered nurses in their first year of practice. *International Journal of Mental Health Nursing, 12,* 56-63.

Meloy, J. R., Roshdi, K., Glaz-Ocik, J., & Hoffman, J. (2015). Investigating the Individual Terrorist in Europe. *Journal of Threat Assessment and Management, 2* (3), 140-152.

Meloy, J. R., Hoffman, J., Roshdi, K. & Guldimann, A. (2014). Some Warning Behaviours discriminate between school shooters and other students of concern. *Journal of Threat Assessment and Management, 1*(3), 203-211.

Meloy, J. R., Hoffman, H., Guldimann, A., & James, D. (2012). The Role of Warning Behaviours in Threat Assessment: An Exploration and Suggested Typology. *Behavioural Sciences and the Law*, 30, 256-279;

Reddy., M., Borum, R., Berglund, J., Vossekuil, B., Fein, R., & Modzeleski, W. (2001). Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches. *Psychology in Schools, 38*(2), 157-170;

Tusikov, N., Fahlman, R. (2008). Threat and Risk Assessments. In Ratcliffe, J (ed.). *Strategic Thinking in Criminal Intelligence* (2nd edition). The Federation Press, NSW: Leichhardt.

Vandepeer, C. (2011a). *Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non State Actors*. (Doctoral Dissertation, University of Adelaide: School of History and Politics, Australia).