THREAT INSIGHT
CTAG Glossary – 2021 Update

Issued: 5 November 2021

21-151-TI

(R) This product provides descriptions of core concepts and common language related to CTAG's assessment of terrorism, violent protest and violent crime threats. This is intended to be a living document, to be updated periodically to incorporate developments in our understanding of terrorism language, partner terminologies and lessons learned. Additions or alterations to the previous edition [20-230-TI refers] are denoted in red.

CTAG Mandate

1. **Terrorism:** Under New Zealand law, a terrorist act is defined as an ideologically, politically, or religiously motivated act – including, but not limited to, those causing death or serious bodily injury – intended to intimidate a population, or to compel the government to do or not do certain things. (see also New Zealand's *National Strategy for Countering Terrorism and Violent Extremism*).

2. **Violent Protest:** a premeditated decision or agreement by a group of protestors to commit violence against people or significant damage to public or private property, as part of their protest activity. This includes acts of sabotage, which may be conducted outside formal protest activity, for ideological reasons. [21-25-TI refers].

3. **Violent Crime:** violent, organised criminality with the potential to target New Zealanders and New Zealand interests abroad.

Violent Extremism

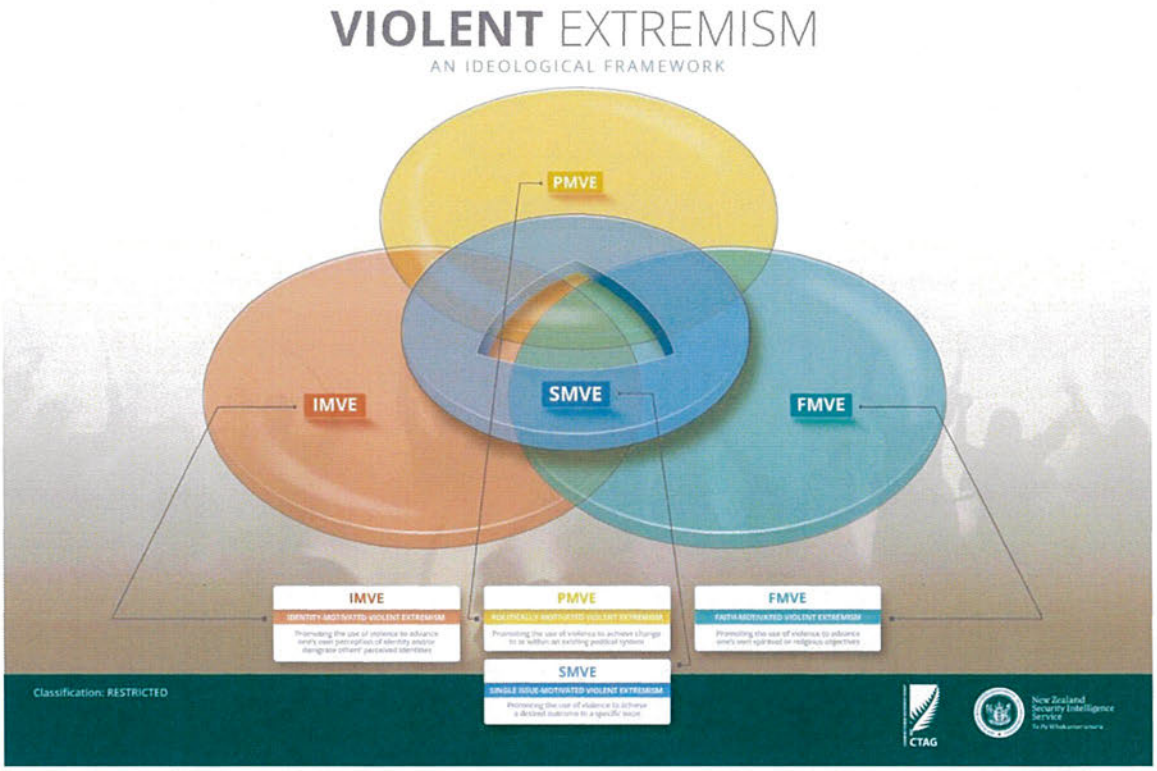
4. **Ideology:** a set of ideals, principles, doctrines, myths, or symbols of a social movement, institution, class, or group that explains how society should work, and offers some political and cultural plans for a certain social order.

5. **Extremism:** Religious, social or political ideologies that exist substantially outside of more broadly accepted belief systems in large parts of society, and are often seen as objectionable to large parts of society. Extreme ideologies may seek change in government, religion or society or to create a community based on their ideology (per *National Strategy for Countering Terrorism and Violent Extremism*).

6. **Violent Extremism:** the justification of violence to achieve a change in government, religion or society. This violence is often targeted against groups seen to threaten violent extremists' success or survival or undermining their worldview (per *National Strategy for Countering Terrorism and Violent Extremism*).

a. **Violent Extremist [individual]:** a person exhibiting a deep commitment to a violent extremist ideology, whether or not they have personally committed an act of violence. (To be used sparingly)
b. **Violent Extremist Organisation/Group:** an organisation or group adhering to or promoting a violent extremist ideology, whether or not it has committed an act of violence.

7. **Violent extremist ideology:** one or a combination of four overarching ideological motivations [20-229-TI refers]. These motivations also include individuals who identify as following an ideology or violent extremist organisation without having a formal connection to either. They also include individuals who use an ideology, or claim an affiliation, as a pretext to justify violence in pursuit of personal grievances.



8. **Identity-Motivated Violent Extremist (IMVE):** promoting the use of violence to advance one's own perception of identity and/or denigrate others' perceived identities.
   a. **White IMVE:** an ultra-conservative ideology, promoting violence to oppose progressive change from a perceived ideal dominated by white, European-descended heterosexual males [21-94-TI refers].
   b. ***Hindutva* IMVE:** an extreme form of Hindu nationalism that advocates for Hindu supremacy in India, based on the denigration of others for their identity as "non-Indian" [21-36-TI refers].
   c. **Involuntary Celibates ('Incel') IMVE:** individuals who advocate violence against the opposite sex for denying them sexual relationships to which they believe themselves entitled [21-79-TI refers].

9. **Politically-Motivated Violent Extremist (PMVE):** promoting the use of violence to achieve change to or within an existing political system.
   a. **Khalistani PMVE:** intent on re-establishing an independent Sikh homeland in the Punjab area of India [21-32-TI refers].
   b. **Uyghur PMVE:** intent on the re-establishment of a Uyghur homeland in East Turkistan in the western People's Republic of China [21-134-TI refers].

10. **Faith-Motivated Violent Extremist (FMVE):** promoting the use of violence to advance one's own spiritual or religious objectives.

11. **Single Issue-Motivated Violent Extremist (SMVE):** promoting the use of violence to achieve a desired outcome to a specific issue. Ordinarily used only in combination with one of the above.

12. **Radicalisation:** the process by which an individual progressively adopts a violent extremist ideology (see above).
    a. **Radicalisation Pathway:** the sequence of steps taken by an individual in their radicalisation.

13. **Mobilisation [to violence]:** the process by which a radicalised individual takes steps to undertake an act of extremist violence.

14. **Disengagement [from violence]:** the process whereby individuals move away from, or discontinue, actions associated with supporting and/or preparing for acts of terrorism or violent extremism.

Threat Actors

15. **Threat Actor:** an individual, group or organisation presenting a threat of terrorism, violent protest or violent crime.

16. **Movement:** a collection of entities or individuals, united around a central ideology, but functioning autonomously.

17. **Organisation:** a formal entity comprising multiple individuals, with a recognisable hierarchy and structure, acting in concert towards a collective goal.

18. **Group:** an informal collection of individuals, with little or no recognisable hierarchy or structure, acting in concert towards a collective goal.

19. **Lone Actor:** an individual committing, or seeking to commit, a violent act without direct participation from others in the act itself.

20. **Foreign terrorist fighter:** An individual who has travelled outside their country of citizenship or typical residence in order to participate in the activities of a terrorist organisation offshore.

21. **State-sponsored terrorism:** the threat actors have been enabled and/or directed by a recognised sovereign state or official component thereof.

22. **Non-state actor:** a threat actor operating without the support or direction of a sovereign state.

23. **Degrees of involvement**
    a. **Directed:** a threat actor is acting on the orders of a violent extremist individual, group or organisation, which has provided oversight and direct material support to the operation (e.g. 9/11 attacks).
    b. **Enabled:** a threat actor, in pursuit of a self-determined goal, has personally received specific instructional, material, logistical or ideological support from a violent extremist group or individual (e.g. 2009 Fort Hood attack).
    c. **Inspired:** a threat actor has been motivated to act by violent extremist rhetoric, individuals, groups and/or other attacks but has no apparent direction or support from a violent extremist individual, group or organisation (e.g. 2019 Christchurch attacks).

Threats

24. **Threat:** the intent and capability of an actor to carry out an act of terrorism, violent protest or violent crime (i.e. *posing* a threat).

25. **Threatening Rhetoric:** hostile statements intended to inspire or intimidate, regardless of an actor's actual 'intent' or 'capability' to follow through on the stated intention (i.e. *making* a threat). This could include instances where the actor's purpose is to buy credibility within their own ideological circle, rather than present a threat to the ostensible target of the rhetoric.

26. **Intent:** a threat actor's desire, resolve and planning to inflict harm.

27. **Capability:** a threat actor's access to the knowledge and resources required to conduct harm [21-80-TI refers].
    a. **Advanced:** capabilities in the environment that require an advanced level of access, coordination, training, and technology.
    b. **Intermediate:** capabilities in the environment that require an intermediate level of access, coordination, training, and technology.
    c. **Basic:** capabilities in the environment that require a basic level of access, coordination, training, and technology.

28. **Target**
    a. **(noun):** the location or entity intended to be attacked by a threat actor.
        i. **Hard target:** a location or entity with extensive security measures, including fortifications and restricted access (e.g. a military base in a combat zone).
        ii. **Soft target:** an easily accessible location or entity with minimal or no security measures (e.g. an open-air market).
        iii. **High-profile target:** a location or entity with significant public profile, targeted with the intent to attract attention (e.g. a prominent landmark, government facility, politician or celebrity).
    b. **(verb):** the act of selecting and pursuing the specific 'target' (noun) of an attack.

29. **Disruption:** attack planning has been permanently or temporarily halted, typically by government action (e.g. the arrest of one or more participants) (also see: 'interdicted attack').

30. **Locality**
    a. **Localised threat:** contained to a specific geographic area and are not representative of the threat in other parts of the country.
    b. **Non-Localised threat:** spread throughout the country or could occur anywhere in the country.

31. **Coordination** (also see: 'sophistication' and 'complex attack')
    a. **Coordinated threat:** involving the coordination of efforts with other parties in a way that amplifies the threat.
    b. **Uncoordinated threat:** an individual or a group of persons who share an end goal but undertake acts without meaningful coordination with others.

32. **Timeframes**
    a. **Imminent:** the event is to occur within the next three weeks (21 days)
    b. **Short-term:** within six months
    c. **Medium-term:** between six months and three years
    d. **Long-term:** over three years
    e. **Enduring:** there is no foreseeable end point at this time

Attacks

33. **Terrorist act/attack:** a deliberate act of violence by a threat actor that meets the threshold for 'terrorism' (also see: section 5, *Terrorism Suppression Act 2002*).

34. **Opportunistic attack:** a threat actor conducts an attack with little to no planning by taking advantage of a change in target, environment, or event; *or* a threat actor establishes an operational plan without a specific target with the intent to attack targets of opportunity present in a certain area.

35. **Complex attack:** an attack involving a high degree of coordination or sophistication, potentially including multiple targets, simultaneous timing, multiple capabilities etc.

36. **Copy-cat attack:** an attack intended to evoke a previous attack by replicating its tactics and/or targets, sometimes imminently after the original attack.

37. **Retaliatory attack:** an attack carried out against the real or perceived perpetrators of an attack, often purportedly to avenge the victims (*alt.* **reprisal attack**)

38. **Insider attack:** an attack conducted or facilitated by an employee or associate of the targeted site or organisation (e.g. "green on blue" or "blue on blue").

39. **Mass casualty attack:** an attack inflicting or intended to inflict more than 10 deaths or injuries.

40. **Incidental harm:** damage or harm inflicted to targets beyond the intended target of an attack (*alt.* **collateral damage**).

41. **Interdicted attack:** the threat actors have been intercepted *en route* to the attack, causing the attack plot to be temporarily or permanently disrupted (see also 'disruption').

Probabilistic Language

42. **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.

43. **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 (*alt.* **very likely**, **highly probable**, **very probable**).

44. **Likely:** a scenario that is more likely than not to occur or be currently accurate. In such cases, alternative scenarios remain, but do not outweigh the likely scenario (*alt.* **probable**, **could well occur**).

45. **Possible:** a scenario that has a realistic chance of occurring or being currently accurate, but which does not outweigh all other alternative possibilities (*alt.* **realistic possibility**).

46. **Unlikely:** a scenario that is plausible, but which has only a small chance of occurring or being currently accurate (*alt.* **improbable**).

47. **Highly unlikely:** A scenario that is plausible, but has only a remote chance of occurring or being currently accurate. In such cases, alternative scenarios heavily outweigh the highly unlikely scenario (*alt.* **remote**).

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

Threat Level Definitions

48. **Extreme:** terrorist attack/violent protest/violent crime is expected.

49. **High:** terrorist attack/violent protest/violent crime is assessed as highly likely.

50. **Medium:** terrorist attack/violent protest/violent crime is assessed as feasible and could well occur.

51. **Low:** terrorist attack/violent protest/violent crime is assessed as a realistic possibility.

52. **Very Low:** terrorist attack/violent protest/violent crime is assessed as unlikely.

Likelihood Assessment	Threat Level
Terrorist attack, or violent protest, or violent crime is expected	EXTREME
Terrorist attack, or violent protest, or violent crime is assessed as highly likely	HIGH
Terrorist attack, or violent protest, or violent crime is assessed as feasible and could well occur	MEDIUM
Terrorist attack, or violent protest, or violent crime is assessed as a realistic possibility	LOW
Terrorist attack, or violent protest, or violent crime is assessed as unlikely	VERY LOW

Other Terms

53. **Online environment:** includes websites, internet-based news media, video games, social media platforms, online forums, encrypted messaging applications, the "Dark Web", etc.

54. **Intelligence gap:** information an analyst requires to make an assessment, or to increase confidence in an assessment, but does not currently possess. (*alt.* **information gap**)

55. **Misinformation:** false information disseminated by an individual or organisation believing it to be true.

56. **Disinformation:** false information disseminated by an individual or organisation knowing it to be untrue.

57. **Permissive environment:** an environment in which a threat actor can function – establish a base or safe haven, develop capability, plan and conduct operations – without significant risk of disruption or interdiction.

58. **Non-permissive environment:** an environment in which a threat actor cannot function or faces significant risk of disruption or interdiction.

Handling Instructions

This information is the property of the Combined Threat Assessment Group and is provided to your agency for intelligence purposes only. It may be read by any person in your agency cleared to the classification level of the document with a need to know the information contained in the document, but must not be disseminated outside your agency without the prior written consent of the CTAG Manager. It must not be used or disclosed in any legal, administrative, or review proceedings, nor reclassified, declassified or disclosed under any freedom of information law, without the prior written consent of the CTAG Manager. Electronic systems used to store this material must be accredited at the appropriate level and protected against unauthorised access.

Any CTAG assessment material extracted or copied MUST be accorded the same protection in all respects as the original material, including all caveats and handling instructions.

Queries or feedback can be provided to the following:

s6(a) [redacted]

CTAG Threat Definitions

Likelihood Assessment	Threat Level
Terrorist attack, or violent protest, or violent crime is expected	EXTREME
Terrorist attack, or violent protest, or violent crime is assessed as highly likely	HIGH
Terrorist attack, or violent protest, or violent crime is assessed as feasible and could well occur	MEDIUM
Terrorist attack, or violent protest, or violent crime is assessed as a realistic possibility	LOW
Terrorist attack, or violent protest, or violent crime is assessed as unlikely	VERY LOW

Probabilistic language

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