Long road ahead on defeating hate speech and preventing extremist violence in Australia

Greg Austin[1]

30 April 2026

Australia's counter-terrorism policy is out of balance. The Bondi attack, the rise of online hate, the spread of disinformation, and the resurgence of extremist movements all point to a policy system that is still too heavily shaped by the early post-9/11 paradigm.

The Social Cyber Institute's February 2026 workshop summary, *Workshop on Terrorism, Hate Speech and Disinformation*, captured the problem directly. One of the leading participants, Dr Levi West from the Australian National University, observed that "Australia's counter-terrorism (CT) apparatus, heavily shaped by the early-2000s counter-jihadist paradigm, may require realignment in response to the current fragmented landscape of mixed ideologies, online-Nihilistic ecosystems and state-linked actors." The same report noted the view that governments "cannot meet today's complex threat environments for hate speech, disinformation and terrorism by assigning leadership of this effort only to security agencies or by over-reliance on legislation." That is the starting point for any serious post-Bondi policy reset.

A public-facing campaign, not a politics of panic

Ministers do need a stronger public-facing campaign. But the aim should not be simply to look tougher, announce new offences, or expand symbolic bans. The aim should be to explain clearly what government is trying to prevent, what evidence supports the proposed measures, and how democratic freedoms will be protected while mobilisation to violence is disrupted.

A sure sign that all is not right came on 19 December when the Prime Minister announced five new approaches to holding a gun licence, one of which would be Australian citizenship. This measure was supported by Australians in at least one major poll, with 72 per cent in favour in a poll conducted by Resolve Strategic and Nine Entertainment immediately after the attack. The

---

[1] Greg Austin is a co-founder of the Social Cyber Institute. Beginning in January 2000, Austin has led research or Track 1.5 consultations on counter-terrorism and violent extremism for the International Crisis Group, the Foreign Policy Centre (London), the former EastWest Institute (Brussels). In this field, he has consulted for the UK Ministry of Defence, the US National Security Council, the European Commission and the German Institute for International Affairs.

logic of this citizenship requirement escapes me. It seems to assume that Australian citizenship status might somehow shape a person to oppose illegal gun violence.

That assumption is not sound. One of the two Bondi terrorists was not a citizen but the other was Australian-born and a citizen. Nor is Australian citizenship any protection against extremist violence. The person responsible for one of the most lethal lone-actor terrorist attacks anywhere in the world since 2001 was an Australian citizen who relocated to New Zealand before murdering 51 Muslims in two mosques in 2019. His citizenship was irrelevant. His extreme white supremacist ideology, socialisation, preparation, grievance and pathway to violence mattered far more.

The February workshop report helps sharpen this point. It suggested that "the core policy objective of government should not be the eradication of extremist belief systems per se but rather the prevention of mass casualty events". That is a crucial distinction. Counter-terrorism policy must not confuse the policing of bad ideas with the prevention of violent behaviour. A person may hold hateful or extremist beliefs and never mobilise to violence. The report notes that Australian evidence shows "most of the individuals holding extremist beliefs actually never mobilise to violence" and that factors such as grievance and social isolation are more predictive of violent mobilisation than ideological label alone.

This does not mean ideology is unimportant. It means that the state needs better tools for identifying behavioural risk, network exposure, escalation, access to weapons, online mobilisation, travel triggers, and grievance pathways. A citizenship test for firearms is a blunt proxy for none of these.

Neo-Nazism, selective policing and the credibility problem

A second element of Australian counter-terrorism policy that seems out of balance is the lack of swift and sustained action against neo-Nazi and "white Australia" groups since the Cronulla riots in 2005. There have been some recent official actions, including the cancellation of the visa of a South African in early December 2025 and the near-simultaneous arrest of a UK national on hate-crime charges, likely to lead to his deportation. But by any standard, these actions were late in coming.

The weakness in policing of hate crimes was highlighted in a statement on 2 September 2025 by the Human Rights Law Centre, one day after a neo-Nazi attack on First Nations people at Camp Sovereignty in Melbourne. The Centre called on political leaders to investigate and condemn the attacks, and pointedly asked why Victoria Police were unable to prevent or stop the attack.

Australian counter-terrorism policy faces a credibility problem if marginalised communities believe that hate directed at them is treated less seriously than hate directed at others. This is not only a moral failure; it is an operational weakness. It erodes trust, reduces reporting, weakens intelligence flow, and makes communities less likely to cooperate with police and prevention programs.

The February workshop report therefore rightly insists that women, LGBTI people, disabled people and First Nations communities must be "co-producers of policy, not merely consultees or

data points." It also calls for a permanent, funded "communities collaborative" that would work against hate within communities and ease tensions where communities target each other, including in digital spaces. This is the sort of institutional innovation Australia needs. It moves beyond a model in which government speaks about communities only after violence has occurred.

Hate speech law needs precision, not theatre

Australia does need effective laws against incitement, serious vilification and advocacy of force or violence. But rushed and over-broad criminalisation can do harm. The February workshop report supports "targeted and well-defined criminal and civil law punishments for incitement and serious vilification," but says this must be accompanied by better guidance and training for frontline police and regulators. It warns that overly broad offences and criminalised symbol bans risk diverting scarce operational capacity toward people who are hateful but non-violent, while chilling artistic, critical and community expression.

That judgement matters for the current hate speech debate. The government's hate speech legislation is likely to have limited effect on hate crimes unless it is part of a larger prevention system. Laws passed in haste may satisfy a political need to appear responsive, but they will not by themselves reduce the social, online and organisational conditions in which violence becomes thinkable.

There is also a strategic danger. Terrorism aims not only to kill but to polarise. Policies that deepen polarisation, erode civil liberties and weaken trust can hand extremists part of the victory they seek. This is why the workshop report points toward embedding civil liberties and social cohesion into counter-terrorism decision-making, rather than treating them as secondary concerns.

Data, prediction and the limits of intelligence

A third element of Australian policy that seems out of balance is the way available data relevant to potential terrorist attack is handled. It is too early to tell whether this was a decisive factor in the failure to prevent the Bondi attack, but it deserves close scrutiny.

According to the Prime Minister on 15 December, the Australian-born terrorist involved in the Bondi attack had been investigated in October 2019 and "there was no indication of any ongoing threat or threat of him engaging in violence." When asked whether this was a failing, he said he had reported factually on what ASIO had found. Home Affairs Minister Tony Burke later said that in 2019 the conclusion was that Akram did not have a violent ideology matching those with whom he associated, and that agencies could never be "all seeing and all-knowing" (Home Affairs transcript).

That is true as far as it goes. But the policy question is whether Australia is doing enough to distinguish actual threat at a single point in time from probable risk over time. The workshop report is careful here. It notes that researchers still "can't predict" individual behaviour with accuracy, and that risk factors interact in complex, adaptive ways. Existing CVE frameworks and risk-assessment tools were not designed for the current hybrid threat environment.

This means two things at once. First, intelligence agencies should not be expected to predict every individual act of violence. Second, government should still invest in better system-level analysis, better data integration, and stronger review of known associations, travel, firearms access, online activity and triggering geopolitical events. The goal is not omniscience. It is to reduce avoidable blindness.

In the Bondi case, several triggers deserve close review: the 2019 investigation in one of the Bondi terrorists and his continuing associations; the Hamas attack of 7 October 2023 and its aftermath; alarming sermons by Wissam Haddad in November 2023; firearms training and licence activity; and travel by Akram and his father to Davao City in the Philippines in November 2025. There can be no guilt by association, but in counter-terrorism, continuing close association with extremists is a legitimate basis for renewed assessment, especially after major international triggers. I warned in March 2024 that the aftermath of 7 October was likely to be a major trigger for renewed political violence in Australia.

Online environments and platform responsibility

The February workshop report is especially strong on online harms. It concludes that "cultures of violence are increasingly shaped in online environments" and that online hate creates "sticky spots" and permissive environments in which violence becomes thinkable. It also notes that Australia's dependence on foreign-owned platforms and the flood of disinformation by great power actors and extremists have reduced the room for effective monitoring and response by governments and communities.

This is a major gap in Australian policy. The problem is not simply that harmful content exists online. It is that platform design, recommendation systems, encrypted channels, gaming spaces, influencer ecosystems and grievance networks can accelerate social permission for hate and violence. The report's stark observation that "allowing more hate is more profitable" should be central to any policy conversation about platform governance.

But the answer cannot be takedowns alone. The report calls for robust platform governance to tackle explicit incitement and harassment without suppressing legitimate debate. It also calls for digital literacy and civic education from an early age so citizens can assess online content critically. That is the right balance: more responsibility for platforms, better capability for citizens, and transparency in state action so that anti-government conspiracy narratives are not fuelled by opaque censorship.

From social cohesion to peaceful pluralism

The government will need to do more than repair counter-terrorism machinery. It must also decide what kind of social order it is trying to protect. The phrase "social cohesion" is useful but insufficient. The workshop report records criticism that social cohesion can become an inadequate organising principle if it implies conformity or suppresses legitimate conflict. It points instead to "peaceful pluralism," "social solidarity" and inclusive democracy as better goals.

That is a useful reframing. Australia is not going to eliminate ideological difference, religious tension, anger about the Middle East, resentment about immigration, misogyny, racism, or anti-

government grievance. The realistic democratic objective is to prevent those conflicts from becoming organised hate, intimidation, violent mobilisation or social abandonment. That requires more than police and intelligence. It requires schools, universities, local councils, religious institutions, platforms, employers, media organisations and community leaders to be part of the prevention architecture.

The long road ahead is therefore not simply about defeating hate speech. It is about building a national system that can prevent hate, grievance and disinformation from escalating into violence while preserving democratic freedoms. That system must be evidence-based, multi-disciplinary and co-produced with affected communities. It must rebalance counter-terrorism and countering violent extremism, invest in civil society, build better hate-incident data, improve platform governance, and resist the temptation to mistake symbolic toughness for strategic effectiveness.