Australian Government
Department of Home Affairs

# Joint submission to the Inquiry into extremist movements and radicalism in Australia

## Department of Home Affairs, Department of Foreign Affairs and Trade, Attorney-General's Department

Parliamentary Joint Committee on Intelligence and Security

17 February 2021

# Table of Contents

## Introduction

The Department of Home Affairs, the Attorney-General's Department and the Department of Foreign Affairs and Trade, welcome the opportunity to provide a joint submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into *extremist movements and radicalism in Australia*. This submission provides the PJCIS with information on existing laws and policy frameworks in relation to terrorism and violent extremism, and other matters outlined in the Inquiry's Terms of Reference.

The threat from terrorism and violent extremism continues to evolve. Terrorists and violent extremists continue to use the internet to sow division, spread propaganda, recruit, and radicalise individuals to violence. The COVID-19 pandemic and the resulting economic and social impacts have intensified the spread of extremist ideologies online, while the increasing use by extremists of secure communications poses a growing challenge to law enforcement.

Australia's counter-terrorism laws and arrangements and countering violent extremism (CVE) architecture are ideology agnostic, focusing on prevention, threat and criminality regardless of ideology and motivation. Since 2001, 88 people have been convicted of terrorism related offences.

- 52 of these people are currently serving custodial sentences.
- 25 people are currently before the courts for terrorism offences.

Since 12 September 2014, when Australia's National Terrorism Threat Level was raised, the Australian Government has invested an additional $2.3 billion, and passed 22 tranches of legislation, to strengthen our nation's defences against terrorism.

Around 70 Australian (and former Australian) men and women are currently in Syria or Iraq and have fought with, or were otherwise associated with Islamist extremist groups which remain in the region.

The growth in the threat from extreme right-wing groups and individuals has seen a commensurate growth in the efforts of intelligence and law enforcement agencies to counter it. In 2020, there were a number of instances of enforcement action in relation to individuals with extreme right-wing ideologies.

- In early 2020, a right-wing extremist had their passport cancelled, and was prevented from leaving the country to fight with an extreme right-wing group on a foreign battlefield.
- In March 2020, the NSW Joint Counter Terrorism Team (JCTT) charged two men, who it is alleged were attempting and planning to purchase or acquire military equipment, including firearms and items capable of making improvised explosive devices (IEDs). They have both been charged for other acts in preparation for, or planning, terrorist act (section 101.6 of the *Criminal Code*). The matter remains before court.
- In November 2020, Melbourne-based individual, Phillip Galea, who had been in custody since August 2016, was sentenced to 12 years imprisonment in relation to acts in preparation for, or planning, a terrorist act (section 101.6 of the *Criminal Code*); and attempting to make a document likely to facilitate a terrorist act (section 101.5 of the *Criminal Code*). These offences related to a plot to attack various sites linked to left-wing causes in Melbourne.
- In December 2020, the NSW JCTT arrested and charged an 18 year-old man in regional NSW following an identified escalation in his extremist rhetoric online. It will be alleged in court that the man has regularly used social media forums and communications applications during 2020 to encourage other people to commit violent acts in furtherance of an extreme right-wing ideology. This included allegedly expressing support for a mass casualty event and potentially his involvement in that event. The man was charged with one count of urging violence against members or groups contrary to section 80.2A(1) of the *Criminal Code* and advocating terrorism contrary to section 80.2C(1) of the *Criminal Code*.

The threat of terrorism and violent extremism to Australia's national interests, domestically and abroad, is and will continue to be a priority for Australia's National Intelligence Community (NIC). The NIC plays an important role in supporting Australia's terrorism framework, including through the provision of priority strategic and operational intelligence. The NIC works through a range of domestic and international partnerships to understand current and emerging terrorism threats.

The Department of Home Affairs' Counter-Terrorism Coordination Centre (CTCC), and Countering Violent Extremism Centre (CVEC), coordinate counter-terrorism and CVE efforts across Commonwealth and state and territory governments, including in relation to:

- Developing and implementing policy;
- Coordinating national capabilities to prevent and respond to terrorism and violent extremism; and
- Working collaboratively with intelligence, law enforcement, security and policy agencies to manage counter-terrorism risks.

## The Australia-New Zealand Counter-Terrorism Committee (ANZCTC)

Close partnerships between the Commonwealth, state and territory governments is critical to Australia's ability to counter-terrorism. The 2017 Intergovernmental Agreement on Australia's National Counter-Terrorism Arrangements sets out how governments work together and establishes the ANZCTC. The ANZCTC is the primary forum for developing and coordinating nationally consistent approaches to countering terrorism across the prevent, prepare, respond and recover spectrum with an emphasis on interoperability, and the provision of timely expert strategic and policy advice to Prime Ministers, Premiers, Chief Ministers and other relevant ministers.

The ANZCTC is also responsible for developing and managing national counter-terrorism coordination strategies, plans and other documentation. The ANZCTC has established capabilities in such areas as crisis management and coordination, command and control, intelligence and investigation and media cooperation. The ANZCTC is co-chaired by a state or territory representative and the Commonwealth Counter-Terrorism Coordinator, and comprises senior representatives from the Commonwealth, states and territories and New Zealand. Secretariat support is provided by the CTCC.

The ANZCTC is committed to coordinating an effective framework for countering terrorism and violent extremism. The ANZCTC creates strong, cooperative and consultative relationships that recognise constitutional responsibilities and maximise the respective abilities of Australian governments to prevent, prepare for, respond to and recover from terrorism and its consequences.

## High Risk Terrorist Offenders

The growing cohort of released terrorist offenders poses a potential threat to the Australian community. There are currently 51 incarcerated offenders eligible for consideration under the High Risk Terrorist Offenders (HRTO) regime in Part 5.3 of the *Criminal Code*, 13 of whom are due for release over the next five years.

The Department of Home Affairs (Home Affairs) leads the implementation of the HRTO regime[1], which provides for the Minister for Home Affairs to apply to a Supreme Court of a State or Territory to seek an order for a convicted terrorist to continue to be detained beyond their head sentence. Continuing Detention Orders are intended to apply to the highest-risk category of convicted terrorist offenders.

The Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Bill 2020, which remains before the Parliament at the time of this submission, seeks to extend the HRTO regime to include Extended Supervision Orders (ESOs). If passed, ESOs will enable the court to impose conditions on offenders whom the court does not consider should be detained beyond their sentence, but who still pose a risk to community safety.

[1] The operation of the scheme is governed by Division 105A of the *Criminal Code*.

Home Affairs assesses eligible offenders on a case-by-case basis. Since the scheme came into effect in 2017, only one application for a Continuing Detention Order has been made.

Home Affairs has considered other offenders who were eligible for continuing detention, but the evidence was not available to support the making of applications in those cases. Control orders applied for by the Australian Federal Police (AFP) in the Federal Court have been used to manage the risk posed by these offenders.

Home Affairs is focussed on ensuring effective long-term management of the growing HRTO caseload. This will be complex, time intensive, and require effective coordination and engagement across the Commonwealth and state and territory jurisdictions. Administration of the scheme has shown it to be a tool reserved for the highest-risk offenders.

Management of the ongoing risk posed by each terrorist offender at the end of their sentence requires a broader suite of measures which can be tailored to the risk posed by each individual. Home Affairs considers the proposed ESO scheme will extend the risk management options available to the Commonwealth.

Home Affairs notes that there is an intersection between the HRTO regime and the provisions in the *Australian Citizenship Act 2007* (Cth) that enable the Minister for Home Affairs to cease an eligible individual's Australian citizenship if they have repudiated their allegiance to Australia. See Box 1 for further information.

*Box 1 - Section 36D of the Australian Citizenship Act 2007*

Home Affairs administers the *Australian Citizenship Act 2007*, which includes provisions enabling the Minister for Home Affairs to cease an eligible individual's citizenship if they have repudiated their allegiance to Australia.[2] In particular, section 36D of the Act enables the Minister to cease a person's Australian citizenship if they have been convicted of a particular offence (including a specified terrorism offence), sentenced to at least 3 years' imprisonment due to that conviction, and the Minister is satisfied the person has repudiated their allegiance to Australia and it would be contrary to the public interest for the person to remain an Australian citizen.

The provisions were enacted to ensure the safety and security of Australia and its people, and to ensure the community of Australian citizens is limited to those persons who continue to retain an allegiance to Australia. The purpose clause of the provisions is explicit:

*…the Parliament recognises that Australian citizenship is a common bond, involving reciprocal rights and obligations, and that citizens may, through certain conduct incompatible with the shared values of the Australian community, demonstrate that they have severed that bond and repudiated their allegiance to Australia.* [3]

To date, the Minister has made one determination under section 36D – the case of Mr Abdul Nacer Benbrika. The Minister's determination was referred to during proceedings relating to a Continuing Detention Order application.[4] The Minister also made a public statement in relation to this case.[5]

[2] Subdivision C *Australian Citizenship Act 2007* (Citizenship cessation determinations: 'Purpose of this Subdivision').
[3] Section 36A *Australian Citizenship Act 2007*
[4] The court judgment is Minister for Home Affairs v Benbrika, [2020] VSC 888. Available online at http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VSC/2020/888.html
[5] The Minister's statement is available online at: https://minister.homeaffairs.gov.au/peterdutton/Pages/joint-press-conference-with-us-ambassador-culvahouse.aspx.

# Listing of Terrorist Organisations

## Criminal Code

Under Division 102 of the *Criminal Code*, an organisation may be found to be a terrorist organisation:

- by a court, as part of the prosecution of a terrorist organisation offence; or
- by being 'listed' under *Criminal Code Regulations*.

A court can only consider whether an organisation is a terrorist organisation during a prosecution for a Division 102 offence, and cannot consider this as a standalone matter. The listing process enables terrorist organisations to be identified outside of judicial proceedings.

Section 102.1 provides that before an organisation is listed by the Governor-General, the Minister for Home Affairs must be satisfied on reasonable grounds that the organisation:

- is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act; or
- advocates the doing of a terrorist act.

There are a large number of organisations that meet the legislative criteria and could be considered for possible listing. To guide and prioritise the identification of organisations for consideration by the Minister, security and law enforcement agencies may also give regard to a range of non-legislative factors. The key non-legislative factors include:

- the organisation's engagement in terrorism;
- the organisation's ideology;
- links to other terrorist groups;
- links to Australia;
- threats to Australian interests;
- listing by the United Nations or like-minded countries; and
- engagement in peace or mediation processes.

Depending on available information, some factors may carry more weight than others in identifying organisations for consideration may. A lack of information with respect to one or more factors will not preclude an organisation from being considered for listing.

Division 102 sets out offences in relation to terrorist organisations:

- Section 102.2 – directing the activities of a terrorist organisation.
- Section 102.3 – membership of a terrorist organisation.
- Section 102.4 – recruiting for a terrorist organisation.
- Section 102.5 – training involving a terrorist organisation.
- Section 102.6 – getting funds to, from or for a terrorist organisation.
- Section 102.7 – providing support to a terrorist organisation.

It is also an offence to associate with a member of a listed terrorist organisation in certain circumstances where, amongst other things, such association intentionally provides support to that organisation (section 102.8).

**Purpose of listing under the Criminal Code**

The listing of an organisation as a terrorist organisation serves a number of purposes.

A listing can provide the basis for establishing the fact that an organisation is a terrorist organisation in a criminal proceeding. In providing that an organisation may be listed where the Minister is satisfied that it advocates the doing of a terrorist act, the legislation provides the Executive with broader criteria for finding that an organisation is a terrorist organisation than that available to the courts. The association offence in section 102.8 also only applies to listed organisations.[6]

Listing an organisation has the potential to disrupt terrorism-related activities and serve as a deterrent, allowing the Australian Government to put an organisation and members of the public on notice that the organisation is a terrorist organisation under Australian law, and that certain dealings with the organisation – such as membership, funding or providing resources – are criminal offences.

The listing of an organisation also has symbolic value: it sends a clear public message that the Australian Government does not condone the actions of groups that use terrorism to achieve their political, religious or ideological objectives.

**Reliance on listing regulations in prosecutions for terrorism offences**

Since the provisions were introduced in 2002, 16 people have been convicted and sentenced for offences under Division 102 of the *Criminal Code*. Of these, eight were members of the Benbrika organisation sentenced between 2007 and 2009. The Benbrika organisation was found to be a terrorist organisation by the court during the prosecution of these individuals.

The remaining eight offenders were convicted of offences in relation to organisations listed in *Criminal Code Regulations*, between 2017 and 2020. Of these eight, one offender was convicted of offences in relation to the Kurdistan Worker's Party, and the other seven were convicted of offences in relation to Islamic State.

**Limitations of listing in the current threat environment**

Listing a terrorist organisation under the existing legislation is effective where terrorism is carried out or advocated through identifiable organisational structures.

However, the existing provisions do not address the threat posed by lone actors who are not members of a terrorist organisation, or of extremist groups who are ideologically supportive of political violence but whose conduct falls short of engaging in or advocating terrorism.

The radicalisation of lone actors, including both online and by extremist groups whose conduct is below the threshold for listing, diminishes the effectiveness of the existing listing provisions to prevent and prosecute terrorism. The listing regime will also not effectively address the threat posed by politically, ideologically or religiously-motivated ad hoc violence, potentially fuelled by online activities.

**Review and oversight of terrorist organisation listings**

Provisions for listing terrorist organisations were first inserted into the *Criminal Code* by the *Security Legislation Amendment (Terrorism) Act 2002* (Cth), which specified that listings would sunset after two years. The sunsetting requirement was extended to three years by the *National Security Legislation Amendment Act 2010* (Cth) in accordance with the recommendations made by the PJCIS in its 2007 Inquiry.

The ongoing review of organisations for re-listing in line with the three-year sunsetting requirement is a complex and administratively burdensome process. There may be opportunities to either extend or remove the three-year sunsetting requirement, if coupled with alternative safeguards to enable Ministerial and Parliamentary review.

[6] For a court to find that an organisation is a terrorist organisation, it must find that the organisation is directly or indirectly engaged in preparing, planning, assisting or fostering the doing of a terrorist act.

### Charter of the United Nations Act 1945 (Cth)

Listings under the *Criminal Code* have a distinct operational and policy intent compared to listings made under Part 4 of the *Charter of the United Nations Act 1945* (Cth) (COTUNA) and *Charter of the United Nations (Dealing with Assets Regulations 2008* (Cth).

Part 4 of COTUNA gives effect to Australia's international obligations under paragraphs 1 (c) and (d) of United Nations Security Council (UNSC) Resolution 1373 (2001) to impose targeted financial sanctions against persons associated with terrorism.

UNSC Resolution 1373 is one of two UNSC frameworks imposing obligations on United Nations (UN) Member States to apply sanctions to terrorists: the other is the Islamic State of Iraq and the Levant (ISIL)/Al Qaida Sanctions Regime, currently mandated under UNSC Resolution 2253 (2015). Under the ISIL/Al Qaida Sanctions Regime, a Committee established by the UNSC determines to which individuals and entities the sanctions must apply. Under UNSC Resolution 1373, each individual UN Member State must determine which individuals and entities to target.

Under Part 4 of COTUNA, the Minister for Foreign Affairs must list a person or entity if satisfied on reasonable grounds that they are:

- a person who commits, attempts to commit, participates in or facilitates the commission of terrorist acts;
- an entity owned controlled by such a person; or
- or a person or entity acting on behalf of, or at the direction of, such a person or entity.

It is then an offence under COTUNA, punishable by up to 10 years imprisonment and/or significant financial penalties, to use or deal with the assets of a listed person or entity (this has the effect of freezing such assets); or to make any asset available to a listed person or entity.

The listing criteria under Part 4 of COTUNA differ to the criteria under section 102 of the *Criminal Code* in key respects. Most obviously, Part 4 COTUNA criteria apply to individuals and "entities" and are thus not limited to "organisations". In addition, the listing criteria for entities under COTUNA focus on the conduct of the individuals who own or control the entity, and not on the conduct of the entity itself, as is the case for listing an organisation under the *Criminal Code*. This means that the type of entity captured under COTUNA listings are necessarily broader than the organisations listed under the *Criminal Code*, including, for example, an entity that is owned or controlled by a terrorist, even if that entity itself is not known to have engaged in terrorist acts.

Finally, the Minister for Foreign Affairs does not need to list under Part 4 of COTUNA any individual or entity already listed by the UNSC's ISIL/Al Qaida Sanctions Committee, as a different Australian sanctions measure (the Charter of the United Nations (Sanctions – Al Qaida) Regulations 2008) separately applies identical targeted financial sanctions to them.

A detailed comparison of current listings under Part 4 of COTUNA and Part 5.3 of the *Criminal Code* is at Attachment A.

## Counter-Terrorism Strategy

On 9 August 2019, the Council of Australian Governments (COAG) agreed to task the ANZCTC to update Australia's Counter-Terrorism Strategy (CT Strategy), which was released in 2015. Development of the CT Strategy is currently underway and is being led by the CTCC on behalf of the ANZCTC.

The CT Strategy is structured around: (a) the terrorism threat environment; (b) the principles and core elements underpinning Australia's response to the threat; and (c) counter-terrorism governance and accountability arrangements. The CT Strategy will include updates and additions relating to emergent technologies and forms of extremism, such as the threat from right-wing extremists, the ongoing need for partnerships to counter the threat of terrorism and build community resilience, and the importance of prevention through CVE and social cohesion.

# Hate speech and symbols and insignia associated with terrorism and extremism

## Hate speech

Whilst a commonly used and accepted term more broadly, Australian law does not define 'hate speech' itself. The same appears to be true internationally. A UN document on hate speech from May 2019 states the following:

> *There is no international legal definition of hate speech, and the characterization of what is 'hateful' is controversial and disputed. In the context of this document, the term hate speech is understood as any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. This is often rooted in, and generates intolerance and hatred and, in certain contexts, can be demeaning and divisive.*[7]

Hate speech includes speech that is hateful in itself (i.e. directed at a target person or group), and speech that incites hatred against a person or group by other persons. The latter is vilifying speech, which applies to a narrower range of conduct designed to incite hatred, contempt or ridicule of the target group by other (third party) persons.

## Prohibitions on racial discrimination, vilification and hate speech in Commonwealth, state and territory laws

There are a range of civil and criminal provisions in state, territory and Commonwealth law that seek to prevent and address violence, abuse and discrimination based on race.

Commonwealth offences: Division 80 of the *Criminal Code* contains a range of offences directed at the security of the Commonwealth which were drawn from the previous sedition offences in the *Crimes Act*. Section 80.2A(2) of the *Criminal Code* currently creates an offence for a person who intentionally urges another person or group to use force or violence against another group distinguished by race, religion, nationality, national or ethnic origin, or political opinion. The offence requires the first person to intend that force or violence occur. The offence carries a maximum penalty of 5 years' imprisonment. Section 80.2A(1) creates an aggravated offence where the force or violence would threaten the peace, order and good government of the Commonwealth. The aggravated offence carries a maximum penalty of 7 years. Section 80.2B creates similar offences with the same penalties for a person who urges force or violence against a member of a group distinguished on the same criteria as in section 80.2A.

State offences: All states except South Australia, Tasmania, and the Northern Territory include race based violence/vilification offences in their Criminal Code/Crimes Act. Offences carry penalties of a fine, or between 6 months to 5 years imprisonment.

[7] United Nations Strategy and Plan of Action on Hate Speech, May 2019, available at https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf (accessed 14 January 2021).

Commonwealth anti-discrimination legislation: The *Racial Discrimination Act 1975* (Cth) (RDA) protects an individual's right from discrimination on the grounds of race, colour, descent or national or ethnic origin in any field of public life and prohibits unlawful discrimination or vilification on these grounds. Section 18C of the RDA makes it unlawful to do an act, otherwise than in private, that is reasonably likely to 'offend, insult, humiliate or intimidate another person because of their race, colour or national or ethnic origin. If a person believes they have been unlawfully discriminated against, they may make a complaint to the Australian Human Rights Commission (AHRC). The AHRC will attempt to settle the complaint through conciliation. Outcomes will vary depending on the nature of the complaint. However, agreements can include an apology, reinstatement to a job, compensation for lost wages, changes to a policy or putting in place anti-discrimination policies. If the complaint can't be resolved through conciliation, a person can apply to have the matter heard in the Federal Court of Australia or the Federal Circuit Court of Australia.

State and territory anti-discrimination legislation: All jurisdictions have anti-discrimination legislation which protects people from racial vilification and unfair treatment on the basis of their race, colour, descent or national or ethnic origin in certain fields of public life. If a person believes they have been unlawfully discriminated against, the appropriate avenue for complaint is through the relevant Anti-Discrimination Commission in their jurisdiction. Complaints are generally settled through conciliation, similar to the process for the AHRC.

General offences such as harassment, the threat of bodily harm, assault, grievous bodily harm, murder and other crimes against the person are criminalised in Australia, primarily within state and territory legislation. These offences apply regardless of the victim's race, ethnicity or any other attribute.

Details of specific provisions on racial discrimination, vilification and hate speech are in the table at Attachment B.

### Carriage Service Offences

A carriage service is defined in the *Telecommunications Act 1997* (Cth) as a service for carrying communications by means of guided and/or unguided electromagnetic energy. This includes, for example, voice calls, text messages and online communications. Section 474.15 of the *Criminal Code* makes it an offence to use a carriage service to make a threat to kill, or seriously harm. This offence carries penalties of 10 years and 7 years imprisonment respectively.

Section 474.17 of the *Criminal Code* makes it an offence to use a carriage service in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive. This offence carries a penalty of three years and applies to an Australian citizen, even if the conduct occurred wholly outside of Australia.

Following the 2019 Christchurch terrorist attacks, Subdivision H was introduced to Part 10.6 of the Criminal Code through the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (the AVM Act). Subdivision H includes new offence provisions relating to the use of a carriage service for sharing of abhorrent violent material. Section 474.34 creates a new offence for content and hosting service providers who fail to expeditiously remove abhorrent violent material (AVM). This offence attracts a penalty for individuals of imprisonment for up to three years or a fine of up to 10,000 penalty units, or both. For bodies corporate, it attracts a pecuniary penalty of up to 50,000 penalty units or 10% of the annual turnover of the period when the offence occurred. Content, internet and hosting providers are also required to, within a reasonable time, report to the Australian Federal Police (AFP) abhorrent violent conduct that is happening in Australia and accessible through, or hosted on, their services. The AVM Act also provides the eSafety Commissioner the power to notify service providers that abhorrent violent material is available on their services. These notices create a presumption that the provider is aware of the material and puts providers on notice that such material should be removed.

## Border control of objectionable goods under existing customs legislation

The customs legislation prohibits the import and export of objectionable goods via regulation 4A of the *Customs (Prohibited Imports) Regulations 1956* and regulation 3 of the *Customs (Prohibited Exports) Regulations 1958*. The customs legislation is limited to tangible objectionable goods, which includes publications such as magazines and books. It does not include online content or electronic goods, unless the objectionable good is contained on a tangible good, such as a hard drive or phone.

The maximum penalty for importing or exporting objectionable material is 1000 penalty units or 5 years imprisonment, if the goods are in a commercial quantity of 25 or over. Where a person imports or exports less than a commercial quantity of objectionable material (without lawful exception), and the material is not for certain public or commercial purposes, the maximum penalty is will be 1000 penalty units.[8]

Determining whether terrorism or extremist material is an 'objectionable good' for the purposes of import or export requires the goods to:

- describe, depict, express or otherwise deal with matters of crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be imported or exported; or
- promote, incite or instruct in matters of crime or violence; or
- advocate the doing of a terrorist act.

## Symbols and insignia

Public display of terrorist symbols or insignia may be used to promote affiliation with a proscribed terrorist organisation and encourage support for such organisations. Flags and other terrorism-related insignia feature extensively on terrorist propaganda websites and may contribute to the online radicalisation trend.

The public display of terrorism-related material, such as flying an ISIL flag, does not of itself constitute a Commonwealth offence but could:

- support the prosecution of a number of terrorist organisation offences, such as being a member of, recruiting for, providing support to, or associating with a terrorist organisation;
- support the prosecution of an offence for advocating terrorism; or
- be subject to civil action under Commonwealth, or state and territory laws.

Customs legislation does not prohibit the import of goods that display terrorism-related symbols or insignia, such as flags or crests, for that reason alone. However, material that does meet the current definition of objectionable goods—for example, publications that advocate the doing of a terrorist act—may contain symbols and insignia.

[8] Regarding the penalty for importing/exporting less than a commercial quantity, which is not for certain public or commercial purposes; if the Court can determine the value of the objectionable goods, the penalty is the greater of either (a) three times the value of that material or (b) 1000 penalty units: s 233AB(2) of the *Customs Act 1901*. Practically speaking, in relation to the type of material relevant here, the higher penalty will likely be 1000 penalty units.

# Social Cohesion and Countering Violent Extremism

Social cohesion and CVE are complementary programs and policies that support a united, secure and prosperous Australia. Prevention initiatives seek to promote social cohesion, stop radicalisation before it starts and include online, digital and media-based initiatives. Intervention initiatives engage with individuals who are vulnerable to extremist ideologies and recruitment or who have become radicalised to violence.

## Social Cohesion

The Scanlon Foundation Research Institute, which has undertaken a series of detailed surveys on social cohesion and population issues in Australia since 2007, has found that we continue to have relatively strong social cohesion. The Scanlon-Monash *Index of Social Cohesion* was 89.6 in 2019, close to the level of six of the last seven years, which averaged 89.2 index points.[9]

Australia's strong social cohesion is built on our inclusive national identity and shared liberal democratic values. This supports and promotes community resilience to a range of threats that seek to divide and weaken us, including violent extremism.

Australia's social cohesion policies and programs foster a cohesive and resilient society so that individuals are less susceptible to social disengagement, marginalisation, radicalisation and terror.

Home Affairs takes a leading role in strengthening Australia's social cohesion.[10] Home Affairs is implementing the Australian Government's $62.8 million package of initiatives announced in the 2020-21 Budget to strengthen Australia's social cohesion and community resilience during the COVID-19 recovery period. Australian Government initiatives to strengthen social cohesion include:

- a revised Australian Values Statement – which commenced on 30 October 2020 – that articulates our core values as a longstanding and successful liberal democracy and is agreed by visa and citizenship applicants;
- promoting the uptake of Australian Citizenship and updating the Australian citizenship test – which commenced on 15 November 2020 – to include questions about the core values that are so important to our success and keep us together;
- opening up the Adult Migrant English Program by lifting the cap on tuition hours available to eligible migrants, expanding it to provide lessons up to vocational English, and removing time limits for commencement and completion of the lessons;
- deepening our engagement with communities by strengthening the Home Affairs' Community Liaison Officer network to include more officers with dual language skills; and
- further investment to understand and track our social cohesion including a focused research program designed to better understand community sentiment towards social cohesion.

This investment builds on the Australian Government's $71 million package of social cohesion initiatives to create a stronger, more cohesive Australia announced in the 2019-20 Budget.

Home Affairs also has a dedicated social media presence, alongside community engagement activities, to undermine violent extremist propaganda by showcasing Australia's inclusive national identity and values and promoting positive messages that build trust within the Australian community. The program also encourages people to engage respectfully online, think critically, and counter hateful and extremist narratives.

[9] Scanlon Foundation Research Institute, *Mapping Social Cohesion* (2019)

[10] See also Department of Home Affairs, *Submission to the inquiry into nationhood, national identity and democracy* and Department of Home Affairs, *Submission to the inquiry into issues facing diaspora communities in Australia*.

## Countering Violent Extremism

CVE is a core element of Australia's approach to preventing terrorist and extremist violence. CVE refers to initiatives that aim to prevent individuals from becoming or remaining violent extremists. CVE initiatives support and are supported by social cohesion and community resilience initiatives and counter-terrorism responses. Australia's CVE efforts aim to do this by:

- building the resilience of communities to help prevent violent extremism;
- supporting the diversion of individuals at risk of radicalizing and becoming violent extremists; and
- rehabilitating and reintegrating violent extremists.

Since 2013-14, the Australian Government has invested over $61 million in CVE programs. Australia's approach to CVE is designed to address all drivers of extremism including political, religious, social, cultural or issue-specific ideology. It involves all levels of government, along with a number of private sector and non-government organisations. While policing and security agencies play a critical role, the preventative focus of CVE means that a range of health, social welfare, educational and cultural government agencies are also involved in coordinating and delivering initiatives.

CVE is a joint responsibility between governments. Efforts are directed through the Countering Violent Extremism Sub-Committee (CVESC) under the ANZCTC. CVE contributes to three pillars of the current CT Strategy: challenging violent extremist ideologies; stopping people from becoming terrorists; and shaping the global environment.

CVESC is responsible for coordinating and providing expert advice on the development and maintenance of a CVE capability to achieve best practice. This includes funding of around $2 million each year for projects to strengthen CVE capabilities and outcomes. In addition to managing CVESC, the Australian Government maintains research partnerships to align CVE policy and programs with the latest evidence; and develops and delivers training to CVE practitioners.

CVE Intervention initiatives focus on:

- Identifying and working with people who are at-risk of radicalisation to violent extremism, or who have started radicalising. People may be displaying signs of radicalisation such as accessing extremist material, expressing their support for an extremist group or ideology, or engaging with other extremist individuals.
- People who are already radicalised and may be engaged in extremist violence and/or groups. They may also be individuals who have been incarcerated for violent extremist offences or radicalised in prison.

### Living Safe Together Intervention Program

In 2015, the Australian Government established the national CVE intervention program, *Living Safe Together*. The program aims to reduce the risk of violent extremist incidents occurring in Australia by identifying at-risk people and referring them to support and disengagement services. The program focusses on reconnecting participants with their families and communities through individualised case management plans designed to address the root causes of their radicalisation. Home Affairs provides $3 million annually for the program to support delivery by state and territory agencies.

*Living Safe Together* is designed to address all forms of violent extremism, including Islamist extremism, left and right-wing extremism and issue based extremism. Participation in the program is voluntary.

Home Affairs is responsible for the program at the national level and provides strategic oversight, funding, governance arrangements, research and capability building. The states and territories are responsible for implementing the program within their jurisdiction. This includes developing internal identification, referral, assessment and case management processes. Each jurisdiction implements the program according to their local conditions and threat environment.

The majority of the support to states and territories is for a CVE Intervention Coordinator in each jurisdiction. The CVE Intervention Coordinators identify, assess and deliver tailored intervention and case management plans that link participants to support from a range of services. This can include mentoring and coaching, counselling, education, religious guidance and employment support to divert individuals from violent pathways.

Program delivery varies based on the relevant risk and participant profile in each jurisdiction. Some jurisdictions take a police-led approach (Tasmania, Victoria, Queensland and Western Australia), while others coordinate program delivery through non-law enforcement departments, working in close cooperation with them (New South Wales, Australian Capital Territory, Northern Territory and South Australia).

### CVE in prisons and community corrections

CVE programs for terrorist and violent extremist offenders seek to rehabilitate and reintegrate offenders in preparation for re-entering the community and to reduce the risk of recidivism or influencing other at-risk people.

Home Affairs' main effort is the Radicalisation and Extremism Awareness Program (REAP). It is a national initiative that aims to improve the capacity of correctional and youth justice staff to recognise and report indicators of risk for violent extremism. It was established in 2014 in custodial settings and updated in 2017 to community corrections and juvenile justice staff. Over 200 trainers and 5,000 front line prison officers have been trained by the REAP.

## Extremist use of social media, encrypted platforms and the dark web

The Australian Government recognises the benefits of social media and supports cyber security tools such as encryption which create and support a well-connected and safe online environment for Australians. However, the malicious use of encryption and the dark web by criminals has significantly degraded the capacity for Australian national security and law enforcement agencies to access communications, conduct investigations and prevent crimes, including combatting the threat posed by extremist movements and radicalism. These technologies provide opportunities for the most serious crimes, including terrorism and other acts stemming from extremism and radicalism, to occur online undetected. Social media is a force multiplier for the spread of abhorrent, hateful or violent material online.

### Social media

Social media enables extremist movements to expand their audience, radicalise and recruit vulnerable individuals, and encourage violent acts. Increasingly, violent extremists from across the ideological spectrum seek to exploit the online environment to spread extreme and harmful propaganda, seed division and draw support for their cause. While Islamist extremist users remain an ongoing feature of the social media landscape, extreme right-wing influencers are also proliferating online.

Despite mainstream social media platforms implementing measures to limit extremists' ability to attract followers and spread abhorrent, hateful or violent material online, it remains readily available in the social media environment.

Extremist users are adapting and modifying their public online behaviours, including via migrations to alternative, non-traditional and unmoderated online platforms where they can espouse their beliefs uncurbed.

During 2020, COVID-19 has been a major topic of discussion within Australian extremist social media pages as they leverage the pandemic to promote their respective causes. The global nature of the pandemic lent itself to increased virtual links and cross-fertilisation of ideas across online extremist communities in Australia and abroad, potentially further radicalising vulnerable individuals and influencing others.

Social media and other online algorithms also create a unique information flow for each user that can be a factor in their radicalisation. This means that the material viewed becomes self-reinforcing of extremist world views, obscuring alternative viewpoints and further perpetuating this problem across social media platforms.

### The dark web, encryption and anonymising technologies

The use of the dark web and anonymising technologies (such as bespoke encrypted devices) has made it easier than ever for extremists to operate and proliferate dangerous propaganda and material at volume and across multiple jurisdictions. This has significantly degraded national security and law enforcement agencies' ability to combat increased radicalisation and extremist movements. Anonymising technologies and criminal methodologies can also be combined for cumulative effect making it technically difficult, as well as time and resource intensive, for law enforcement to effectively respond. Often these technologies are cheap, commercially available and require little technical expertise to use, allowing the scale and sophistication of cyber enabled extremism to grow.

### Challenges to agencies' lawful, essential access to data

The uptake of end-to-end encryption by social media and digital communications companies has made it easier for criminals, including terrorists and violent extremists, to conceal their activities. End-to-end encryption obscures visibility of content hosted on, and facilitated by, communications platforms. End-to-end encryption erodes the ability for communications providers to proactively scan their platforms for harmful content, and to report this content to law enforcement and intelligence agencies for investigation.

The decision by communication platforms to deploy end-to-end encryption by default on messaging services has the potential to significantly deteriorate law enforcement's lawful access and thus visibility of illicit content being shared on its platform, including extremist material. If configured in a detrimental manner, the ability of communications platforms to respond to law enforcement's requests for information – even when law enforcement have a warrant to access the information – will be degraded. Such changes can significantly impede established processes that exist to ensure that law enforcement agencies can protect citizens by investigating insidious crimes and holding criminals to account.

In addition, electronic data is increasingly kept offshore and regularly moves across geographical borders, through servers and other infrastructure located around the globe. Circumstances where foreign communication service providers hold electronic data relevant to offshore criminal matters often involve a complex web of legal compliance and regulation. It also significantly frustrates agencies' access to electronic data to combat crime, putting the Australian community at risk.

International crime cooperation mechanisms (such as mutual legal assistance) remain the principal means to obtain evidence, including electronic data, from foreign jurisdictions for use in criminal investigations and prosecutions. However, these mechanisms have proven to be a slow and cumbersome way of working, not responding sufficiently to this fundamental shift in the offshore storage of Australians' data.

### Response to these challenges

Australia is committed to preventing violent extremism online. We can and should balance personal privacy with public safety in the online context. Australia has, and continues to, take steps to address the role that social media, encrypted communications and the dark web play in allowing online radicalisation and terrorist propaganda to flourish. Australia does this through legislative measures, content referral and working with industry to limit the appeal and access to extremist material online.

Home Affairs plays a key role in coordinating a national approach to combatting online extremism, and in ensuring law enforcement and security agencies have the necessary, proportionate powers they require to protect the Australian community from this threat.

**Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Assistance and Access Act)**

The Assistance and Access Act provides a pathway for national security and law enforcement agencies to seek assistance from industry to overcome technological impediments. The Act also enhances other investigative powers to allow law enforcement to access evidence at a point where it is unencrypted.

Since the Assistance and Access Act came into force on 9 December 2018, agencies have used the industry assistance framework in a targeted and cooperative manner to resolve technical issues impeding the investigation of transnational, serious and organised crime, cybercrime and serious crimes against the person, as well as on national security matters.

The PJCIS is yet to report on its third review of the Assistance and Access Act.

**Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (SLAID Bill)**

The SLAID Bill proposes to strengthen the capacity of Australia's leading federal law enforcement and criminal intelligence agencies—the AFP and the Australian Criminal Intelligence Commission (ACIC)—to identify and disrupt serious criminal activity occurring online, including online extremism. The powers and capabilities of the AFP and ACIC must keep pace with technological trends to ensure that these agencies maintain an edge in tackling serious online crime.

The SLAID Bill introduces three new powers to enhance the ability of the AFP and the ACIC to respond to serious cyber-enabled crime:

- data disruption warrants to enable the AFP and ACIC to access computers and modify data belonging to individuals suspected of criminal activity in order to frustrate the commission of serious offences online;
- network activity warrants to enable the AFP and the ACIC to access computers for the purpose of collecting intelligence on the most harmful criminal networks of individuals suspected of engaging in or facilitating criminal activity, including those on the dark web and using anonymising technologies; and
- account takeover warrants to enable the AFP and the ACIC to take control of a person's online account for the purposes of gathering evidence about criminal activity, to further a criminal investigation.

The SLAID Bill also makes minor amendments to the controlled operations framework in the *Crimes Act* to improve the capacity for agencies to conduct controlled operations online.

The SLAID Bill's disruption, intelligence collection and account takeover warrants will complement the AFP and the ACIC's existing powers by providing new avenues to gather information and respond to serious cyber-enabled crime, including online extremism.

The SLAID Bill is currently being reviewed by the PJCIS. Home Affairs will support the PJCIS review of the SLAID Bill through submissions and appearances at hearings.

**Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (IPO Bill) and US/AUS CLOUD Act Agreement**

The IPO Bill sets out a framework to enable Australia to give effect to bilateral or multilateral cross-border access to data agreements. It stands up a new international production order (IPO) framework that allows Australian law enforcement and national security agencies to, amongst other things, issue extraterritorial orders for electronic data on foreign communications providers where there is an agreement in place. The IPO framework will complement other international crime cooperation mechanisms and is not intended to restrict other means of obtaining electronic data.

The IPO Bill will be a significant step in enhancing the effectiveness of Australian investigations and prosecutions of serious crimes, including terrorism, by providing much faster access to critical electronic data from United States of America (US) communication service providers.

Australia is currently negotiating for a bilateral Clarifying Lawful Overseas Use of Data Act Agreement (CLOUD Act Agreement) with the US. This Agreement would permit Australian agencies to issue orders to US communication service providers, rather than needing to go through the US Government. Noting that the US is the largest data controller in terms of communications technologies, services and platforms, entering such an agreement with the US would have significant benefits to Australian law enforcement and national security efforts.

The PJCIS has reviewed but not yet reported on the IPO Bill.

**Social media content referral measures**

Home Affairs refers content to social media platforms for action against their terms of service policies where that content:

- provides instructions to commit an offence associated with terrorism;
- is extremely graphic in nature; and/or
- expressly promotes or advocates violence against individuals or organisations.

The platforms decide whether to remove content, with reference to their terms of service.

**Working with industry and international partners on detection and removal of content**

Following the 2019 Christchurch terrorist attacks, the Australian Government partnered with digital platforms and internet service providers (ISPs) to form a Taskforce to Combat Terrorist and Extreme Violent Material Online. The Taskforce recommended industry and the Australian Government take 30 actions under five streams of activity: prevention; detection and removal; transparency; deterrence; and capacity building. Digital platforms and ISPs have engaged constructively with Australian Government departments implementing Taskforce recommendations; however, more work is required.

Building on measures already implemented in relation to the recommendations of the Taskforce, Home Affairs is working in close collaboration with partner governments, digital industry and civil society groups to embed consistent and common protocols across platforms to ensure the effective detection and removal of terrorist and violent extremist content online.

In 2020 Home Affairs established an Online Content Incident Arrangement (OCIA) in partnership with industry, eSafety and other responsible government agencies. The OCIA governs arrangements between the Australian Government and industry for removing online content in the scenario of a live-streamed terror attack. On 1 October 2020, Home Affairs successfully conducted an OCIA Testing Event—a tabletop exercise involving senior participants from Microsoft, Google, Facebook, to test responses and interactions in the event of a livestreamed offshore attack going ‘viral’ in Australia.

Home Affairs continues engagement with industry and academia to facilitate information sharing and support research into terrorist and violent extremist material online. As part of this work, Home Affairs facilitated sharing of research and information products between stakeholders across industry, government and academia in order to develop a common understanding of terrorist and violent extremist content online.

Home Affairs is investing in international partnerships that enhance industry efforts to prevent, detect and remove terrorist and violent extremist content online.

- Home Affairs is leading the Australian Government's engagement with industry, governments, academia, and civil society groups, to develop a Voluntary Transparency Reporting Framework for Terrorist and Violent Extremist Content (the Framework), under the auspices of the Organisation for Economic Cooperation and Development. The Framework seeks to establish a common standard for online platforms to implement regular and transparent public reporting on the steps they are taking to prevent, detect and remove terrorist and violent extremist content on their platforms.
- Home Affairs leads the Australian Government's engagement with the Global Internet Forum to Counter Terrorism (GIFCT). The GIFCT was launched in 2020 as an independent, not-for-profit organization, and brings together the technology industry, government, civil society, and academia to foster collaboration and information sharing to counter terrorist and violent extremist activity online.

**Efforts to maintain lawful access to data for law enforcement and security agencies**

Home Affairs has engaged with digital industry to highlight concerns for public safety resulting from the implementation of end-to-end encryption, and governments have collaborated to demonstrate a united approach to this issue:

- In October 2019, Ministerial representatives from Australia, the US and the United Kingdom wrote an open letter to Facebook, asking Facebook to protect user safety by ceasing its plans to move to end-to-end encryption on its messaging platforms. The letter called for responsible encryption, which enhances public safety while protecting privacy and cybersecurity.
- In October 2020, the Australian Government, along with Five Eyes counterparts and the Governments of India and Japan, signed the *International Statement: End-to-End Encryption and Public Safety*. The statement acknowledges the role of encryption in protecting personal privacy, and calls on digital industry to adopt technical solutions that strike a balance with public safety and allow law enforcement agencies to protect citizens and investigate crime.

Despite these efforts, voluntary international reporting mechanisms for digital industry to combat online harms have proven unsuccessful, with minor adherence to the optional "voluntary" measures. We must provide the framework and set expectations for how digital industry is required to operate, in a way which puts community safety at the forefront of technology and design.

## Attachments

Attachment A - Comparison of entities/organisations listed under Part 4 of the Charter of the United Nations Act 1945 and Part 5.3 of the Criminal Code

Attachment B - Comparison of civil and criminal vilification provisions in Australian jurisdictions