

FULL REPORT | MARCH 2023

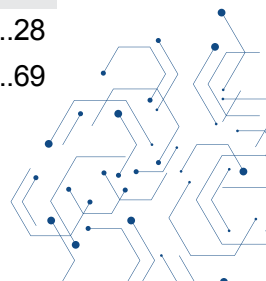
WHO DESIGNATES TERRORISM?

The Need for Legal Clarity to Moderate Terrorist Content Online



TABLE OF CONTENTS

EXECUTIVE SUMMARY	03
GENERAL RECOMMENDATIONS	04
1. INTRODUCTION	06
1.1. Designation.....	06
1.2. Why does designation matter for tech companies?.....	07
2. REVIEW OF DESIGNATION JURISDICTIONS AND PROCESSES	
2.1. Overview Table 1: Overview of designation jurisdictions and processes.....	08
2.2. Challenges with implementing designation to regulate online terrorist content.....	09
The presence of designation systems.....	09
Legality of terrorist content.....	09
Incitement to violence.....	10
Designation of far-right terrorist groups.....	11
Review processes.....	12
Definitions of terrorism and designation systems.....	13
3. UPHOLDING RIGHTS WHILE DESIGNATING TERRORISM	
3.1 Humanitarian.....	14
3.2 Constitutional.....	15
Lack of definitional clarity of terrorism.....	15
Pre-emptive punishment.....	15
Lack of transparency.....	15
Judicial review and the right to remedy.....	16
4. CONCLUSIONS AND RECOMMENDATIONS	
4.1. General recommendations.....	17
4.2. Setting an international framework for terrorist designations.....	19
Outline.....	20
Assessment of our suggested models.....	20
Further Discussion.....	22
4.3. Country-Level Recommendation.....	23
Outline.....	23
Assessment of our suggested models.....	25
5. AREAS FOR FURTHER STUDY	27
6. ANNEX	
6.1. Country-level investigations.....	28
6.2. Methodology.....	69



EXECUTIVE SUMMARY

In this report, Tech Against Terrorism investigates the use of designation: a powerful tool available to governments to facilitate improved action against terrorist use of the internet in a way that upholds the rule of law.

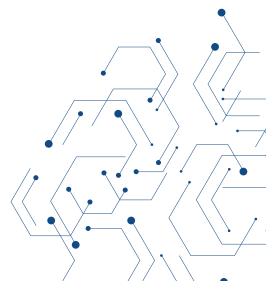
We detail how terrorist designation differs from one jurisdiction to another. We argue that these counterterrorism measures, whether online or offline, must be grounded: judiciary systems must be brought into the 21st century when designating terrorism. In the context of terrorist use of the internet, governments and legislatures must take ownership of the problem, rather than leave the issue to tech companies who must second guess fragmented and incoherent designation processes.

Governments and their legal systems should be responsible for adjudicating on what is illegal terrorist content online, rather than leave the burden to tech companies, as is predominantly the case at the time of writing this report. Global tech companies, whether large or small, are overwhelmingly willing to counter terrorist use of their platforms. In our experience, the likelihood of getting platforms to remove terrorist material increases when terrorist groups are designated, as designation removes a level of uncertainty and provides clear legal basis for removal for tech companies.

While some countries' online legislation, such as the UK draft Online Safety Bill (OSB), references designation, the inconsistency between online regulation and its relationship to designation provides a significant grey area in which tech companies must decide what content should be removed or otherwise restricted. It is highly unlikely that many tech platforms have a significant awareness of the legislative framework, policy apparatus, and general approach to counterterrorism found in any given jurisdiction. By placing the responsibility of determining whether content on tech platforms is terrorist in nature, there is a risk that those who do not meet the definition of terrorism may be subject to unjust curtailment of their right to freedom of expression, while those who are engaged in terrorism may be able to spread their message online without hindrance.

Tech Against Terrorism recognises that reliance on designation is by no means a perfect solution. Aside from the humanitarian and constitutional concerns around designation processes and their offline impact, these legal processes are not currently equipped to respond effectively to the fluidity of the online realm. In particular, designation systems are slow to respond to a rapidly evolving threat picture and are insufficient for tackling the threat of far-right entities as well as lone and non-affiliated terrorist actors. In this report, we suggest means of improving designation so that it is fit to guide the moderation of terrorist content online.

While the main aim of our report is to explore how designation can guide the moderation of terrorist content online, designation per se is not the sole problem disclosed by this study, which illuminates both the inadequacy of contemporary legislation for underpinning measures warranted in the online world, and the irrelevance of the rule of law when systems of justice are not made amenable to digital application. We consider that bringing criminal justice into the 21st century should be the priority of policymakers.



GENERAL RECOMMENDATIONS

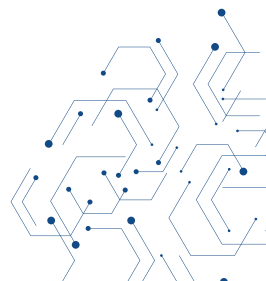
We present here a number of general recommendations for those entities making terrorist designations. In our appendix, we also detail specific recommendations for ten national and two supranational designation systems as appropriate to their context.

Transparent designation systems

- Designating authorities should make their list of designated, proscribed, dissolved, or banned organisations both public and easily accessible. In addition, they should ensure their listing procedures are transparent, making clear reference to the legislative provision which underpins the lists, the legal and practical consequences for listed entities, and the appeal and review processes in place. We further recommend that designating bodies implement a system whereby such decisions and relevant evidence can be made available for judicial inspection and oversight.
- Ensure that there is a separate listing process for the designation of terrorist groups that does not conflate these listings with groups that are anti-constitutional, subject to political proscription, or any other status that is not terrorist. This would ensure that the greater stringency of counterterrorism measures, whether online or offline, is not applied to groups that are not terrorist in nature, and thereby forestall breaches of human rights law by engaging in disproportionate action.

Clarity on the online terrorist content

- Enforce a three-layered system to adjudicate illegal content in the rule of law. This would be content that is produced by a designated or proscribed organisation that leads to the commission of a terrorist offence. This can then be enforced by a regulatory body which makes this implementable for tech companies and a Classification Office that bans specific material so the adjudication of what constitutes as terrorist content is made by public entities rather than private entities.
- Explicitly state in statutory form that online content which incites violence is illegal where it is already illegal offline, and thus ensure that offline and online laws applicable to speech are aligned. This in tandem with designation will ensure that terrorist content which incites violence, but that is not created by a designated entity, can be identified and moderated as such.
- Provide concrete examples of content that are illegal under such a framework and content that has been implicated in successful prosecutions to aid tech company moderators' understanding in what should be removed on legal grounds. This can be done by creating an institution such as the Classification Office in New Zealand.
- Provide a clear definition of "terrorist content" in online regulation or Terrorism Acts to ensure that, with a basis in principles established by law, tech companies can direct their moderation efforts at content that otherwise falls out of the scope of designated terrorist groups. Provision might, for example, be made to automatically designate lone actors as terrorists, so that material from lone actors committing an attack, including manifestos and livestreams, is by default illegal and tech companies therefore entitled to remove it. This is vital to ensure that online counterterrorism becomes better at removing far-right terrorist material.



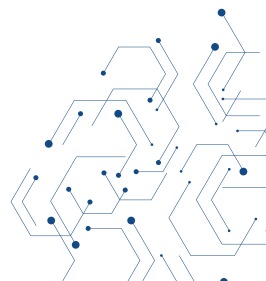
- We recommend countries' classification office to have a content repository that has copies of material that gets banned as terrorist content as well as material that has been used for successful war crimes or terrorist prosecutions. This will help tech companies understand what type of material is illegal and inform them about what type of material has been useful for criminal prosecutions of terrorist offences, as it may be hard for platforms to understand what material they should archive as digital evidence. The Terrorist Content Analytics Platform (TCAP) will support this by creating an archive of verified terrorist content with a page on material that has been used for criminal prosecutions of terrorist offences as well as war crimes.

Designation of far-right terrorist entities

- Reflect the emerging threat landscape by designating more far-right terrorist groups to accurately reflect and respond to the danger stemming from national and trans-national far-right terrorist groups.

Upholding Human Rights

- Establish regular review periods so that designated groups can be delisted if disbanded, or re-designated under a new name in the event of a name change in order to preserve and enhance the efficacy of counterterrorism efforts.
- Lay out clear and accessible appeal mechanisms so that listings can be contested and inclusion discontinued if warranted by law, and thereby relieve executive agencies of some of the burden of initiative and effort in maintaining operationally relevant lists.
- Include civil society representatives, counterterrorism specialists, and human rights lawyers in the process of designating and delisting entities to allow a more nuanced approach with greater oversight from subject matter experts.



1. INTRODUCTION

Tackling terrorist use of the internet, and in particular the dissemination of online propaganda material, has become a primary objective of counterterrorism initiatives across the world following several high-profile terrorist attacks which made effective use of digital methodologies.¹

Spurred by public calls for tech companies to “do more”, global policymakers have therefore within the last five years, aimed to mitigate the spread of terrorist content online.² They have done this by sharpening regulatory approaches and consequently have suggested measures including content removal deadlines, obligatory use of automated content removal technologies, and transparency requirements.

Whilst many such measures may prove to be useful, one legal tool that has been notable by its absence from online counterterrorist discourse is designation – the system by which the authorities within a jurisdiction can classify either a group or an individual as ‘terrorist’.

1.1. Designation

In most jurisdictions, such classification permits the curtailment of designated entities’ rights. This mechanism has been widely used within counterterrorism for over twenty years to limit terrorists’ entitlement to travel or receive funds. Yet, to date, there has been only limited deliberate application in the field of counterterrorism online, despite evidence, which we explore below, that tech platforms are more disposed to take action against specific groups exploiting their platforms if such groups have been designated.

Designation is a mechanism available exclusively to government agencies exercising delimited powers and are subject to democratic accountability. Beyond its practical utility, designation helps to confine restrictions of online content within the parameters of the law when it is practised by private entities such as tech platforms. The decisions of what constitutes terrorism and terrorist content is a political one, and one that ought to be made only by democratically accountable governments and never remitted to private tech companies.

In this report, we survey how designation is currently deployed in twelve jurisdictions. We also examine the implications of existing designation systems for online content, and we recommend how states and inter-governmental organisations might ensure that designation can be practised effectively in the 21st century. In doing so, we answer the following questions:

- 1) What terrorist designation systems are employed by nation states and supranational institutions?
- 2) What implications does the designation (of a terrorist entity) have for online content produced by or in support of the designated entity?
 - i. Is there online terrorist content that falls outside of the scope of existing legal mechanisms?
- 3) What human rights safeguards exist in the designation systems deployed and what are the considerations currently overlooked?
- 4) How can global designation processes be improved to provide guidance for the moderation of online content and as a result improve online counterterrorism efforts?³

¹ [Global Internet Forum to Counter Terrorism](#); [Christchurch Call to Action](#); [European Union Internet Referral Unit](#)

² Online Regulation Series, Tech Against Terrorism, 2021; 2022.



In drafting this report, this work has greatly benefited from expert interviews with Jason Blazakis, Dr. Anna Meier, David Shanks - Chief Censor of the New Zealand Classification Office at the time of writing this report and Gavin Sullivan, Reader in International Human Rights Law at The University of Edinburgh, lead researcher for the UKRI-funded project, *Infra-Legalities: Global Security Infrastructures, Artificial Intelligence and International Law* and lawyer who has provided pro-bono legal representation to people targeted by security lists worldwide, including before the UN Office of the Ombudsperson.

1.2. Why does designation matter for tech companies?

At Tech Against Terrorism, we fundamentally believe in the rule of law and argue that online counterterrorism efforts should be grounded in it. Designation provides a meaningful way of doing this.

Global tech companies, whether large or small, are in general more than willing to counter terrorist use of their platforms. As a case in point, 94% of all terrorist content reported to tech platforms via our Terrorist Content Analytics Platform (TCAP)⁴ has been removed.⁵ This willingness notwithstanding, small platforms often struggle to identify and action terrorist content accurately. While larger tech platforms do have in-house counterterrorism experts capable of supporting such efforts, smaller platforms are markedly less able to afford such resources. Designation can therefore offer valuable authoritative guidance to tech companies in moderating content. This point that has also been made by larger tech companies.⁶

Furthermore, the practice of incorporating designation into moderation guidance explains the high removal rate of identified terrorist content following alerts generated by the Terrorist Content Analytics Platform. Platforms are only notified of content verifiably produced by designated terrorist groups.⁷ Platforms naturally feel more confident about removing material attributable to groups designated by several global jurisdictions.⁸

We also know from experience of notifying material produced by non-designated entities to smaller platforms that designation directly influences a platform's decision to act, because they are able to proceed by reference to material certified as warranting removal. Academic studies provide evidential support for the assertion designation lists can facilitate removal of terrorist content.⁹ There seems to be consensus that when it comes to clearly demarcated terrorist content, or in other words, material produced by designated terrorist organisations, tech companies should moderate this from their platforms.¹⁰

³ A detailed methodology can be found in the annex under section 1.

⁴ The Terrorist Content Analytics Platform (TCAP) is a database of verified terrorist content built by Tech Against Terrorism with the support of Public Safety Canada. The TCAP alerts terrorist content to tech companies when it is identified on their platforms.

⁵ TCAP Transparency Report, Tech Against Terrorism, 2021.

⁶ [Terrorist Definitions and Designations Lists](#), Chris Meserole and Daniel Byman, Global Research Network on Terrorism and Technology: Paper No. 7, 2019; [Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook?](#), Monika Bikert and Brian Fishman, Meta, 2018.

⁷ [TCAP Inclusion Policy](#)

⁸ In fact, removal rates are much lower for far-right terrorist content, which is likely due to the fact that there is much less consensus across jurisdictions about such groups terrorist status. See: [TCAP Transparency Report, Tech Against Terrorism, 2021](#).

⁹ [Terrorist Definitions and Designations Lists](#), Chris Meserole and Daniel Byman, Global Research Network on Terrorism and Technology: Paper No. 7, 2019; [Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook?](#), Monika Bikert and Brian Fishman, Meta, 2018; [Facebook's Secret "Dangerous Organizations and Individuals" List Creates Problems for the Company—and Its Users](#), Jillian York and David Greene, Electronic Frontier Foundation, 2021.

¹⁰ [Marginalizing Violent Extremism Online](#), William Braniff and Audrey Alexandar, Lawfare, 2021.

2. REVIEW OF DESIGNATION JURISDICTIONS AND PROCESSES

The below table is a summary of the designation processes employed by ten countries and two transnational institutions. The annex of this report provides a further breakdown of each jurisdiction. The below table is further explained in the next section.

2.1. Overview

Table 1: Overview of designation jurisdictions and processes.

	United Nations	European Union	United States	United Kingdom	Canada	Australia	New Zealand	France	Germany	Denmark	Sweden	Spain
Does the country have a designation list or a legal equivalent?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
What type of system does the country use?	Designation	Designation and sanctions (UK)	Designation (FTOs) 7 Sanctions (SDN)	Proscription & sanctions	Designation	Proscription	Designation	Dissolution	Proscription, Sanctions, judicial approach	Political proscription	N/A	Proscription
Is terrorist content illegal?	N/A	<input checked="" type="checkbox"/>	Not necessarily, depends on material support or incites imminent unlawfulness	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not necessarily, only if abhorrently violent	Not necessarily, only if objectionable	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not necessarily, only if incites
Is content produced by designated terrorist groups illegal?	N/A	Only if categorised as "terrorist content"	Not necessarily, depends on material support	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not necessarily, only if abhorrently violent	Not necessarily, only if objectionable	<input checked="" type="checkbox"/>	Symbols from all banned groups are illegal	Not as of yet, maybe under proposed legislation	<input type="checkbox"/>	Not necessarily, only if incites
Is content the incited violence or terrorism illegal?	N/A	<input checked="" type="checkbox"/>	Yes, if incites to imminent unlawfulness	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, as it is classified as abhorrently violent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Yes, under proposed regulation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Are far-right terrorist groups represented on the lists?	<input type="checkbox"/>	<input type="checkbox"/>	One on the FTO list, impossible to designate domestic terrorist groups	Yes, but skewed towards Islamist groups	<input checked="" type="checkbox"/>	1 far-right group, heavily skewed towards Islamist groups	Only the Christchurch attack perpetrator, heavily skewed towards Islamist groups	N/A	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A	Only political parties, from those two from the far-right side
Do the lists have human-rights compliant mechanisms in place?	Delisting possible by member States	* Review: 6 months * Appeals can be made by groups and Member States	* Review every 2 years * Appeal in 30 days	* No Review * Appeal for delisting	* Review between 60 days - 5 years	* Review every 3 years * No appeal	* Review every 3 years * Can appeal to the Prime Minister for designation to be revoked	Dissolved groups can appeal		<input type="checkbox"/>	N/A	<input type="checkbox"/>
Is designation tied to the country's definition of terrorism?	<input type="checkbox"/>	Based on the definition of a "terrorist act"	FTO list on "terrorist activity", lack of legislation to designate groups based on the domestic terrorism definition	Linked to definition of terrorism	Based on the definition of "terrorism" and "terrorist activity"	Proscription and judicial approach based on the definition of "terrorism", sanctions are independent of the definition	Based on the definition of a "terrorist act"	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





2.2. Challenges with implementing designation to regulate online terrorist content

Proceeding from Table 1, we identify the principal characteristics of worldwide designation practices. This section discusses, how, as it stands, designation does not bridge the divide between online and offline as it suffers from too many operational challenges to guide the moderation of terrorist content online.

After identifying the challenges, we offer proposals to improve designation so it becomes fit for purpose.

The presence of designation systems

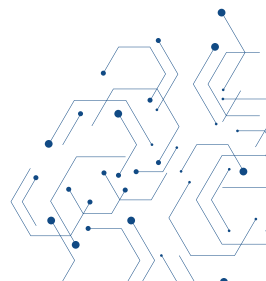
Most countries and institutions examined in this report have some form of designation system by which they classify terrorist groups and maintain a list of these entities. However, these are all referred to differently (as seen in the table from designation, to proscription, to banning, to political proscription) and are based on different legislation. This creates challenges both offline and online.

 Offline	 Online
<p>Unclear and difficult to implement Designation systems diverge because they are based on fragmented sources of national law which equally provide for a variety of legal effects. A globally coordinated response requiring the concerted application of different powers is therefore a complex and demanding exercise.</p>	<p>Unclear and difficult for tech companies, especially smaller ones to understand Tech company moderators may find it difficult to understand the national variants, respective legal bases, and effects of designation. This is especially the case for smaller tech companies who have neither the capacity to acquire nor the capability to deploy the relevant expertise. It is highly unlikely that many tech platforms, large or small, would be able to maintain expertise in the multiple domains of policy, operational practice, and law which are relevant to counterterrorism.</p>



Legality of terrorist content

Countries differ in the extent to which online content produced by or in support of a designated terrorist group is illegal. In the UK, Canada, and Germany, this is made explicit, whereas in many other countries it depends on other criteria, such as whether the material incites violence or whether it is “objectionable” (New Zealand) or “abhorrently violent” (Australia).

In the latter case, this would mean that an internet user or a tech company would have to decide whether such criteria is met before accessing such content or having it on one’s platform.



This leads to the following online challenges.

 <p>Offline</p>	 <p>Online</p>
<p>Unclear how the online incitement leads to offline implications. Online incitement that may lead to organising offline terrorist or violent extremist events and attacks needs to be made illegal in all circumstances, reflecting the same speech laws that account for offline incitement. At the moment, this risks neglecting digital evidence of incitement as well as incitement of terrorism to continue online.</p>	<p>Leaves the responsibility of adjudicating on what constitutes as terrorist content and how to moderate it to tech companies</p> <p>Whilst we recommend countries to make terrorist content clearly illegal, inconsistency between jurisdictions inhibits the full potential benefit of designation as a form of reference for the practice of counterterrorism online. In the absence of such consistent provision, tech companies are forced to decide what content should be classified as terrorist and therefore be moderated. This leads to private entities being responsible for setting speech norms online, rather than democratically elected governments. In addition, by placing the responsibility of determining whether content is terrorist on tech platforms, there is a high risk that, out of an overabundance of caution, those who do not meet the definition of terrorism may be subject to unjust infringement on free speech, while those who are engaged in novel and undetectable but nonetheless terroristic forms of speech may be able to spread their messages online.</p>



Incitement to violence

Most of the countries examined do criminalise the incitement of violence. However, what this constitutes online is not made explicit by most, since legal frameworks rarely clarify if online incitement of violence is illegal.¹¹

¹¹ In the recommendation section of this work, we analyse why we deem this should be made explicit.





This leads to the following offline and online challenges.

 Offline	 Online
<p>Explicit offline Incitement to violence is overwhelmingly illegal offline, including incitement of violence for terrorist purposes. Whereas it may still be difficult to ascertain what is considered incitement to violence, there is judicial oversight.</p>	<p>Implicit online Tech companies often must moderate terrorist content on the assumption incitement to violence is illegal online. There is a lack of clarity on what can be considered as incitement to violence online, and when this is decided, this is done by tech company moderators rather than courts. However, most tech companies already make incitement to violence a breach of their Terms of Service (ToS).</p>

Designation of far-right terrorist groups

Despite the evolving threat picture which has seen a rise in far-right terrorist threats, most examined countries' designation lists are heavily skewed towards Islamist terrorist groups, with either none or only a few far-right terrorist groups listed. Whilst Germany has listed a considerable number of far-right groups, they are listed as "anti-constitutional" and not as "terrorist". Canada and the United Kingdom have, to date, designated the most far-right groups as terrorist, with nine and five (including four aliases) respectively.

This leads to the following consequences offline and online.

 Offline	 Online
<p>Skewed towards Islamist actors, undermining counterterrorism efforts Due to their freedom from designation, far-right terrorist groups are relatively uninhibited in training, recruiting, meeting offline, financing, and fulfilling other terrorist purposes. This significantly undermines the fight against the threat from the extreme violent far-right and also consequently neglects a legal instrument that can be used to tackle it.</p>	<p>Skewed away from far-right actors The dissemination of far-right content is unimpeded by the wide awareness of imagery and tactics which makes online environments increasingly hostile for Islamist actors. As the Terrorist Content Analytics Platform shows, 94% of Islamist content gets removed versus 50% for the far-right, which we consider partly to be due to the lack of designation of far-right terrorist groups and, furthermore, the lack of actionable consensus when they are designated.¹²</p>

¹² [Terrorist Content Analytics Platform Transparency Report](#), Tech Against Terrorism, 2021.



Review processes

Most countries do have regular review processes whereby the designation of a terrorist group is revised and sometimes recalled, but these are often protracted and complex. There is often no formal protocol in place to consider a group which has disbanded or is otherwise wholly inactive.



Offline

Inaccurate lists with consequences for human rights

Inaccuracy means that entities are listed for longer than they should be, resulting in the imputation of criminality and the imposition of punitive measures where neither are warranted. Inaccuracy as a result of the absence of an effective review wastes resources and risks defeating the purpose of designation if listed groups have, since inclusion, begun to operate under a different name, or ceased operation entirely.

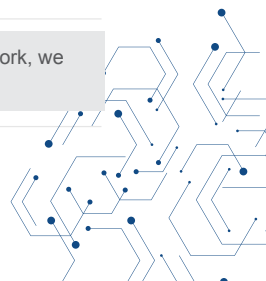


Online

Inaccurate lists with consequences for human rights, especially freedom of expression online

One online effect of unwarranted designation as a result of ineffective review is to wrongly infringe digital rights, especially freedom of expression. A graver effect of this inaccuracy is to confuse those in the private sector tasked with moderation and enforcement in online spaces.¹³ This leads to on the one hand, members of those groups sometimes suffering from stringent restrictions on their rights for too long, and on the other hand, risking leaving terrorist content online due to inaccurate names of groups. This is exemplified by the case of Hay'at tahrir al Sham which is still designated under the al-Nusra front by the US State Department Foreign Terrorist Organisations list.

¹³ In the next section of this report, we delve deeper into these human rights issues, and in the recommendations section of this work, we provide examples of how to ensure human rights are respected and protected more in designation systems.



Definitions of terrorism and designation systems

Countries and institutions are split almost evenly in the coordination between their designation processes and their definitions of terrorism: some designation lists are rooted in the definition of terrorism whilst others are not, such as Canada whose list is dependent on the definition of terrorism and terrorist activity, whilst the UN has not based their list on a definition of terrorism given they don't provide a standard definition.¹⁴



Inconsistency between terrorism and the label of a terrorist group

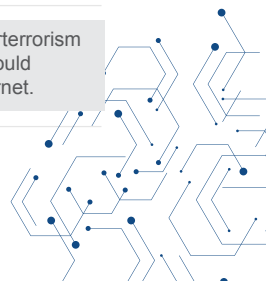
This creates opaqueness and confusion about the thresholds for designation as terrorist groups.



Suboptimal use of legal definitions alongside designation for the moderation of online terrorist content

Designation is but one mechanism capable of guiding the moderation of terrorist content online, and definitions could be another. Without alignment between the two, neither tool will be effective. There will be inconsistency and unclarity about what content falls within scope of the respective tools. In turn, tech companies are unable to remove content because they find it difficult to determine what is terrorist content and whether it is produced by a designated terrorist entity.

¹⁴ We consider that the process of designating terrorist groups should be based on a legal definition of terrorism to ensure counterterrorism policies, online and offline, are rooted in the rule of law. In our models' sections of this work, we will elaborate on how countries could combine these to ensure they provide strategic leadership on regulating the online sphere and countering terrorist use of the internet.



3. UPHOLDING RIGHTS WHILE DESIGNATING TERRORISM

Our review highlights how the instrument of designation is highly complex and fraught with operational challenges. In this section, we draw attention to the human rights concerns associated with designation. It is essential that for anyone thinking of using designation to guide the moderation of terrorist content online, these are addressed.

3.1 Humanitarian

The designation of entities (whether groups or individuals) as terrorist – and the resulting sanctions against those entities – can impede the resolution of conflict, the struggle for self-determination by conventional armed groups, and access to humanitarian aid.

Tech Against Terrorism recognises that there are many problems with this and acknowledge that designation is therefore a highly contested and complex issue. Humanitarian work can be paralysed and civil society organisations maliciously targeted for supposed links to designated groups. Fionnuala Ní Aoláin, the Special Rapporteur on Counter-terrorism and Human Rights, emphasises that the UN requires no exemption clause for civil society actors in national counterterrorism provisions. This requirement leaves humanitarian actors vulnerable to accusations of supporting listed entities.¹⁵ National designation regimes have indeed been criticised for curbing the activities of human rights defenders and civil society actors by use of counterterrorism measures.¹⁶ For example, human rights experts recently condemned the Israeli government's designation of six Palestinian civil society groups.¹⁷

These humanitarian concerns are especially visible following the designation and imposition of sanctions on entities such as the Taliban, Hamas, and Hezbollah. Most recently, there has been uncertainty over how to treat the Taliban as a sanctioned entity (by the UN,¹⁸ Canada,¹⁹ and the US Treasury²⁰) since it became the de facto government of Afghanistan. Reluctance to breach sanctions has caused financial institutions to delay the transfer of funds to humanitarian agencies, which in turn has forced NGOs to scale back their operations and exacerbated the already grave humanitarian crisis in Afghanistan.²¹

In Gaza, the designation of Hamas as a terrorist organisation by some states has had a similar effect, with aid projects cut or blocked and programmes designed to prioritise the management of organisational risk over an effective localised response.²² International assistance to support Lebanon has also been complicated because of terrorist designation. According to the Wall Street Journal, Hezbollah's role in the Lebanese government has meant US aid has been diverted around official channels and impeded its timely disbursement to the Lebanese people.²³ The unintended and potentially detrimental consequences of designation on the lives of civilians living in conflict zones therefore warrants the development of more nuanced measures.

¹⁵ Office of the United Nations High Commissioner for Human Rights, [A/74/335: Promotion and protection of human rights and fundamental freedoms while countering terrorism](#), 2019.

¹⁶ [Human Rights and Counterterrorism](#), Clive Walker, UNOCT, 2016.

¹⁷ [Israel's Counterterrorism Designation Regime: A Process in Need of Reform](#), Lila Margalit and Yuval Shany, *Lawfare*, 2022.

¹⁸ UN Security Council Sanction 2018.

¹⁹ [Canada, Public Safety Canada, Listed Entities](#)

²⁰ [Executive Order 13224, US Department of State](#)

²¹ [U.S. Sanctions Squeeze Humanitarian Assistance in Afghanistan](#), Jacob Kurtzer, Kelly Moss, and Sue Eckert, Centre for Strategic and International Studies (CSIS), 2021.

²² [Counter-terrorism and humanitarian action: Tensions, impact, and ways forward](#), Sara Pantuliano, Kate Mackintosh, Samir Elhawari, and Victoria Metcalfe, Humanitarian Policy Group, 2011.

²³ [U.S. Won't Send Aid to Lebanese Government Over Terror-Finance Concerns](#), Ian Talley and Mengqi Sun, *Wall Street Journal*, 2020.

Whereas these concerns are not to be forgotten – this does not necessarily mean that the process of designation is therefore impossible to apply online – rather that governments need to be aware of such unintended consequences and that these risks need to be mitigated before doing so.

3.2. Constitutional

Lack of definitional clarity of terrorism

The process of designating terrorist entities is not always based on the definition of terrorism formalised by a particular country. Whereas the EU has adopted a definition of terrorism, UN Resolution 1373 encourages states to create their own lists to prevent terrorist financing and further to enact other measures criminalising support for terrorism.²⁴

The absence of a precise definition of what constitutes terrorist acts and groups allows elastic standards and arbitrary powers. Since the 9/11 terror attacks and the new counterterrorism measures that were brought in globally in response, human rights advocates have raised concerns around governments justifying the targeting of political opposition or activists by labelling them ‘terrorists.’²⁵

Pre-emptive punishment

In some jurisdictions, listing entities as terrorist is pre-emptive in that punitive measures are imposed on the basis of suspicion rather than proof of complicity in criminal wrongdoing, and furthermore permits criminalisation by administrative decree. The al-Qaeda and ISIS sanctions lists provide the UN Security Council with unprecedented legal powers and have been described as “a weapon of pre-emptive warfare.”²⁶

Those proposing this description argue that Resolution 1267 grants powers unlimited in jurisdiction or duration for the Security Council to target individuals and entities using secret material suggesting potential ‘association with’ al-Qaeda and later ISIS. The process of delisting through the Ombudsperson involves invasive intelligence gathering on that individual or entity despite listing being pre-emptive, and therefore reverses both the burden of proof and the presumption of innocence.

Lack of transparency

Listing decisions sometimes rely on secret intelligence with determinative evidence withheld from courts and the targeted individual or entity. UN lists and the Ombudsperson’s report on their reasoning for denying or accepting delisting requests is not made available to the petitioner or the public.²⁷

Martin Sheinin, the former UN Special Rapporteur on Counter-terrorism and Human Rights, has recommended that a listing process should involve referring speculative allegations which result from intelligence back to the courts where the underlying evidence can be properly tested and challenged.²⁸ Otherwise, there is a risk of politically motivated and unaccountable covert targeting of individuals or groups.

²⁴ [United Nations Resolution 1373](#), 2001.

²⁵ [The Law of the List](#), Gavin Sullivan, Cambridge University Press, 2020.

²⁶ [The Law of the List](#), Gavin Sullivan, Cambridge University Press, 2020.

²⁷ [Historical Guide of the Ombudsperson Process through Security Council resolutions and Reports of the Office of the Ombudsperson to the Security Council](#), Office of the Ombudsman, 2018.

²⁸ Office of the United Nations High Commissioner for Human Rights, [A/61/267. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism](#), 16 August 2006, paragraph. 31.

Judicial review and the right to remedy

Judicial review is an essential constitutional mechanism by which members of the public, on an individual and collective basis, can hold public bodies accountable for the exercise of their powers, and it is the means by which designated individuals and organisations can dispute listing decisions and rebut the underlying allegations against them. Listing decisions should have an evidential basis capable of withstanding judicial scrutiny to prove interference in the liberty of the subject is not arbitrary.

Within the UN framework, individuals can only be listed based on their association with a designated group, which has the effect of expanding the UN's jurisdiction beyond states to individuals who, when listed, cannot work, travel, or rent a house and could have their finances frozen.²⁹ Individuals can be delisted but this entails a lengthy procedure through the Office of the Ombudsperson.³⁰ The UN Security Council created the UN 1267 Office of the Ombudsperson in 2009, a procedure for redress in which listed individuals, groups, or entities could apply to be delisted by an independent legal expert. Since then, 93 proceedings have been completed with 65 petitions granted resulting in 60 individuals and 28 entities being delisted.³¹ However, it should be noted that the Security Council Sanctions Committee retains the power to reject by consensus delisting recommendations.³²

International proscription regimes, especially the regime operated by the UN Security Council, have been criticised for lacking basic standards of due process, and “systematic violations have been recognised repeatedly in judicial proceedings, particularly within Europe.”³³ In the past, successful legal challenges have been ignored by the executive bodies of the UN and EU with those litigants remaining on blacklists.³⁴ In the landmark *Kadi* decision³⁵ in 2008, the European Court of Justice (ECJ) affirmed that individuals have the right to be informed of the reasons why they are listed, and that the EU must respect fundamental rights when implementing UN sanctions.³⁶

²⁹ [The Law of the List](#), Gavin Sullivan, Cambridge University Press, 2020.

³⁰ [Ombudsman Procedure](#), United Nations Security Council.

³¹ [Status of Cases](#), United Nations Security Council.

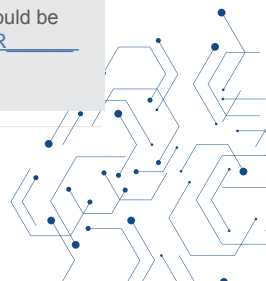
³² [Ombudsman Procedure](#), United Nations Security Council.

³³ Statewatch Analysis Time to rethink terrorist blacklisting, Ben Hayes and Gavin Sullivan, Statewatch Journal, 2010.

³⁴ For example, the cases of [Abdullah Kadi](#) (Statewatch: 2012) and Abousfian Abdelrazik (CanLII Connects 2015).

³⁵ In 2008, the European Court of Justice overturned an EU Court of First Instance ruling that the funds of Yassin Abdullah Kadi could be frozen by a regulation of the Council of the European Union following resolution by UNSC. [European Court of Justice, 2008 E.C.R. \(2008\)](#)

³⁶ [The Law of the List](#), Gavin Sullivan, Cambridge University Press, 2020.



4. CONCLUSIONS AND RECOMMENDATIONS

We have thus far detailed how designation, as it stands, suffers from significant operational challenges that make it difficult to implement online. In addition, there are human rights concerns that critics have highlighted.

However, we find that rather than ignoring an existing legal tool that has the potential to tackle terrorist content online, governments should improve their systems to make it fit for purpose.

Governments and jurisdictions must give a clearer direction for tech companies to follow. In our Annex, we detail a number of recommendations for specific jurisdictions to follow. They are summarised in general recommendations here.

4.1. General Recommendations

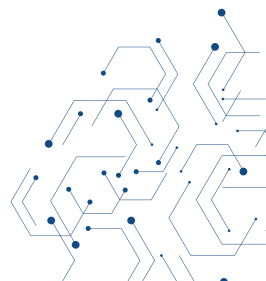
In general, we recommend that all designating entities undertake the following remedial actions. Underpinning all of this is a need for more coordination between designation systems.

Transparent designation systems

- Designating authorities should make their list of designated, proscribed, dissolved, or banned organisations both public and easily accessible. In addition, they should ensure their listing procedures are transparent, making clear reference to the legislative provision which underpins the lists, the legal and practical consequences for listed entities, and the appeal and review processes in place. We further recommend that designating bodies implement a system whereby such decisions and relevant evidence can be made available for judicial inspection and oversight.
- Ensure that there is a separate listing process for the designation of terrorist groups that does not conflate these listings with groups that are anti-constitutional, subject to political proscription, or any other status that is not terrorist. This would ensure that the greater stringency of counterterrorism measures, whether online or offline, is not applied to groups that are not terrorist in nature, and thereby forestall breaches of human rights law by engaging in disproportionate action.

Clarity on the online terrorist content

- Enforce a three-layered system to adjudicate illegal content in the rule of law. This would be content that is produced by a designated or proscribed organisation that leads to the commission of a terrorist offence. This can then be enforced by a regulatory body which makes this implementable for tech companies and a Classification Office that bans specific material so the adjudication of what constitutes as terrorist content is made by public entities rather than private entities.
- Explicitly state in statutory form that online content which incites violence is illegal where it is already illegal offline, and thus ensure that offline and online laws applicable to speech are aligned. This in tandem with designation will ensure that terrorist content which incites violence, but that is not created by a designated entity, can be identified and moderated as such.



- Provide concrete examples of content that are illegal under such a framework and content that has been implicated in successful prosecutions to aid tech company moderators' understanding in what should be removed on legal grounds. This can be done by creating an institution such as the Classification Office in New Zealand.
- Provide a clear definition of “terrorist content” in online regulation or Terrorism Acts to ensure that, with a basis in principles established by law, tech companies can direct their moderation efforts at content that otherwise falls out of the scope of designated terrorist groups. Provision might, for example, be made to automatically designate lone actors as terrorists, so that material from lone actors committing an attack, including manifestos and livestreams, is by default illegal and tech companies therefore entitled to remove it. This is vital to ensure that online counterterrorism becomes better at removing far-right terrorist material.
- We recommend countries' classification office to have a content repository that has copies of material that gets banned as terrorist content as well as material that has been used for successful war crimes or terrorist prosecutions. This will help tech companies understand what type of material is illegal and inform them about what type of material has been useful for criminal prosecutions of terrorist offences, as it may be hard for platforms to understand what material they should archive as digital evidence. The Terrorist Content Analytics Platform (TCAP) will support this by creating an archive of verified terrorist content with a page on material that has been used for criminal prosecutions of terrorist offences as well as war crimes.

Designation of far-right terrorist entities

- Reflect the emerging threat landscape by designating more far-right terrorist groups to accurately reflect and respond to the danger stemming from national and trans-national far-right terrorist groups.

Upholding Human Rights

- Establish regular review periods so that designated groups can be delisted if disbanded, or re-designated under a new name in the event of a name change in order to preserve and enhance the efficacy of counterterrorism efforts.
- Lay out clear and accessible appeal mechanisms so that listings can be contested and inclusion discontinued if warranted by law, and thereby relieve executive agencies of some of the burden of initiative and effort in maintaining operationally relevant lists.
- Include civil society representatives, counterterrorism specialists, and human rights lawyers in the process of designating and delisting entities to allow a more nuanced approach with greater oversight from subject matter experts.

³⁷ Online Regulation Series, Tech Against Terrorism, 2021; 2022.



4.2. Setting an international framework for terrorist designations

We have shown that there are different challenges faced by individual designation systems implemented by nation states and supranational institutions. The fragmented approach to using designation to guide online terrorist content further compounds the challenge of rethinking the practice worldwide. As we have argued elsewhere with respect to online regulation, fragmentation is an inherent risk when divergent legislative regimes undertake concerted action against online harms, and frequently undermines online counterterrorism efforts.³⁷ Terrorist exploitation of the internet is a global problem, and therefore needs a global solution, and the next model argues how the UN can utilise designation as one such potential solution.

To improve current global designations to better equip them for the digital age, we propose three models that can help clarify designation's implications for online terrorist content. Whilst no model can be perfect without application in practice, we believe that what follows nonetheless constitute significant improvements to the current designation mechanisms and can provide a starting point for broader policy discussions.

Whilst this proposal mostly focuses on the designation of groups, we offer reflection on where models might be applicable to lone actors, and mitigation of their online footprint.

In developing our models, we proceeded by reference to necessary criteria for effective designation which emerges from our consideration of what is not effective.

International consensus: Does the model promote international consensus on terrorist designation lists and their online implications, or does it instead maintain or indeed aggravate the fragmentation of designation systems?

Rule of law: Do governments shoulder the responsibility for providing a means to coordinate designation and online enforcement with a proper basis in law, or is adjudication of terrorist content remitted to tech companies by reference only to their Terms of Service?

Practicality: Is the model practicable, capable of implementation within existing frameworks and without jurisdictional conflict, and compatible with domestic variants of designation (political proscription, banning etc.)?

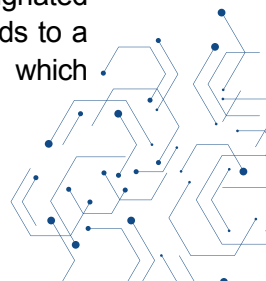
Clarity for tech companies: Does the model supply clear guidelines for tech companies to determine the legality of content on their platforms and shape their moderation practices?

Domestic agency: Does the model create sufficient opportunity for domestic lawmakers to establish online speech norms in their jurisdictions.

Abuse risk: Does the model increase vulnerability to the politicised application of counterterrorism measures and breaches of human rights, as described previously?

Human rights: Does the model afford sufficient positive protection of human rights and engage mechanisms of redress, such as judicial review, which would be capable of protecting freedom of speech?

We have designed two potential models, described below and assessed against the above criteria, that may allow the UN to provide strategic leadership in devolving designation to Member States. These involve a UN Resolution stipulating that official content produced by or in support of a designated terrorist group (based on both national and supranational lists) should be illegal when it leads to a domestic (in the jurisdiction of member states) terrorist offence, and a recommendation which recommends member states to do so only based on their own domestic terrorist offences.

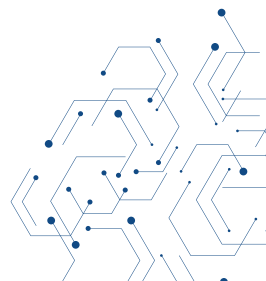


Outline

Model 1 - UN Resolution	Model 2 - UN Recommendation
<p>A UN Security Council Resolution stipulates that official content produced by or in support of a designated terrorist group (based on both national and supranational lists) should be illegal when it leads to a domestic (in the jurisdiction of member states) terrorist offence. This stipulation would subsequently be given legislative effect by Member States.</p>	<p>The UN Security Council recommends that member states introduce legislation that makes online content produced by domestically designated terrorist groups illegal when it leads to a domestic terrorist offence.</p>
<p>The essential difference between these models lies in the nature of the UN declaration, which in model 1 would be binding, and advisory in model 2. In addition, model 1 suggests adherence to both the UN and domestic lists, whilst model 2 suggests only domestic lists would be adhered to.</p>	

Assessment of our suggested models

RULE OF LAW	
Model 1 - UN Resolution	Model 2 - UN Recommendation
<p>Ensures that the UN, with the help of Member States, sets speech norms on what constitutes terrorist content online, based on the outcome of designation. This would ground global counterterrorism efforts in the rule of law.</p>	<p>Provides guidance on how Member States can set speech norms on what constitutes as terrorist content online, based on the legal instrument of designation. This would ground counterterrorism efforts in the rule of law.</p>
<p>Assessment: Both are equally grounded in the rule of law. Model 1 adheres to both international and national law, whilst model 2 suggests relying on the national laws of member states.</p>	



PRACTICALITY	
Model 1 - UN Resolution	Model 2 - UN Recommendation
Given the involvement of both the UN and Member States, this model would suffer from considerable operational challenges both in developing a global consensus and harmonising implementation.	The greater reliance on Member States, with the UN acting in an advisory capacity, promises to be more practicable.
Assessment: Model 2 is more practicable.	

CLARITY FOR TECH COMPANIES	
Model 1 - UN Resolution	Model 2 - UN Recommendation
Provides tech companies with clearer legal parameters for the adjudication of content. However, given that there are multiple jurisdictions and lists that need to be considered, continuing compliance will prove difficult for tech companies, and especially for smaller tech companies.	Affords a similar degree of clarity, and would also only compel reference to domestic lists, though compliance will remain difficult for smaller tech companies.
Assessment: Model 1 creates a larger requirement for tech companies to understand local as well as international jurisdictions. However, in practice most tech companies already consult the UN list.	

INTERNATIONAL CONSENSUS	
Model 1 - UN Resolution	Model 2 - UN Recommendation
Creates internationally applicable guidance for improved counterterrorist use of designation, deriving from harmonised domestic and supranational lists.	Provides similar guidance in the application of designation to counterterrorism, but eschews alignment of international and domestic lists with reference only to the latter.
Assessment: Model 1 would provide greater international consensus and less fragmentation than model 2.	

DOMESTIC AGENCY	
Model 1 - UN Resolution	Model 2 - UN Recommendation
Stipulates that domestic states must use designation for online counterterrorism efforts and adhere to the UN list as well as their own.	Requires member states to use designation for online counterterrorism efforts, but only based on their own lists.
Assessment: Model 2 would provide greater domestic agency than model 1.	

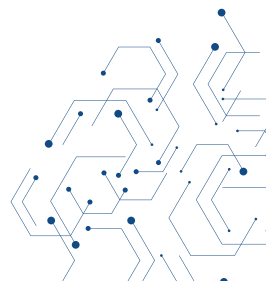


RISK OF ABUSE	
Model 1 - UN Resolution	Model 2 - UN Recommendation
Designation will remain a legal tool that can be politicised and used by nation states to stifle dissent. In the country models we find possible solutions to this.	Designation will remain a tool carrying an inherent risk of politicisation, especially when no supranational guidance is available.
Assessment: Given model 1 relies on both the international and national lists, we deem the risk of abuse to be lower than model 2 which engages solely domestic interests.	

PROTECTION OF HUMAN RIGHTS	
Model 1 - UN Resolution	Model 2 - UN Recommendation
We deem that by following the practical steps mentioned below, through the involvement of civil society, counterterrorism experts and human rights lawyers, this model can build in safeguards for human rights.	Safeguards remain theoretically possible, but are not enforceable at the supranational level.
Assessment: We argue model 1 provides more opportunity to build in human rights safeguards than model 2, as model 1 combines the supranational and domestic levels, whilst model 2 confines enforcement to remedies available domestically.	

Further Discussion

- This framework does not suggest that designation is the only way in which terrorist content can be criminalised and its dissemination impeded; it would be used alongside other instruments, such as the definition of terrorism, or terrorist content, in existing legislation.
- We refer to content that “leads to a domestic terrorist offence”. With that, we mean the legality of official content produced by terrorist groups depends on whether it leads to a domestic terrorist offence in a particular jurisdiction such as support for a terrorist group or incitement to violence. At the time of writing, we found that in some national legislation which criminalises speech inciting violence, it is not explicit that this applies to online content that incites violence.
- In designing these, we recommend that the UN Security Council establish a sanctions sub-committee concerned specifically with the threat of far-right terrorist entities as they did with the sanctions committee concerning ISIL and al-Qaeda.
- We recommend that, in order to ensure the feasibility and efficacy of member states’ legislation the UN seek input from tech platforms, internet companies, and other stakeholders to better understand how terrorists use the internet and how it can be moderated effectively.



4.3. Country-Level Recommendation

Outline

We envision the international and national model working in tandem, and do not deem it necessary to refer to developments at the international level when engaging in domestic reform.

Our proposed national model has three main functions:

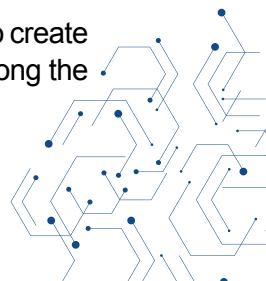
1. Facilitates practical implementation of designation online
2. Clarifies for tech companies the legality of official terrorist content online
3. Counters terrorist use of the internet more effectively with a firmer basis in the rule of law

First, to prevent burdening tech companies with the responsibility of adjudicating what constitutes terrorist material, we argue that countries should pursue a comprehensive regulatory and legislative approach to the subject. The relevance to online material of legislation enacted for offline communications, and how such legislation could be made relevant to the moderation practices that might be adopted by tech companies, is often unclear, and enforcement conducted on this basis can be defective and indeed violative of civil liberties. In the twenty-first century, it is essential that terrorism legislation, in all jurisdictions worldwide, be enacted with explicit provision for online speech.

Second, we recommend that a regulatory body should ensure that tech companies are provided with sufficient guidance on how to put either online regulation or offline terrorism legislation into practice. A regulatory approach conducted on this basis would protect the diversity of the internet by creating equitable requirements that take account of the size of tech companies (both big and small). It would also allow governments to advise that content in support of designated terrorist groups, or content created by terrorist groups, carries a presumption that its dissemination or retention on a platform is unlawful. Such an approach would clarify the parameters incumbent to tech companies in making moderation decisions. However, we warn that non-democratic governments could utilise this system to subvert this – therefore we deem that the international and domestic levels should both be used to implement designation for the regulation of terrorist content online.

Finally, we also recommend that governments establish classification offices, to provide conclusive guidance on what type of material constitutes terrorist content. An example of this is Islamic State's weekly magazine. If on the one hand, Islamic State is a designated terrorist group (which it is globally), relevant regulation should specify that their publications are illegal, whether online or offline if it incites terrorism, or leads to a terrorist offence (see option 2 in the international models). However, this then requires tech companies to decide whether that particular magazine can properly be accredited to Islamic State, before taking action accordingly. A Classification Office could provide concrete examples and guides that can inform tech companies what type of content typically belongs to such groups. An example of such an institution working well is in New Zealand, where the Chief Censor and the Classification Office ban particular types of material. In addition, we would highlight that when an individual believes their content has been banned illegitimately, they can appeal to the Classification Office to contest the ruling which helps to uphold and protect human rights online.

The below model suggests how Member States might reconfigure their designation practices to create domestic systems compatible with however designation at the UN level might develop (i.e., along the lines of either Model 1 or Model 2).



NATIONAL DESIGNATION MODEL

LEVEL 1: GOVERNMENT

CREATE DESIGNATION LEGISLATION

Design online regulation or adapt terrorism legislation to ensure it can be implemented online.

For online regulation, we recommend transparent, effective, operational, and human rights compliant legislation around terrorist content. This should clearly define what is considered online terrorist content.

Terrorism legislation, outlining terrorist offences such as incitement to violence or inviting support for a terrorist group, should clearly guide tech companies on the legality of terrorist content online.

LEVEL 2: REGULATOR

ENFORCE DESIGNATION LEGISLATION FOR ONLINE REGULATION

A regulator would provide more clarity for tech companies on practical steps tech companies can take to identify and remove illegal terrorist content.

Ensure tech platforms comply with regulations.

Assist in adapting relevant legislation to support smaller tech platforms.

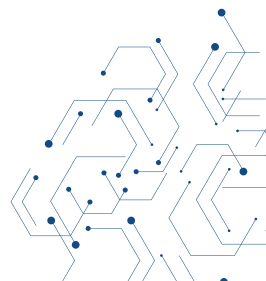
LEVEL 3: CLASSIFICATION OFFICE

DEFINE AND CLASSIFY TERRORIST CONTENT

Independent body where material from designated groups can be considered and classified as terrorist material.

Based on the definition of online terrorist content, counterterrorism experts alongside civil society representatives would adjudicate on the legality of specific pieces of content.

Through banning specific pieces of terrorist content, this would ensure greater guidance for tech companies in removal of terrorist content.



Assessment of our suggested models

Rule of law

This model will tackle the legal grey area of online terrorist content by equating online and offline illegality. For example, official terrorist content (produced by designated entities) that leads to the commission of an existing terrorist offence (e.g., inciting violence, material support etc.) will be illegal online. The Classification Office would be an independent body comprising counterterrorism experts adjudicating whether specific pieces of content pass the threshold to be ‘classified’ as terrorist content. Such a model would ensure that governments rather than tech companies prescribe what is illegal online. The removal of illegal content will be subject to scrutiny through judicial review.

Practicality

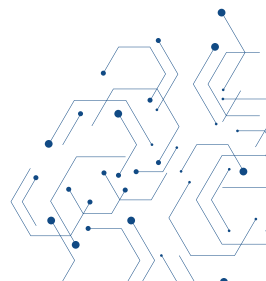
This model is designed to facilitate and make practicable the implementation of designation online. It adapts existing legislation and makes it applicable online, by clarifying that material that commits a terrorist offence is illegal online. The Classification Office then interprets this legislation by determining the legality of specific content, making the removal and moderation of terrorist content by tech companies more effective. The online regulator supports the practical implementation of legislation by providing guidance on how to implement regulation, clarifying tech companies’ responsibility, and advising on identification and removal processes for companies of varying sizes. A potential obstacle for the Classification Office is addressing the vast scale of online terrorist content and classifying new content fast enough to tackle it before it spreads across platforms.

Clarity for tech companies

Providing clarity for tech companies on the legality of terrorist content is a central component of this model. Tech companies often develop their own Terms of Service for countering T/VE content based on their own lists of banned groups or based on a prima facie incitement to violence. By adopting laws which base the legality of content on terrorist designation, tech companies see more clearly which groups to target in their terms of service. Content not affiliated with designated terrorist groups can also be classified based on the definition within legislation concerning terrorism or terrorist content, meaning “grey content” can also be tackled. For specific pieces of content (such as terrorist publications), tech companies can refer to the Classification Office to easily identify and remove known terrorist content. A drawback of this model, especially for smaller tech companies, is they would require awareness of different domestic legislation in order to assess the type of content that leads to a domestic terrorist offence.

Abuse risk

Whilst there is a risk of politicisation within any counterterrorism legislation, this model builds in several safeguards. Vague definitions of terrorism and terrorist content can be exploited to violate freedom of expression and crack down on political speech. More detailed online regulation or terrorism legislation that equates the online and offline illegality of material can prevent this. More importantly, an independent Classification Office adjudicates on specific content reducing the incentives for tech companies to over-remove content based on vague law and a regulator provides a mechanism to ensure that tech companies are adhering to their duty to uphold the law.

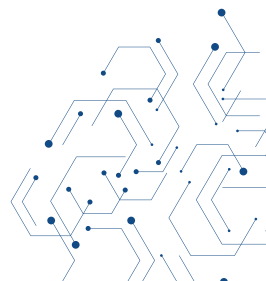


Human rights

In its role as an independent adjudicator on specific content, a Classification Office would reduce the incentives for tech companies to over-remove content based on vague law. The Classification Office would comprise counterterrorism experts and human rights lawyers to ensure classification is accurate and informed by the interests of civil society. Decisions should be subject to challenge through judicial review to judge the legality of specific cases.

Lone and non-affiliated terrorist actors

This model would also allow countries to adopt a system whereby they either designate lone actors as terrorists, and thereby make their online content illegal through the suggested model or could apply the terrorism definition to lone actors' online content. This would allow countries to choose how to tackle online content produced by lone actors, however labelling it explicitly as terrorist content, providing clarity for tech companies. Given that recent attacks by far-right terrorist actors have shown that far-right terrorist attacks are often committed by lone actors, it would also ensure that governments tackle the threat posed by the far-right more efficiently, and that their online content does not remain categorised as "grey content".



5. AREAS FOR FURTHER STUDY

This research has focussed on the designation of terrorist groups, rather than the sanctioning of individuals. This remains an understudied field academically, although human rights advocates and lawyers have shown that these sanctions often lead to significant human rights abuses.

Secondly, whilst the human rights section of this work highlighted the human rights concerns of designation for the offline realm as well, more research should be done on how to ensure designation becomes more important in guiding online regulation, whilst also improving the system offline.

Thirdly, we have focussed on the designation processes by Western democratic nation states and supranational institutions. We would like to expand this study to other countries, learning from other designation systems.

Fourthly, there are types of terrorist content, that are simply difficult to relate to designated terrorist groups, and more work should be done on how to ensure those types of terrorist materials should be banned online, whilst simultaneously balancing freedom of expression and other human rights. A follow-up study to this report should be done to investigate how actors can be designated that operate outside of terrorist groups. This could be with relevance to lone-actor terrorists as well as post-organisational, more fluid terrorist entities.

Finally, recent examples such as the designation of the Islamic Revolutionary Guard Corps (IRGC) by Canada³⁸ and the potential designation of the Wagner group³⁹ following the Russian invasion of Ukraine show the continued importance of designation as a legal tool. There is debate over whether the designation of these entities that operate in conflict situations or entities tied to hostile governments should be designated as terrorist, or whether there are other legal mechanisms that are better fit for purpose. The implications of the designation of these entities in relation to their online content should also be considered.

³⁸ [Canada to implement new measures against the Iranian regime](#), Prime Minister of Canada Justin Trudeau, 2022.

³⁹ Both the United Kingdom and Canada have considered designating the Wagner group as a terrorist entity. [IntelBrief: Will the United Kingdom Proscribe the Wagner Group as a Terrorist Entity?](#), The Soufan Center, 2023.

6. ANNEX

6.1 Country-level investigations

The following section analyses 10 countries and 2 institutions' designation systems. We examine the system employed, the legal basis, the terrorism definition applicable, the balance between the number of violent Islamist and far-right terrorist entities designated, the review process, and the appeal process. We then examine the challenges identified in the system and recommendations to help solve those.



UNITED NATIONS

Does the country or institution have their own list of designated, banned, or proscribed groups?

Yes

What type of system does the country or institution use?

Designation of terrorist entities by the United Nations (UN) is composed of official sanctions. The "Consolidated Sanctions List" is comprised of lists from numerous Sanctions Committees that deal with various sanctions, including those against terrorist entities, state actors, as well as those who commit violations of international law and human rights law.¹ Entities can be recommended for inclusion on the Sanctions List by any member state.

The sanctions regime that has been used to designate terrorist entities is the 1267 regime relating to Islamic State in Iraq and the Levant (ISIL), Al-Qaeda and the Taliban. The Security Council Committee² was initially established pursuant to resolution 1267 (1999)³, which imposed limited sanctions (air embargo and assets freeze) on the Taliban (but not as a 'terrorist entity'). In 2011, the Security Council adopted resolutions 1988⁴ and 1989⁵, which split the designation list in two, one targeting Al-Qaeda (1989) and one targeting the Taliban (1988). In 2015, the Security Council adopted resolution 2253⁶ which expanding the listing criteria to including individuals and entities supporting ISIL. Therefore, the list concerned with terrorist entities is the ISIL (Da'esh) and Al-Qaida Sanctions List (reaffirmed with resolution 2610 (2021)⁷ which is separate to the 1988 Sanctions List relating to individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan.

Additionally, through resolution 1373 (2001), the Security Council introduced a parallel regime by requiring Member States to prevent and suppress the financing of terrorist acts, freeze the funds and resources of individuals who commit, attempt to commit, facilitate or participate in terrorist acts, as well as prohibit the nationals from making funds, financial services or economic resources available to such persons.⁸

As a result, many States have in place, at a national level, legal and institutional frameworks for the designation of individuals or groups, that are either on the United Nations list, or are designated for national or multilateral (e.g., European Union) purposes.

¹ [United Nations Security Council Consolidated List](#)

² In full, the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaeda and associated individuals, groups, undertakings and entities.

³ [United Nations Security Council Resolution 1267 \(1999\)](#)

⁴ [United Nations Security Council Resolution 1988 \(2011\)](#)

⁵ [United Nations Security Council Resolution 1989 \(2011\)](#)

⁶ [United Nations Security Council Resolution 2253 \(2015\)](#)

⁷ [United Nations Security Council Resolution 2610 \(2021\)](#)

⁸ [United Nations Security Council Resolution 1373 \(2001\)](#)





<p>What is the definition of “terrorism” the country or institution employs?</p>	<p>While there is no internationally agreed upon definition of terrorism, the 19 international legal instruments to prevent terrorist acts can guide Member States in the criminalization of acts considered terrorist in nature. The Counter-Terrorism Committee, in its “Technical Guide to the Implementation of Security Council Resolution 1373 (2001) and Other Resolutions”,⁹ has recommended that States ensure that terrorist acts are defined in national legislation with precision and in a manner consistent with the international counter-terrorism instruments.</p> <p>The United Nations Human Rights Office of the High Commissioner argues that key elements of the acts of terrorism in Security Council resolution 1566 (2004)¹⁰ should be used, as well as the Special Rapporteur’s model. The Special Rapporteur’s model specifies that– as the minimum “Terrorism involves the intimidation or coercion of populations or governments through the threat or perpetration of violence, causing death, serious injury or the taking of hostages.”¹¹</p>
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>The designation of terrorist entities by the UN sanctions regime is not guided by a particular definition of terrorism. However, under the 1267 sanctions regime,¹² the overarching criterion for designation is activities indicating association with ISIL, Al-Qaida, or their affiliates, which include participating in the financing, planning, facilitating, preparing, or perpetrating of activities by, supplying, selling or transferring arms and related material to, and recruiting for, or providing any other forms of assistance to, Al-Qaida, ISIL or affiliates. The 1267 Committee provides further guidance on these criteria and its decision-making process in its Guidelines¹³ and the work of the Committee is supported by an Analytical Support and Sanctions Monitoring Team..</p> <p>As mentioned above, UN Resolution 1373 encourages states to create their own designation lists to prevent terrorist financing and to further enact other measures criminalising support for terrorism.¹⁴ However, as noted by Office of the High Commissioner for Human Rights (OHCHR), “ambiguous definitions of terrorism in some States have led to policies and practices that violated the fundamental freedoms of individuals and populations, and discriminate against particular groups.”¹⁵ It is therefore important that national definitions of terrorism “always comply with international principles of legality and legal certainty.”¹⁶</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>N/A</p>

⁹ [Technical guide to the implementation of Security Council resolution 1373 \(2001\) and other relevant resolutions](#), United Nations Security Council (UNSC) Counter-Terrorism Committee Executive Directorate (CTED), 2017.

¹⁰ [United Nations Security Council Resolution 1566 \(2004\)](#)

¹¹ The Office of the High Commissioner for Human Rights (OHCHR) and terrorism and violent extremism

¹² Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da’esh), Al-Qaeda and associated individuals, groups, undertakings and entities

¹³ Guidelines of the Committee for the Conduct of its Work, 2018.

¹⁴ United Nations Security Council Resolution 1373 (2001)

¹⁵ The Office of the High Commissioner for Human Rights (OHCHR) and terrorism and violent extremism

¹⁶ The Office of the High Commissioner for Human Rights (OHCHR) and terrorism and violent extremism





<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>The relationship is complex. The UN does not legislate on what types of online content is permissible. Member States are responsible for implementing online regulation. However, the UN does have the capability to create obligations for Member States to regulate online content through UN Security Council Resolutions.</p> <p>While the legality of online content created by terrorist groups is left to member states, individuals posting online content that incites acts of terrorism for ISIL, Al-Qaeda, or their affiliates or supports those groups (for example, through recruitment, fundraising or through internet hosting) could constitute an act that meets the criteria for designation. The 1267 Sanctions Committee has construed the scope of asset freeze broadly through its resolutions and “Explanation of Terms” on Asset Freeze document, which covers “financial and economic resources”, and includes “internet hosting or related services”. That could mean that if someone provides internet hosting to ISIL, Al-Qaeda or their affiliates for whatever purpose, but particularly where there is a financial dimension or service, subject to the view of the Committee, that individual or entity might have violated asset freeze sanctions measures, even if unwittingly. This provision has not been widely used to date by Member States though.</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>Given the broad designation criteria, online content that incites acts of terrorism for ISIL, Al-Qaida or their affiliates could constitute an act that meets the criteria for designation.</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>Given the broad designation criteria, online content that supports the terrorist groups designated by the UN (ISIL, Al-Qaeda or their affiliates), for example, through recruitment or fundraising for the groups, could constitute an act that meets the criteria for designation.</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No. Individuals and entities can only get designated by association with an entity previously designated (currently ISIL and Al-Qaeda), which means that if there are no far-right terrorist entities listed, individuals tied to such organisations cannot get designated at the time of writing.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>Delisting is possible through the UN 1267 Office of the Ombudsperson, a procedure for redress in which listed individuals, groups, or entities could apply to be delisted by an independent legal expert.¹⁷ Since then, 93 proceedings have been completed with 65 petitions granted resulting in 60 individuals and 28 entities being delisted.¹⁸ However, the Security Council Sanctions Committee retains the power to reject by consensus delisting recommendations.¹⁹ The delisting process contains various stages of review, dialogue, and reporting, the length of the appeal is highly variable.</p>

¹⁷ Procedure, Ombudsperson, United Nations Security Council

¹⁸ Status of Cases, Ombudsperson, United Nations Security Council

¹⁹ Procedure, Ombudsperson, United Nations Security Council



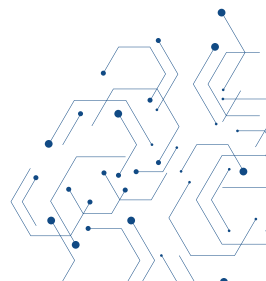


What are the weaknesses in the designation process?

- As far as the 1267 sanctions regime is concerned, there is a clear procedure to delist a defunct entity, either through the Ombudsperson's Office or proposed by the Designating State. However, the current delisting process is long and complex which risks listing groups, entities, and individuals unfairly without evidentiary justification or for longer than necessary.
- Online activities that propagate, recruit, fundraise, and purchase weapons for ISIL, Al-Qaeda and their affiliates meet the criteria for designation. However, given the broad designation criteria for individuals and entities set out in Resolution 1267, it is unclear what specific activities in relation to online propaganda content meet the threshold for designation.
- The designation list does not currently include any far-right terrorist entities given individuals and entities can only get designated by association with an entity previously designated (currently ISIL and Al-Qaeda, and their affiliates). This undermines the UN's wider strategy and advocacy to counter ideological, white supremacist or far-right extremism and terrorism.

What do we recommend?

- The UN Security Council should consider encouraging Member States to review counterterrorism tools and legislations to make sure they adequately reflect the nature of the far-right terrorist threat. The UN would set a good standard in highlighting the threat of these groups and encourage Member States to effectively designate far-right terrorist groups and individuals where appropriate.
- Provide clarity on what online content and activity constitutes an act that meets the criteria for designation. Specify whether this goes beyond incitement of a terrorist act or support through recruitment or fundraising for the designated groups. Additionally, clarify whether individuals providing internet hosting services for terrorist operated websites (for ISIL, Al-Qaeda or their affiliates) meet the criteria for designation.
- The UN could provide strategic leadership and act as a normative voice on counterterrorism and human rights when it comes to the regulation of terrorist content by promoting the use of designation to ground the moderation of terrorist content online in the rule of law.
- The UN could consider doing this through drafting a Security Council resolution calling on member states to utilise the UN list and/or their own domestic designation lists to guide the online regulation of terrorist content. This could be done in a several ways, including banning official content produced by terrorist groups that makes one guilty of a terrorist offence in member states' jurisdictions, or removing material produced by terrorist entities that incites violence.
- The UN should focus on raising awareness of the UN Sanctions List among various stakeholders, including social media platforms, and the designation process among Member States. It could also encourage more listing proposals and improve the quality of designations.





Further information and comments

Additional information provided by UN Security Council Counter-Terrorism Committee Executive Directorate (CTED) with regards to the designation of the terrorist groups and the freezing of terrorist funds and assets:

1. “Technical guide to the implementation of Security Council resolution 1373 (2001) and other relevant resolutions (2019)” notes that
 - “States should have in place a legal provision that provides for the freezing of terrorist funds and assets pursuant to resolution 1373 (2001) and establish a designating mechanism with adequate due process consideration, as well as a dedicated mechanism to address foreign asset-freezing requests.” (para. 51)
 - States remain sovereign in their determination as to whether to incorporate regional or other national asset-freezing lists domestically, should they meet their own designation criteria, and pursuant to their own legal and regulatory frameworks., (para. 56)
2. There is the International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing Recommendation 6, published by The Financial Action Task Force (FATF) available here.

²⁰ [Technical guide to the implementation of Security Council resolution 1373 \(2001\) and other relevant resolutions](#), United Nations Security Council (UNSC) Counter-Terrorism Committee Executive Directorate (CTED), 2017.

²¹ [International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing Recommendation 6](#), The Financial Action Task Force (FATF).





EUROPEAN UNION

<p>Does the country or institution have their own list of designated, banned, or proscribed groups?</p>	<p>Yes.</p>
<p>What type of system does the country or institution use?</p>	<p>Designation is used, through the linked list.⁷³</p>
<p>What is the definition of “terrorism” the country or institution employs?</p>	<p>The definition of a terrorist offence is provided in Directive 2017/541 on Combating Terrorism.⁷⁴</p> <ul style="list-style-type: none"> • A “terrorist offence” is one of the “intentional acts” listed under Art. 3.1 of the Directive, when conducted in view of terrorist aims (as listed in Art. 3.2) • The EU definition of a terrorist offence is thus an exhaustive list of serious acts that member states are to classify as terrorist in their national law when said acts have “particular terrorist aims” – whether an act is committed or there is a threat to commit it. • “Terrorist aims” are defined as: <ul style="list-style-type: none"> o seriously intimidating a population; o unduly compelling a government or an international organisation to perform or abstain from performing any act; o seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>Proposals (which can be made by Member states or third states) for listing/delisting entities are reviewed by the Working Party on Restrictive Measures to Combat Terrorism (COMET working party),⁷⁵ which makes recommendations to the Council. The working party considers whether the persons, groups or entities in question are involved in terrorist acts as defined above.</p> <p>These recommendations are based on a decision by a judicial or relevant entity concerning an individual or entity convicted for a terrorist act or concerning the initiation of an investigation or prosecution for a terrorist act/ attempt to carry out a terrorist act/ facilitate such act.</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>The EU maintains three designation lists for terrorism:</p> <ul style="list-style-type: none"> • The EU terrorist list,⁷⁶ itself sub-divided into lists of internal and external terrorists, which lists individuals and entities that the Council of EU has designated as terrorists. • Implementation of the UN Security Council Resolutions (1267 Regime) • Autonomous sanctions measures against Islamic State and al-Qaeda.

⁷³ Terrorist Designation List, European Union.

⁷⁴ Directive 2017/541 on Combating Terrorism, European Union, 2017.

⁷⁵ Working Party on restrictive measures to combat terrorism (COMET), European Council and Council of the European Union.

⁷⁶ Terrorist Designation List, European Union.





<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>The EU Directive on Combating Terrorism requires Member States to take the necessary measures to ensure that public provocation to commit a terrorist offence is punishable as a criminal offence when committed internationally.⁷⁷ Member States are to take the necessary measures to prompt removal of online content constituting a public provocation to commit a terrorist offence including by blocking or removing such content (Art. 21).</p> <p>Regulation 2021/784 on addressing the dissemination of terrorist content online (TERREG) defines what constitutes terrorist content in Article 2.⁷⁸</p> <p>Neither the proposed Digital Safety Act (DSA) nor TERREG make explicit reference to designated terrorist groups, and therefore content produced by these groups is not necessarily illegal.</p> <p>EU designation lists are focused on financial sanctions as well as on increased judicial and police cooperation, with no direct implication for terrorist content online. However, as the definition of terrorist content under Article 2 of TERREG includes soliciting “to participate in the activities of a terrorist group”, competent authorities could consider designated terrorist groups to fall under this definition.</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>Yes. According to the Directive, content is to be assessed according to the content itself and the message it transmits, or in relation to a terrorist group as defined in Art. 2.3, not necessarily according to designation lists.</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>This is complex. Terrorist content, as defined by TERREG in article 2, includes content that incites the commission of terrorist offences or that solicits a person to participate in the activities of a terrorist group. General support for designated terrorist groups is therefore not necessarily illegal.</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No. At the time of writing there are 15 persons and 21 groups and entities on the EU terrorist list. Whilst several violent Islamist groups are included in the list, no far-right groups have been included.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>The EU lists are reviewed at least every 6 months. Proposals for delisting can be made by the listed persons or entities, or by the states that had originally proposed the listing. A decision on delisting is made by the Council and published in the official journal with a statement on the reasons. While listed entities and persons can propose their delisting, there does not seem to be an autonomous or rigorous appeals process. However, the inclusion of individuals or entities on EU sanctions lists can be challenged before EU courts (General Court, and on appeal the ECJ), many of these having been successful.⁷⁹</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • There is no direct tie to online regulation, leaving the judgement of removing terrorist content on tech companies. • There are currently no far-right groups designated.

⁷⁷ Directive 2017/541 on Combating Terrorism, European Union, 2017.

⁷⁸ Regulation 2021/784 addressing the dissemination of terrorist content online, European Union, 2021.

⁷⁹ De-listing, European Union Sanctions,





What do we recommend?

- TERREG has made welcome progress on prohibiting terrorist content online. However, we advise TERREG to more clearly define terrorist content to consider the source of the content to ensure that official content from designated terrorist groups can be included. This would tie designation to online regulation and thus provide tech companies with a clear legal and factual basis for removing terrorist content.
- Regulatory bodies at the national level should be advised by the EU to provide more clarity for tech companies on the practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance.
- We recommend prioritising designation as a counter-terrorism strategy and providing the ability to designate a variety of entities, creating a balance between listing Islamist and far-right groups, as well as including other terrorist ideologies.
- We advise working with the UN to provide strategic leadership in setting online speech norms, so that tech companies are informed about what type of material they should consider terrorist and moderate as such.
- The EU should be commended for its relatively transparent and regular review process of designations. However, we suggest designing a flexible and adaptive designation system, in which the list reflects the changing terrorist threat landscape and makes it easy to delist groups when relevant. This proposed system should involve civil society, counterterrorism specialists, member states, and human rights lawyers in designation process.
- We strongly recommend that the EU designate more far-right groups.
- We advise the EU to consider designating lone actors and criminalising content they produce (especially manifestos and livestreams).
- We recommend that the EU consider other types of terrorist ideologies beyond far-right, far-left, separatist, and Islamist actors, such as incel attackers who have been deemed terrorists by certain governments.
- We advise keeping records so that the designation of a group, actor, or content occurs transparently and to implement a system whereby such records can be made available for judicial oversight.

Further information and comments

A definition of what constitutes a “Terrorist group” is provided in Directive 2017/541 on Combating Terrorism (Art. 2.3): “a structured group of more than two persons, established for a period of time and acting in concert to commit terrorist offences; ‘structured group’ means a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.”⁸⁰

⁸⁰ Directive 2017/541 on Combating Terrorism, European Union, 2017.





UNITED STATES

Does the country or institution have their own list of designated, banned, or proscribed groups?

Yes

What type of system does the country or institution use?

The United States has two primary counterterrorism sanction authorities:

Foreign Terrorist Organizations (FTOs): Section 219 of the Immigration and Nationality Act (INA)¹ authorizes the Secretary of State to designate certain groups that meet the statutory criteria as FTOs.² The consequences of an FTO designation include: all funds of the organization under the control of U.S. institutions may be frozen; aliens who are members or representatives of, provide material support to, solicit funds for, or recruit members for the FTO are ineligible for U.S. visas and other immigration-related benefits; and it is illegal for persons subject to the jurisdiction of the United States as defined in the statute to knowingly provide material support or resources to an FTO, and those who provide such support may be subject to significant civil and criminal penalties, including fine or a term of imprisonment.

Specially Designated Global Terrorists (SDGTs)³: Executive Order (E.O.) 13224⁴, issued pursuant to the International Emergency Economic Powers Act (IEEPA) and other authorities, authorizes the Secretaries of State and the Treasury to designate terrorist actors, terrorist supporters, leaders of terrorist organizations, and those who participate in training to commit acts of terrorism as SDGTs. This results in the blocking of any property, or interests in property, of these persons that are located in the United States or that are controlled by U.S. persons (including legal persons) anywhere in the world. It also prevents U.S. persons or persons located in the United States from having any dealings with the property or property interests of designated persons.

All designated FTOs and SDGTs are added to the U.S. Department of the Treasury – Office of Foreign Asset Control (OFAC)’s Specially Designated Nationals And Blocked Persons List (SDN).⁵

¹ Immigration and Nationality Act (1997)

² Foreign Terrorist Organizations, U.S. Department of State

³ [Specially Designated Nationals And Blocked Persons List \(SDN\)](#), US Department of Treasury.

⁴ [Executive Order 13224](#), US Department of the Treasury

⁵ Specially Designated Nationals And Blocked Persons List (SDN), U.S. Department of the Treasury.





What is the definition of “terrorism” the country or institution employs?

The United States has several definitions of terrorism for specific and generally limited purposes:

For purposes of Chapter 113B (Terrorism) in Title 18 of the U.S. Code:

International terrorism is defined as “activities that— (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended— (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum.”⁶

Domestic terrorism is defined as “activities that— (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.”⁷

For purposes of designating a group as an FTO under INA Section 219, a foreign organization must engage in either “terrorism” or “terrorist activity” as defined in the statute or retain the capability and intent to do so:

Terrorism is defined as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.”⁸

Terrorist activities is defined as “any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following: (I) The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle). (II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained. (III) A violent attack upon an internationally protected person (as defined in section 1116(b)(4) of title 18) or upon the liberty of such a person. (IV) An assassination. (V) The use of any— (a) biological agent, chemical agent, or nuclear weapon or device, or (b) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property. (VI) A threat, attempt, or conspiracy to do any of the foregoing.”⁹

⁶ 18 U.S.C. §2331(1)

⁷ 18 U.S.C. §2331(5)

⁸ 22 U.S.C. §2656f(d)(2)

⁹ 18 U.S.C. §1182(a)(3)(B)(iii)





Engaged in terrorist activities is defined as “in an individual capacity or as a member of an organization— (I) to commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity; (II) to prepare or plan a terrorist activity; (III) to gather information on potential targets for terrorist activity; (IV) to solicit funds or other things of value for— (aa) a terrorist activity; (bb) a terrorist organization described in clause (vi)(I) or (vi)(II); or (cc) a terrorist organization described in clause (vi)(III), unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization; (V) to solicit any individual— (aa) to engage in conduct otherwise described in this subsection; (bb) for membership in a terrorist organization described in clause (vi)(I) or (vi)(II); or (cc) for membership in a terrorist organization described in clause (vi)(III) unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization; or (VI) to commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training— (aa) for the commission of a terrorist activity; (bb) to any individual who the actor knows, or reasonably should know, has committed or plans to commit a terrorist activity; (cc) to a terrorist organization described in subclause (I) or (II) of clause (vi) or to any member of such an organization; or (dd) to a terrorist organization described in clause (vi)(III), or to any member of such an organization, unless the actor can demonstrate by clear and convincing evidence that the actor did not know, and should not reasonably have known, that the organization was a terrorist organization.”¹⁰

For purposes of designating an individual or entity (defined in the E.O. to mean partnerships, associations, corporations, or other organizations, groups, or subgroups) as an SDGT under E.O. 13224:

- Terrorism is defined as “activity that— (i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended— (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.”¹¹

How does the designation process relate to the relevant authority’s definition of terrorism?

Yes, both the INA and E.O. 13224 (including its implementing regulations) set forth legal criteria that must be satisfied before the United States may make a designation, including what activity constitutes terrorism or terrorist activity.

Domestic terrorist organisations – in this case meaning organisations based in the US which engage in the activities above defined as terrorist – cannot be designated under the international terrorism or terrorist activity definitions.

Domestic terrorist groups could in theory be designated based on the domestic terrorism definition, however there is at the time of writing no legal framework to facilitate this.¹² More on this below.

¹⁰ 18 U.S.C. §1182(a)(3)(B)(iv)

¹¹ E.O. 13224, Section 3(d)

¹² Blazakis, Jason. , USA Today (2021). Lack of a domestic terrorism law creates an imbalance, USA Today (2021) ; Blazakis, Jason. [It’s a real possibility that our next 9/11 could arrive within](#), The Washington Post (2021).





<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Yes, the United States implements its UN obligations relating to sanctions through a variety of U.S. executive orders including E.O. 13224.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>Online content that constitutes material support to an FTO is criminal and is not protected by the First Amendment. A U.S. Supreme Court case ruled that, as applied, the material support statute did not violate the freedom of speech guaranteed by the First Amendment.¹³ Material support is defined in U.S. law as any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials. Depending on the facts, online content could potentially implicate other U.S. laws.</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>Other forms of expression not protected by the First Amendment include true threats, incitement to imminent unlawful action, and speech integral to criminal conduct, like solicitation and conspiracy.</p> <p>“True threats” are defined in <i>Virginia vs Black</i> (2003)¹⁴ as “those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals. The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats protect(s) individuals from the fear of violence and from the disruption that fear engenders, in addition to protecting people from the possibility that the threatened violence will occur.”¹⁵ This may include online content.</p> <p>Incitement to imminent lawless action was defined in <i>Brandenburg vs Ohio</i> (1969)¹⁶ which said that “the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.” Critics have argued that due to online content often being broad and unspecific on timeframes, this makes it difficult to ever determine that online speech is unlawful under this exemption. Critics have therefore argued that the imminent clause should be removed when it comes to criminalising online content.</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>Sometimes. Knowingly providing material support, as defined by U.S. law, to a designated FTO violates U.S. law. Other online content that could be illegal includes content that constitutes a “true threat,” imminent incitement to violence, or child sexual abuse.</p>

¹³ 08-1498 *Holder v. Humanitarian Law Project* (06/21/2010); *Terrorism, Violent Extremism, and the Internet: Free Speech Considerations*, Congressional Research Service (2019).

¹⁴ *Virginia vs. Black* (2003), Supreme Court Resources.

¹⁵ *True Threats*, Freedom Forum Institute, First Amendment Center (2008).

¹⁶ *Brandenburg vs Ohio*, 1969, Supreme Court Resources.





Is there a sufficient balance between far-right and violent Islamist groups and individuals?

The United States has designated one domestic racially or ethnically motivated violent extremist group, which has ties to foreign violent extremists. In 2020, the United States designated the Russian Imperial Movement (RIM) along with several of its leaders as SDGTs under E.O. 13224. Since then, the United States has designated two additional RIM supporters as SDGTs. The United States also designated Anton Thulin as an SDGT. Thulin, who previously received paramilitary training from RIM, was convicted in connection with the detection of a powerful homemade bomb near a Swedish refugee residential center and continued to seek similar training after his release from prison.

Current U.S. law does not allow for the U.S. government to designate purely domestic terrorist organizations. There are no U.S.-based far-right groups currently designated as FTOs or SDGTs.¹⁷

However, some U.S. entities have been designated as SDGTs in cases where they have provided support to groups designated as SDGTs. One noteworthy case where this occurred was when a U.S.-based charity was designated as an SDGT for providing financial and material support to Hamas, which is designated as both an SDGT and an FTO.¹⁸ Individuals can also be designated as SDGTs based on specific types of activities associated to designated SDGTs. This also applies to U.S. citizens. A notable case is Anwar al-Awlaki who was a dual national (Yemeni and U.S.), who was designated as an SDGT for supporting acts of terrorism and for acting for or on behalf of al-Qaeda in the Arabian Peninsula (AQAP), which is designated as both an SDGT and an FTO.

Are there human rights-compliant mechanisms in place for delisting a group?

A designated FTO may file a petition for revocation two years after its designation date or two years after the determination date on its most recent petition for revocation. The Secretary of State may also at any time revoke a designation, and shall revoke upon a finding that the circumstances forming the basis for the designation have changed in such a manner as to warrant revocation, or that the national security of the United States warrants a revocation. A designation may also be revoked by an Act of Congress or set aside by a Court order. Furthermore by law, an organization designated as an FTO may seek judicial review of the designation in the U.S. Court of Appeals for the District of Columbia Circuit not later than 30 days after the designation is published in the Federal Register.

SDGTs may also seek administrative reconsideration of their designation or petition for removal from the SDN List, including based on arguments that there is an insufficient basis for the listing or that the circumstances resulting in the designation no longer apply.¹⁹ An SDGT de-listing request must be made by the blocked person and addressed to OFAC. Upon the U.S. government making a final determination to delist, the U.S. government then takes appropriate administrative actions, including removing the person as an SDGT from the SDN List on the OFAC website, and, if appropriate, working with the UN to remove the person from the UN's Consolidated Sanctions List. Although there is an administrative procedure for seeking de-listing, there is always the possibility to challenge SDGT designations and other OFAC decisions in court.

For individuals, human rights lawyers have criticised the fact that individuals need to be present in the US in order to appeal the designation, meaning that is very difficult for the majority of SDNs to contest their designation.²⁰

¹⁷ Blazakis, Jason, Lack of a domestic terrorism law creates an imbalance, USA Today (2021).

¹⁸ Holy Land Foundation case, United States District Court.

¹⁹ 31 CFR 594.201, note 3, and 31 CFR 501.807

²⁰ Sullivan, G. (2020). The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law. (Global Law Series). Cambridge: Cambridge University Press. doi:10.1017/9781108649322.





<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • There is no legislation in place to designate purely domestic terrorist groups undermining efforts to counter the far-right, domestic threat. • Some online content produced by a terrorist group, or in support of a terrorist group, may not be considered material support under U.S. law, when balanced against the First Amendment. • Some tech companies have stated that it is difficult to apply the standards of true threats and incitement to imminent violence, such as the level of imminence necessary, to apply to online content. This is particularly the case for smaller tech companies. • Designated individuals and human rights critics also complain that deadlines for appealing a designation decision is very short and de facto may hinder effective appeals.²¹ • Some of the group names on the FTO and SDGT lists are out of date. Up-to-date terminology is essential to effectively moderate terrorist content produced by these groups in order for tech companies attempting to moderate content produced by groups on U.S. terrorist designation lists.
<p>What do we recommend?</p>	<ul style="list-style-type: none"> • The United States could consider enacting legislation that provides the ability to designate domestic terrorist groups and individuals. In our view, enabling the designation of domestic terrorist groups constitutes a mechanism which could help the United States counter its rising violent extremist threat. • Domestic terrorist organisations should be addressed with a comparable seriousness of approach, consistent with U.S. law, as given to international terrorism and as equally severe in order to counter both types of organizations effectively. • The United States should consider putting in place increased human rights safeguards as part of its FTO designation processes, including lengthening the appeal time for groups. • The United States' counterterrorism efforts, particularly online, would be more effective if they were to respond to the changing landscape of terrorist groups and be swifter in responding to terrorist groups' name changes and dissolution. • We recommend the US government to designate individuals that are not directly associated to a designated terrorist group but that are known terrorist offenders. This can help counter the threat and influence of lone-actor terrorists.
<p>Further information and comments</p>	

²¹ Ibid.





UNITED KINGDOM

<p>Does the country or institution have their own list of designated, banned, or proscribed groups?</p>	<p>Yes</p>
<p>What type of system does the country or institution use?</p>	<p>The UK uses proscription. Groups can be added to the proscribed terrorist groups or organisations list by the Secretary of State if they believe that the group is “concerned in terrorism” and that proscription is a proportionate action to take. This decision is then debated and voted on in the UK Parliament.⁴⁰ The proscription comes into force if Parliament approves the proscription order.</p>
<p>What is the definition of “terrorism” the country or institution employs?</p>	<p>“Terrorism”, as defined in section 1 of the Terrorism Act (TACT) 2000, means the use or threat of action which:</p> <ul style="list-style-type: none"> ● involves serious violence against a person; ● involves serious damage to property; ● endangers a person’s life (other than that of the person committing the act); ● creates a serious risk to the health or safety of the public or section of the public; or ● is designed seriously to interfere with or seriously to disrupt an electronic system. <p>The use or threat of such action must be designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public and be made for the purpose of advancing a political, religious, racial, or ideological cause.⁴¹</p>
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>Groups may only be designated if the Secretary of State believes the group:</p> <ul style="list-style-type: none"> ● commits or participates in acts of terrorism; ● is preparing to commit or participate in terrorism; ● promotes or encourages terrorism (including the unlawful glorification of terrorism); or ● is otherwise concerned in terrorism. <p>This is based on the definition of terrorism provided within TACT 2000.⁴²</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Terrorist groups and individuals are designated under financial sanctions in the UK under UN and UK sanction regimes.⁴³</p>

⁴⁰ Proscribed terrorist groups or organisations, United Kingdom Government Home Office.

⁴¹ Terrorism Act, United Kingdom Government, 2000.

⁴² Terrorism Act, United Kingdom Government, 2000.

⁴³ Financial sanctions targets: list of all asset freeze targets, HM Treasury.





<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>The current Interim Code of Practice on Terrorist Content and Activity Online states that any material created by a proscribed terrorist group, any dissemination of terrorist materials, or any material which meets the definition of an “act of terrorism” or “encouragement of terrorism”, should be removed.⁴⁴ However, this Code is voluntary and not legally binding.</p> <p>Unlawful terrorism-related content is determined by whether the content of the material could potentially give rise to any criminal liability if it were ever hosted, published or distributed by a person who could be apprehended and prosecuted in the UK, subject to the context in which it appears.</p> <p>The draft Online Safety Bill will consider both terrorist content from proscribed entities and content which meets the threshold of encouraging or glorifying terrorism.⁴⁵</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>The UK has a number of criminal offences that may be made out, depending on the specific circumstances of the case, including (but not limited to):</p> <ul style="list-style-type: none"> • Sections 1 and 2 of TACT 2006 criminalise public statements that encourage terrorism and the dissemination of terrorist publications, respectively. • Sections 59 to 61 of TACT 2000 make it an offence to incite another person to commit an act of terrorism wholly or partly outside the United Kingdom where that act would, if committed in the UK, constitute one of a number of specified offences. • Section 58 of TACT 2000 makes it an offence to collect, possess or view online, a record of information likely to be useful to a person committing or preparing an act of terrorism. • It is also possible that encouraging someone to carry out a terrorism offence could constitute an offence under the Serious Crime Act 2007.
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>The UK has a number of criminal offences that may be made out, depending on the specific circumstances of the case, including (but not limited to):</p> <ul style="list-style-type: none"> • Section 12 of TACT 2000 makes inviting support for a proscribed organisation illegal. • Section 13 of TACT 2000 makes it illegal to publish an image of an item of clothing or other article (such as a flag) of a proscribed group online in circumstances arousing reasonable suspicion that a person is a supporter of the proscribed group.
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>While the UK has proscribed a number of far-right terrorist groups in recent years, its list of proscribed terrorist organisations is currently outweighed by a far greater number of Islamist terrorist groups.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>Proscribed organisations can apply to the UK government to be deproscribed. Deproscription applications are considered by the Secretary of State. If the application is refused, the applicant may appeal to the Proscribed Organisations Appeal Commission (POAC). The Commission will allow an appeal if it considers that the decision to refuse deproscription was flawed, applying judicial review principles. Either party can seek leave to appeal the POAC’s decision at the Court of Appeal.⁴⁶</p>

⁴⁴ Interim code of practice on terrorist content and activity online (accessible version), United Kingdom Government Department for Digital, Culture, Media & Sport, 2020.

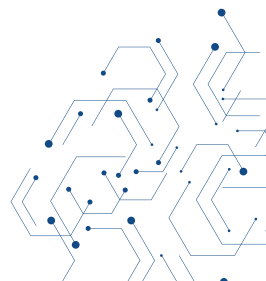
⁴⁵ [Draft Online Safety Bill](#), United Kingdom Government Department for Digital, Culture, Media & Sport, 2021.

⁴⁶ The Proscribed Organisations Appeal Commission (Human Rights Act 1998 Proceedings) Rules, United Kingdom Government, 2006.





<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • The current delisting process does not have a regular, transparent review procedure undertaken by an independent reviewer. While other deproscription processes in the UK meet a thorough human rights standard, this absence highlights a defect in the UK's overall process. • Very few violent far-right extremist groups have been proscribed relative to Islamist terrorist groups. Content from far-right violent extremist groups is, in practice, in a grey area that tech companies themselves must decide whether to regulate.
<p>What do we recommend?</p>	<ul style="list-style-type: none"> • We advise the UK to proscribe more far-right violent extremist groups and their affiliates, in line with ongoing and emerging threats. • The UK could consider expanding their current proscription regime to similarly proscribe individual actors, in line with other nations such as Canada and New Zealand. This would assist in online content moderation of proscribed terrorist material. • We recommend that the UK better synthesise the financial sanctions list and the proscription list to ensure that all proscribed organisations are subject to the same sanctions. • We advise the UK to establish a transparent, regular review process of the proscription list by an independent reviewer to ensure that the process upholds human rights and sufficient safeguards. • We recommend the UK ensures the Online Safety Bill places the responsibility of creating and disseminating terrorist content on the content producers rather than on tech platforms.
<p>Further information and comments</p>	<p>The UK plays a leading role in the proscription of terrorist entities, and its proscription activity within recent years has resulted in the proscription of several extreme right-wing terrorist groups. The UK proscription process has been shown to be a particularly influential model to other democratic nations.</p>





CANADA

Does the country or institution have their own list of designated, banned, or proscribed groups?	Yes
What type of system does the country or institution use?	Canada uses designation for all terrorist entities, both groups and individuals. There are no proscriptions, banning, or financial sanctions lists. Individuals and groups are both listed as “Designated Entities.” ⁴⁷
What is the definition of “terrorism” the country or institution employs?	A terrorist act is one committed “in whole or in part for a political, religious or ideological purpose, objective or cause” with the intention of intimidating the public “with regard to its safety, including its economic security, or compelling a person, a government or a domestic or international organisation to do or refrain from doing any act.” ⁴⁸
How does the designation process relate to the relevant authority’s definition of terrorism?	<p>The Canadian Anti-Terrorism Act (ATA) allows for the Government of Canada to create a list of “entities” that:</p> <ul style="list-style-type: none"> • Have knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity. • Knowingly acted on behalf of, at the direction of or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated terrorist activity.⁴⁹ <p>Designation is, therefore, based on the established definition of terrorism.</p>
Does the country follow UN or EU (if relevant) designation lists and sanctions?	On top of the Designated Entities list, Canada also follows the UN Resolutions on the suppression of terrorism, and the Resolutions on the Taliban, ISIL (Da’esh), and al-Qaeda.
Does designation have an effect on the online realm? Is content created by terrorist groups illegal?	Yes, a listing provides a clear indicator for service providers to remove an entity’s online presence on social media and other associated online platforms.
Is online content that incites acts of terrorism illegal?	Yes
Is online content that supports designated terrorist groups illegal?	Yes
Is there a sufficient balance between far-right and violent Islamist groups and individuals?	Yes, Canada has made a recent effort to designate a fuller range of domestic and international ideologically motivated groups and individuals.

⁴⁷ [Listed Terrorist Entities](#), Public Safety Canada

⁴⁸ Definitions of Terrorism and the Canadian Context, Government of Canada.

⁴⁹ [Anti-terrorism Act](#), Government of Canada, 2003.





<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>Within 60 days of being listed, an applicant may apply for judicial review of the decision. There is a rolling review of all entities on the designation list carried out at a maximum of every five years.⁵⁰ If a group is disbanded or wholly inactive, it is possible that they will be removed from the designation list through this review process.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • There is no formal protocol outside of rolling review for delisting a disbanded or inactive group. • The Government of Canada has stated that “terrorist propaganda” includes any content produced by designated entities. However, the phrasing of this legislation is unclear and could be refined for clarity. • There is no apparent or accessible appeal process for removal from the designation list after 60 days of listing. There is also no formal mechanism for safeguarding human rights in the designation process.
<p>What do we recommend?</p>	<ul style="list-style-type: none"> • We recommend that Canada designate ideological counterparts of existing designated entities (such as Sonnenkrieg Division and Feuerkrieg Division). • We advise Canada to provide a clearer definition of what constitutes “terrorist propaganda” in relation to designated entities, to ensure that tech platforms understand what content is within the remit of the current legislation. • While acknowledging the Government of Canada’s commitment to introducing new legislation that establishes regulations for harmful content online, we recommend Canada ensures that small tech platforms are not overly targeted by terrorist users due to the platform’s struggle to moderate content. If the regulation is not reviewed, the platforms will likely receive an influx of terrorist activity which they are unable to moderate, resulting in heavy fines; it would be beneficial for these platforms to receive extra support. • We recommend that Canada consider designating entities which pose a gender-based violent extremist threat, such as Alek Minassian, in the same way James Mason has been designated. As this is a prominent threat both in Canada and the neighbouring US, it is highly likely that this threat will continue to grow if no effective action is taken.
<p>Further information and comments</p>	<p>Terrorist propaganda is not ‘banned’ under any specific law. No individual pieces of literature or media are banned. However, if it fits the definition of “terrorist propaganda” it can be confiscated and destroyed by law enforcement - this is applicable to both offline and online material.</p>

⁵⁰ List of Entities, Government of Canada.





AUSTRALIA	
Does the country or institution have their own list of designated, banned, or proscribed groups?	Yes
What type of system does the country or institution use?	<p>Executive Proscription:</p> <ul style="list-style-type: none"> The government can list an entity as a terrorist organisation ⁵¹ if the Minister for Home Affairs is satisfied that the organisation is: “engaged in preparing, planning, assisting or fostering a terrorist act; or advocating the doing of a terrorist act.” ⁵² <p>Financial sanctions:</p> <ul style="list-style-type: none"> This comes in the form of the Department for Foreign Affairs and Trade Consolidated List ⁵³ of persons and entities who are subject to targeted financial sanctions. Designating a group in this way is a milder measure than executive proscription as there is no specific offence committed by being a member or associate of these entities and individuals. However, it does become a criminal offence to “use or deal with the assets of listed persons or entities, or to make assets available to them.” <p>Judicial approach:</p> <ul style="list-style-type: none"> In the Australian judicial process, a court can find an individual or organisation, guilty of “directly or indirectly engaging in preparing, planning, assisting or fostering the doing of a terrorist act.” In this process, the prosecution must first prove that the individual or organisation in question is terrorist in nature. The judicial approach does not allow for the group to be deemed a terrorist organisation solely for advocating terrorism; instead there must be some form of direct or indirect engagement. This approach also does not criminalise association with the group in question.
What is the definition of “terrorism” the country or institution employs?	<p>A Terrorist Act ⁵⁴ is defined as an action that:</p> <ul style="list-style-type: none"> Causes serious physical harm to a person; causes serious damage to property; causes a person’s death; endangers a person’s life, other than the life of the person taking the action; creates a serious risk to the health or safety of the public or a section of the public; seriously interferes with, seriously disrupts, or destroys, an electronic system. The action is committed or the threat is made with the intention of advancing a political, religious, or ideological cause. The action is also committed, or the threat is made with the intention of coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or intimidating the public or a section of the public. This offence applies whether or not the alleged offence occurs in Australia, or whether or not the result of the alleged offence occurs in Australia.

⁵¹ [Listed Terrorist Organisations](#), Government of Australia.

⁵² [Protocol for listing terrorist organisations](#), Government of Australia, 2021.

⁵³ [Department for Foreign Affairs and Trade Consolidated List](#), Government of Australia, 2021.

⁵⁴ [Criminal Code Act](#), Government of Australia, 1995.





<p>How does the designation process relate to the relevant authority's definition of terrorism?</p>	<p>The inclusion of entities on the Executive Proscription list ⁵⁵ is dependent on the established definition of terrorism. The Judicial Approach also relies on the established definition of terrorism. However, Financial Sanctions ⁵⁶ do not require an entity to meet the definition of terrorism as the list is heavily influenced by the UN sanctions list.</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>The Executive Proscription and Financial Sanctions lists appears to be heavily influenced by the UN sanctions list.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>The relationship is complex: if the content can adequately be described as "abhorrently violent," then it can be removed regardless of whether the entity creating/publishing the content is a proscribed entity. Content that does not meet this threshold, but is created/published by a proscribed entity may remain online.</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>The illegality of the content depends on whether it meets the threshold of "abhorrently violent".</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>No, unless it also meets the threshold of "abhorrently violent".</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No, both the Executive Proscription list and the Financial Sanctions list are dominated by Islamic terrorist entities. At the time of writing there are 29 listed terrorist organisations on the Executives Proscription List, 3 of which are far-right groups.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>There is a 3-year rolling review process which may remove an entity from the executive proscription list.⁵⁷ Any person or entity can make a de-listing application.⁵⁸ This application must be made to the Minister for Home Affairs, who must consider the application if the person or entity claims that there is no lawful basis for proscription. However, there is limited transparency around how a person or entity might make an appeal.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> ● Current legislation appears to allow non-violent content posted by proscribed terrorist groups to remain online, and does not acknowledge the use of non-violent material within terrorist recruitment. ● There is no clear review available for a proscribed group which disbands. ● The number of far-right groups proscribed is limited relative to the threat. At present, content from far-right violent extremists is in a grey area in which tech companies themselves must decide whether they should remove it. ● Current legislation places the responsibility for terrorist content on tech platforms, rather than on the creators of the content.

⁵⁵ [Executive Proscription List](#), Government of Australia.

⁵⁶ [Consolidated List](#), Government of Australia Department of Foreign Affairs and Trade.

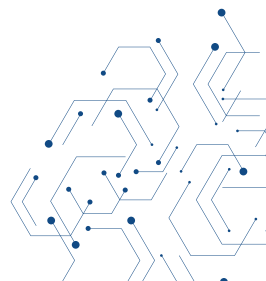
⁵⁷ [Protocol for listing terrorist organisations](#), Government of Australia, 2021.

⁵⁸ [Protocol for listing terrorist organisations](#), Government of Australia, 2021.





<p>What do we recommend?</p>	<ul style="list-style-type: none"> • We recommend that Australia make a significant effort to place more far-right violent extremist groups onto the executive proscription list, especially those that pose a direct threat within the country, such as Combat 18. • We advise that this list also consider ideological counterparts to currently proscribed groups such as Atomwaffen Division as an affiliate of Sonnenkrieg Division. • We recommend Australia amend current legislation (chiefly the Criminal Code) to better bridge the gap between counterterrorism legislation and the executive proscription list, as it is currently unclear how the proscription list should be employed. • We advise Australia to refine the current definition of a “document” in regard to terrorist content to make the legislation clearer for third-parties who wish to remove terrorist content from their websites. • The current legislation can require entire websites to be taken down by ISPs, rather than singular posts. This is likely to result in limiting free speech and is highly likely to receive backlash from the public. We recommend that this legislation is rewritten to consider the abilities of tech platforms and ISPs while ensuring that free speech and other human rights are upheld.
<p>Further information and comments</p>	





NEW ZEALAND

<p>Does the country or institution have their own list of designated, banned, or proscribed groups?</p>	<p>Yes</p>
<p>What type of system does the country or institution use?</p>	<p>Designation is the only form used, proscription and banning are not used.</p>
<p>What is the definition of “terrorism” the country or institution employs?</p>	<p>Terrorism Suppression Act (TSA) Section 5 (2):⁵⁹ An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3)⁶⁰, and is carried out for 1 or more purposes that are or include advancing an ideological, political, or religious cause, and with the following intention: (a) to intimidate a population; or (b) to coerce or to force a government or an international organisation to do or abstain from doing any act.</p>
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>An entity may be designated by the Prime Minister if they believe there are reasonable grounds the entity has engaged in a terrorist act, based on the established definition of a terrorist act. When the ‘Terrorist Designations Working Group’ are considering an entity for designation, they should consider whether the threat is consistent with that outlined in section 5 of the TSA and the nature and scale of the entity’s involvement in terrorist acts or supportive activity. Before designating an entity as a terrorist or associated entity, the Prime Minister consults the Attorney-General on whether the legislative requirements in the TSA are satisfied.</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Yes, the UN lists and sanctions are followed.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>No. Content which is considered “objectionable” according to the Films, Videos, and Publications Classification Act 1993 is illegal to make, copy, import, supply, possess or sell under New Zealand law.⁶¹ A sub-clause (Section 3(3) (d)) in the definition of “objectionable” includes the “extent and degree” to which it is determined that the content “promotes or encourages criminal acts or acts of terrorism,” but this is not dependent on terrorist designation. An independent Crown entity (the Classification Office) and Board of Review have the authority to determine whether content is objectionable.</p>

⁵⁹ [Terrorism Suppression Act \(TSA\) Section 5 \(2\)](#), Government of New Zealand, 2002.

⁶⁰ Outcomes specified in Section 3 are “(a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act); (b) a serious risk to the health or safety of a population; (c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d); (d) serious interference with, or serious disruption to, critical infrastructure, if likely to endanger human life; (e) introduction or release of a disease-bearing organism, if likely to cause major damage to the national economy of a country.” Government of New Zealand, [Terrorism Suppression Act \(TSA\) Section 5 \(2\)](#), 2002.

⁶¹ Films, Videos, and Publications Classification Act, Government of New Zealand Department of Internal Affairs, 1993.





<p>Is online content that incites acts of terrorism illegal?</p>	<p>Yes, according to the Films, Videos, and Publications Classification Act 1993 section 3, any content which “promotes or encourages criminal acts or acts of terrorism” may be determined objectionable, and therefore illegal to make, copy, import, supply, possess or sell.⁶²</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>No, unless it meets the definition of “encouraging acts of terrorism.” This means other official content produced by designated terrorist groups is legal.</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No, New Zealand has only designated three far-right entities. These include the Christchurch attack perpetrator, and more recently, in June 2022, The Base and the Proud Boys were also designated.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>There is a regular 3-year rolling review process to which every listed entity is subject, allowing for removal from the designation list if they no longer pose a threat to New Zealand or meet the established definition of a terrorist group. A designated entity can apply in writing to the Prime Minister for the designation to be revoked on the grounds that the entity does not satisfy the section 22 TSA test or that the entity is no longer involved in any way in acts of the kind that made it eligible for designation. Judicial review proceedings are also possible in respect of a designation under the TSA.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • New Zealand has designated three far-right entities (the Christchurch perpetrator, The Base and the Proud Boys) but no others. This does not accurately reflect the current threat landscape and the threat posed by the violent far-right. Experts have warned this is because the TSA fails to mention the extreme far-right, making designations of those entities difficult.⁶³ • The criteria used to designate terrorist entities specifies consideration of the threat posed to New Zealand and the extent and nature of the entity’s presence in New Zealand.⁶⁴ While this criteria does not necessarily have to be met, there is a danger this encourages reactive designation of entities having already committed attacks against New Zealanders (such as the designation of Brenton Tarrant). Additionally, this may limit the territorial scope of designation which may overlook threats from abroad. • Given online regulation currently covers “objectionable” rather than purely terrorist content while overlooking the source, there is a disconnect between designation and the regulation of TVE content online.

⁶² Films, Videos, and Publications Classification Act, Government of New Zealand Department of Internal Affairs, 1993, section 3.

⁶³ [New Zealand Terror List Needs to be Expanded](#), Katie Scotcher, Radio New-Zealand, 2021.

⁶⁴ [Terrorist Designation Process Legal framework](#), New Zealand Police, 2017.





What do we recommend?

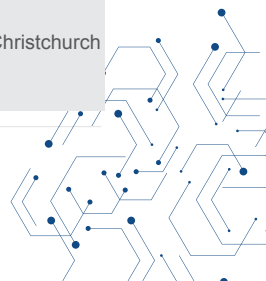
- We recommend reconsidering the criteria used for designation of terrorist entities to incorporate a broader range of ideologies and threats. This should include greater consideration of the threat of online radicalisation from external terrorist entities, as Australia have done in their designation of UK-based Sonnenkrieg Division.⁶⁵
- We recognise that the recent designations of The Base and the Proud Boys⁶⁶ constitute positive progress in this regard, and commend New Zealand for their transparent reasoning for these additions. However, we believe there is no reason not to consider designating other internationally recognised groups such as Atomwaffen Division or National Socialist Order, especially given groups such as the IRA and ETA are on the list.
- We suggest this may also involve updating the definition of terrorism to reflect the threat of the extreme far-right, which is in line with the Royal Commission into the Christchurch Mosque attack's recommendations.⁶⁷
- We also recommend that New Zealand consider other types of terrorist ideologies beyond far-right, far-left, separatist, and Islamist actors, such as 'incel' attackers who have been deemed terrorist in nature by certain governments.
- New Zealand should also recognise that grouping unsavoury material with TVE content under the Films, Videos and Publications Classification Amendment Bill could limit freedom of speech and remit the adjudication of "objectionable content" to the discretion an individual (the Chief Censor or Inspector of Publications).⁶⁸ In this regard, transparency and consultation for these decisions is vital.
- Additionally, we propose developing an explicit definition of online terrorist content as part of online regulation legislation, which would mandate consideration of the source of the content to ensure official content from designated terrorist groups can be included. This would tie designation to online regulation and thus provide tech companies with a clear legal and factual basis for removing terrorist content.

⁶⁵ [Designation of Sonnenkrieg Division](#), Government of Australia, 2021.

⁶⁶ [Designation of Proud Boys](#), New Zealand Police, 2022.

⁶⁷ [Recommendations to improve New Zealand's counter terrorism effort](#), Royal Commission of Inquiry into the terrorist attack on Christchurch mosques, 15 March 2019.

⁶⁸ Films, Videos, and Publications Classification Act, Government of New Zealand Department of Internal Affairs, 1993.





	<ul style="list-style-type: none"> • We believe that as the founding member of the Christchurch Call to Action,⁶⁹ New Zealand is certainly capable of effectively tackling terrorist and violent extremist content online. We commend New Zealand’s Classification Office in leading on banning certain terrorist content by means of thorough and transparent consultation processes, as happened in the case of the Christchurch livestream and manifesto, the Halle attack video,⁷⁰ and most recently the ‘Oslo’ manifesto.⁷¹ This criminalises possessing, distributing, viewing, and hosting this material and provides tech companies with the legal basis to remove it. We do however believe these classifications should be criminalised under ‘terrorist content’ rather than ‘objectionable content’, and that the scope of ‘terrorist content’ should consider official material produced by designated terrorist organisations. This is to provide additional clarity for tech companies.⁷² This criminalises possessing, distributing, viewing, and hosting this material and provides tech companies with the legal basis to remove it. We do however believe these classifications should be criminalised under ‘terrorist content’ rather than objectionable content’, and that the scope of ‘terrorist content’ should consider official material produced by designated terrorist organisations. This is to provide additional clarity for tech companies. • Alongside online regulation, the establishment of a regulatory body should be considered to provide more clarity for tech companies on the practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance.
<p>Further information and comments</p>	<p>New Zealand should be commended for its transparent designation process, managed by the Terrorist Designations Working Group. In particular, we applaud the legal criteria on which designations are based and the direct connection to the terrorism definition laid out in the TSA.</p>

⁶⁹ Christchurch Call to Action, Government of New Zealand, 2019.

⁷⁰ [Chief Censor bans livestream of antisemitic shooting in Halle](#), Thomas Manch, Stuff, 2019.

⁷¹ [White supremacist manifesto banned](#), New Zealand Classification Office, 2021.

⁷² [White supremacist manifesto banned](#), New Zealand Classification Office, 2021.





FRANCE

Does the country or institution have their own list of designated, banned, or proscribed groups?	No
What type of system does the country or institution use?	<p>France's counterterrorism legislation is based on the sanctioning of terrorist undertaking – individuals can be convicted of acts of terrorism, but there is no list of terrorist entities.</p> <p>France also has a process to order the dissolution of a group or organisation that represents a significant security threat.⁸¹</p> <p>France also has a Financial Sanctions list.⁸²</p>
What is the definition of “terrorism” the country or institution employs?	Acts related to “an individual or collective undertaking aimed at seriously disturbing the public order by intimidation or terror” ⁸³
How does the designation process relate to the relevant authority’s definition of terrorism?	As there is no designation list, terrorism convictions are assessed on a case-by-case basis.
Does the country follow UN or EU (if relevant) designation lists and sanctions?	Both the UN and EU lists are included within the Financial Sanctions list.
Does designation have an effect on the online realm? Is content created by terrorist groups illegal?	As there is no designation process, there is no impact on online content. There is also no legal provision governing the production or sharing of content produced by a group dissolved for incitement to terrorism.
Is online content that incites acts of terrorism illegal?	Yes, under the heading of glorifying terrorism. ⁸⁴
Is online content that supports designated terrorist groups illegal?	No, illegality is conditional on the content itself, rather than on its source.
Is there a sufficient balance between far-right and violent Islamist groups and individuals?	As there is no formal designation list (or in this case, a consolidated dissolution list), it is unknown what the balance is between far-right and Islamic terrorism.
Are there human rights-compliant mechanisms in place for delisting a group?	As there is no designation list, there is also no mechanism for delisting. If an individual is convicted of a terrorist offence, they can appeal the same as any other conviction. For groups that have been dissolved, there is no apparent appeal process.

⁸¹ [Article L212-1 Homeland Security Code](#), Government of France, 2021.

⁸² [Practical information relating to measures to freeze assets for the purpose of combating terrorism](#), Government of France Ministry of the Economy, Finance and Industrial and Digital Sovereignty, 2021.

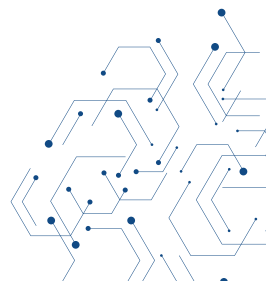
⁸³ [Section 421-1 Penal Code](#), Government of France, 2016.

⁸⁴ [Section 421-2-5-1 Penal Code](#), Government of France, 2016.





<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> ● As there is no national-level designation list, the legislation surrounding online regulation is unclear and places the responsibility of decision making on tech companies. ● There is no clarity in the current definition of terrorism and it is very open to interpretation, again placing decision making for online regulation on tech companies. ● There is no clear appeal process for groups that have been dissolved. ● There is a lack of transparency throughout dissolution processes, and it is unclear what criteria are consulted when dissolving a group.
<p>What do we recommend?</p>	<ul style="list-style-type: none"> ● We recommend that France publish a consolidated dissolution list to increase transparency and support the tracking of terrorist entities that have been dissolved. ● We recommend that France create clarity in the terrorism definition to ensure counterterrorism efforts and online regulation are less open to interpretation. ● We advise France to amend the current legislation to make clearer how the status of dissolved groups impacts terrorism convictions. ● We suggest that France should establish a formal designation process to allow for offline and online counterterrorism efforts to be more cohesive and based in the due process. ● We recommend that France tie designation to online regulation, which would provide tech companies with legal grounding to counter terrorist use of the internet within the rule of law. ● We advise France to create a review process for groups that are dissolved to protect human rights and ensure the power is not used against legitimate groups. ● When a formal designation process has been established, we recommend that France ensure that it contains adequate processes of review and appeal, and that it respects due process.
<p>Further information and comments</p>	





GERMANY

<p>Does the country or institution have their own list of designated, banned, or proscribed groups?</p>	<p>Yes, these lists (split by ideology) can be found here.⁸⁵</p>
<p>What type of system does the country or institution use?</p>	<p>Banning - organisations are banned for being anti-constitutional. This criminalises membership, as well as the dissemination and possession of propaganda. The government will ban an organisation in accordance with Article 9(2) of the constitution⁸⁶ in conjunction with Section 3 of the Associations Act (Vereinsgesetz).⁸⁷</p> <p>What is the definition of terrorism the country employs?</p> <p>German legislation does not seem to provide a definition of terrorism, and domestic bans of organisations are based on their “anti-constitutional” nature rather on their association with terrorism. However, the Criminal Code’s section 129a⁸⁸ on forming and supporting terrorist organisations does provide some guidance on the meaning of a “terrorist organisation”, which can be understood as:</p> <p>“an association aimed at causing serious physical/mental harm to another person or committing crimes against the environment (including murder, manslaughter, genocide, crimes against humanity, war crimes, crimes against personal freedom)” when such acts are intended to “intimidate the population in a significant way, OR to unlawfully attack a government agency or IO with violence/threat thereof, with the aim of threatening the normal functioning of the state or challenging the political, constitutional, economic or social structures of the state.”</p>
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>As mentioned, the country’s banning process does not relate to a definition of terrorism but rather to the constitution.</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Yes - both.</p>
<p>Does designation have effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>This is complex. The Netzwerkdurchsetzungsgesetz (NetzDG) adopted in 2017 compels tech firms to combat hate speech, terrorist propaganda, criminal material, and misinformation on their sites and platforms. This law focuses on the content rather than the source, but does include the dissemination of propaganda and symbols from banned organisations.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>Yes- A package of legislation from April 2021 (adding further requirements to NetzDG) requires companies to assess whether users engage in prohibited types of expression including “training in and support of criminal or terrorist organisation” or “incitement to hatred.”⁸⁹ The list of expressions are included in 3a (2) of the NetzDG.</p>

⁸⁵ [Subjects List](#), Federal Office for the Prosecution of the Constitution.

⁸⁶ Article 9(2) Basic Law for the Federal Republic of Germany in conjunction with Section 3, Government of Germany,

⁸⁷ [Law on the regulation of public association law \(association law\)](#), Government of Germany, 1964 last amended 2020.

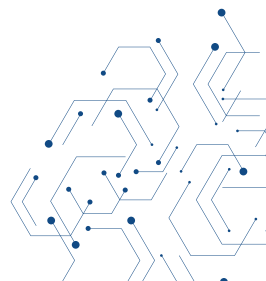
⁸⁸ [Section 129a Criminal Code](#), Government of Germany, 1998 last amended 2021.

⁸⁹ [3a \(2\) of NetzDG](#), Federal Law Gazette archive of the editions published between 1949 and 2022, 2021.





<p>Is online content that incites acts of terrorism illegal?</p>	<p>Yes, see above.</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>Yes, Germany has banned over 60 far-right groups and regularly updates this list. It has also banned Islamist groups included the Islamic State and most recently Hezbollah.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>Section 8 of the Associations Act prohibits the formation of ‘substitute’ organisations. Section 6 outlines that if a prohibition is contested, its lawfulness can be tested in the courts.</p> <p>There does not seem to be a regular review process for banned organisations capable of sufficiently protecting human rights.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • While Germany is leading in terms of recognising the far-right threat, Germany’s lists for banned organisations are not easily accessible or centralised. This undermines guidance to tech companies, and further risks undermining Germany’s leadership in this area. • Additionally, Germany has a list of banned far-right organisations but does not have its own list of designated groups or individuals, relying on EU/UN lists for non-far right groups. There is a section of the Associations Act (section 14) which covers the banning procedure for ‘Foreign Associations.’ • There seem to be differing implications for online content depending on whether the group is banned or designated. The NetzDG explicitly refers to prohibiting dissemination of propaganda and symbols from banned organisations. However, there is no such reference to the content of designated groups. • The implication is that the content of designated groups not banned can only be removed if it explicitly encourages or supports a terrorist organisation. This remits the responsibility for adjudicating terrorist content to tech platforms. • The lack of a review process for banned organisations suggests insufficient protection of human rights.





<p>What do we recommend?</p>	<ul style="list-style-type: none"> ● We recommend that Germany makes their list of banned organisations more easily accessible to support tech companies who are mandated to remove this content. Germany should keep records so that the designation of groups, actors, or content happens transparently, and should also implement a system whereby such records can be made available for judicial oversight. ● We believe governments should accurately designate far-right terrorist groups by including civil society representatives, CT specialists, and human rights lawyers in suggesting designating/delisting entities. We welcome Germany's leadership in this area, as the government has to date banned over 60 far-right violent extremist and terrorist organisations. This has as a result provided tech companies in Germany the appropriate legal grounding to moderate their platforms effectively.⁹⁰ ● However, we recommend Germany considers banning non-German far-right groups whose online content remains a threat to German citizens. ● We advise Germany to consider designating lone actors who have committed an attack, with a basis in online regulation, so that associated manifestos become illegal. ● The NetzDG definition of terrorist content focuses on the content rather than the source, but does include the dissemination of propaganda and symbols from banned organisations. We propose the propaganda and symbols of designated groups should also be considered. ● Alongside online regulation, the establishment of a regulatory body should be considered to provide more clarity for tech companies on the practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance. ● In addition to online regulation and a regulator, we propose considering an independent 'classification office' where material from designated groups and content falling under the definition of terrorist content can be considered and classified. Based on the definition of online terrorist content, counterterrorism experts alongside civil society representatives would adjudicate on the legality of specific pieces of content. This would provide additional clarity for tech companies.
<p>Further information and comments</p>	

⁹⁰ Online Regulation Series, Tech Against Terrorism, 2021; 2022.





DENMARK

Does the country or institution have their own list of designated, banned, or proscribed groups?

Yes.

What type of system does the country or institution use?

Political proscription. Article 78 of Danish constitution states that “Associations employing violence, or aiming at the attainment of their object by violence, by instigation to violence, or by similar punishable influence on persons holding other views, shall be dissolved by court judgement.”⁹¹ Decisions to proscribe are justifiable in the Danish courts.

In recent years, the use of the law has mainly been confined to gangs (such as the 2020 ban of Loyal to Familia,⁹² the only contemporary organisation in Denmark to face proscription) and Islamist organisations, such as Hizb ut-Tahrir, which has been under intensified surveillance since 2008.

What is the definition of “terrorism” the country or institution employs?

Section 114 in the Criminal Code punishes “terrorist crimes.” This includes financing, providing training/ education conducive to terrorism, and travel to designated “terrorist areas”.

Terrorist crimes are described as follows: “For terrorism, imprisonment for life is punishable for anyone who, with intent to intimidate a population, severely or unjustifiably to force Danish or foreign public authorities or an international organisation to commit or fail to commit an act, or to destabilise or destroy a country or the fundamental political, constitutional, economic or societal structures of an international organisation, commit one or more of the following acts, where the act, by virtue of its nature or the context in which it is committed, may cause serious harm to a country or international organisation:

- 1) Manslaughter under § 237 .
- 2) Serious violence under § 245 or § 246 .
- 3) Detention under section 261 .
- 4) Disruption of traffic safety pursuant to section 184, subsection 1 , unlawful disturbances in the operation of ordinary means of transport, etc. pursuant to section 193, subsection 1 , or gross vandalism pursuant to section 291, subsection 2 , if these violations are committed in a way that could endanger human life or cause significant financial loss.
- 5) Hijacking of means of transport pursuant to section 183 a .
- 6) Violations of the legislation on weapons and explosives in particularly aggravating circumstances pursuant to section 192 a .
- 7) Arson pursuant to section 180, blasting, dispersal of harmful gases, flooding, shipwreck, railway or other transport accident pursuant to section 183, subsection 1 and 2 , hazardous pollution of the water supply pursuant to section 186, subsection 1, hazardous pollution of things intended for general distribution, etc. pursuant to section 187, subsection 1.
- 8) Possession or use, etc. of radioactive substances pursuant to section 192 b .”
 - o Provisions of Paragraphs 114(c) and 114(d) criminalize recruitment and training in relation to crimes under Sections 114 to 114(b). Section 114(e) contains a provision on criminal liability for those who otherwise promote the activities of a person, group or association who commits or intends to commit acts covered by Paragraphs 114 to 114(d).

⁹¹ [The Constitution Act of Denmark](#), Government of Denmark.

⁹² [Loyal to Familia is dissolved according to § 78 of the Basic Law](#), Copenhagen Police, 2020.





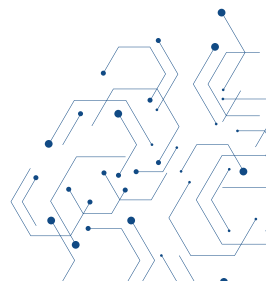
<p>How does the designation process relate to the relevant authority's definition of terrorism?</p>	<p>There is no relationship between the proscription process and the country's definition of terrorism because proscription is based on the Danish constitution relating to an association's use of violence.</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Yes, the EU and UN lists.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>The Danish government recently proposed legislation which would impose removal deadlines for and large fines to social media platforms that do not swiftly remove content relating to illegal activity (including terrorist propaganda).⁹³ However, it is unclear whether this will be connected to the designation lists Denmark relies on. It is more likely the law will judge on the nature of the content rather than its source which may nonetheless remit to tech companies the responsibility of adjudicating what constitutes terrorist content.</p>
<p>Is online content that incites acts of terrorism illegal?</p>	<p>Section 114(e) of criminal code contains a provision on criminal liability for those who otherwise promote the activities of a person, group or association who commits or intends to commit acts covered by Paragraphs 114 to 114(d). There is no specific mention of online content, leaving the inclusion of online content that promotes terrorism open to interpretation. The proposed legislation mentioned above would make terrorist propaganda illegal and force tech companies to remove this content or face large fines. The definition of terrorist propaganda is not currently clear.</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>Not currently. It is likely this content would be illegal under the new legislation, but this will depend on how exactly terrorist propaganda is defined.</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No, Denmark adheres to the EU/UN designation lists, neither of which has designated any extreme far-right groups.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>There does not appear to be an appeals process for political proscription that would help protect human rights. However, as stated in the constitution governments cannot dissolve associations and cases must be decided by the Supreme Court.</p>

⁹³ [Why have governments been so slow to remove illegal social media posts?](#), Sarah Manavis, New Statesman, 2022.





<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> • Denmark relies on EU/UN lists so does not have its own formal designation process in place resulting in a lack of autonomy in this area. Supranational lists are the object of familiar criticisms, including a lack of transparency in their inclusion policies and a bias towards designation of Islamist extremist groups over extreme far-right groups (See our EU/UN profiles). • While organisations in Denmark can face political proscription, this is a measure confined to the use of violence within Denmark. Hence this law is not focused on international terrorist acts so is not a suitable framework for expanding designation. • Denmark does not have any legislation that explicitly refers to online terrorist content or indeed attempts to define it. Proposed legislation is likely to address this gap. • There is a disconnect between designated terrorist organisations (EU/UN list) and the legality of their official content online.
<p>What do we recommend?</p>	<ul style="list-style-type: none"> • We recommend developing a definition of online terrorist content as part of the new legislation, ensuring it considers official content produced by designated terrorist groups. This would provide tech companies with legal grounding for countering terrorist use of the internet. • Alongside online regulation, the establishment of a regulatory body should be considered to provide more clarity for tech companies on practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance. • In addition to online regulation and a regulator, we propose considering an independent 'classification office' where material from designated groups and content falling under the definition of terrorist content can be considered and classified. Based on the definition of online terrorist content, counterterrorism experts alongside civil society representatives would adjudicate on the legality of specific pieces of content. This would provide additional clarity for tech companies. • Depending on EU/UN progress in this area, Denmark should consider developing national designation processes in addition to EU/UN lists to consider entities that threaten national security, especially with reference to extreme far-right groups. • We advise including civil society representatives, counterterrorism specialists, and human rights lawyers in designating or delisting relevant entities. • We recommend designating extreme far-right groups or lone actors who have committed an attack and making their content, such as manifestos, illegal. This would tie designation to online regulation, ensuring that governments set the norms on what is legal and illegal speech rather than tech companies making adjudications of content by reference to vague definitions. • We advise keeping records so that the designation of groups, actors, or content happens transparently and a system whereby such records can be made available for judicial oversight.
<p>Further information and comments</p>	





SWEDEN

Does the country or institution have their own list of designated, banned, or proscribed groups?	No.
What type of system does the country or institution use?	Sweden does not have its own system of designation.
What is the definition of “terrorism” the country or institution employs?	<p>There is no definition of the term ‘terrorism’ in Sweden’s criminal law. However, act 2003:148 regulates what constitutes “terrorist crimes.”⁹⁴ The conditions for criminal liability for terrorist crimes are set out in sections 2 and 3. Section 3 outlines the specific acts that can constitute terrorist offences (inc. murder, aggravated assault etc.).</p> <p>A terrorist crime is defined as an “act [as defined in sec. 3] that can seriously harm a state or an intergovernmental organization and the intention of the act is to (either or at least one of):</p> <ul style="list-style-type: none"> • instil serious fear in a population or a population group, • unduly force public bodies or an intergovernmental organization to take or to refrain from taking action, or • seriously destabilize or destroy basic political, constitutional, economic or social structures of a State or of an intergovernmental organization” - Section 2
How does the designation process relate to the relevant authority’s definition of terrorism?	As Sweden does not have its own designation process, there is no relationship to a standard definition of terrorism.
Does the country follow UN or EU (if relevant) designation lists and sanctions?	Yes, both the EU and UN lists are used.
Does designation have an effect on the online realm? Is content created by terrorist groups illegal?	No. Content may be illegal under generally applicable rules, but there is no specific ban on content created by terrorist groups.

⁹⁴ [Lag \(2003:148\) om straff för terroristbrott](#), Sveriges Riksdag, 2003.





<p>Is online content that incites acts of terrorism illegal?</p>	<p>Yes.</p> <p>The act on Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crime (2010:299) contains several offences that may be relevant, in particular public provocation.⁹⁵ This offence consists of urging or otherwise trying to induce others, in a communication to the public, to commit a terrorist offence and may be committed online. The same applies to the offences of recruitment and providing terrorism training.</p> <p>This law also criminalises sharing material online with the explicit purpose of providing education for others that could help to commit terrorist crimes (i.e., just sharing such material recklessly is not criminalised).¹ The decisive factor for criminal liability is what the sharer knows about the recipient's criminal purposes, not the sharer's own intentions.</p> <p>It is conceivable that criminal liability may be incurred by sharing online material capable of inciting a terrorist crime according to the law 2003:148 on punishment of terrorist crimes. Instigating a terrorism offence and conspiracy to commit a terrorist offence could also be committed online.</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>No, only if content falls within scope of general provisions such as those mentioned above. Note that public provocation to conspire with a terrorist organisation is criminalised. There is no specific offence of collaboration with designated terrorist groups; for the purpose of this offence a terrorist organisation is defined by reference to the crimes its members commit (e.g., terrorist offences).</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>No, Sweden adheres to the EU and UN designation lists which have not designated any far-right groups.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>As Sweden does not have its own designation process, there are no delisting processes.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> ● Sweden does not have its own list for proscription, designation, or banning. ● Sweden relies on EU/UN lists so does not have its own formal designation process in place resulting in a lack of autonomy in this area. These lists are the object of familiar criticisms, including a lack of transparency in their inclusion policies and a bias towards designation of Islamist violent extremist groups over far-right violent extremist groups. ● While there are some references to the online sphere in national terrorism legislation, such as the criminalisation of sharing material online with the explicit purpose of instructing others to commit terrorism, this law is applied on a case-by-case basis and provides a high threshold. ● Hence, there is a disconnect between designated terrorist organisations (EU/ UN lists) and the legality of their official content online, which leaves tech companies to adjudicate on what is considered terrorist content.

⁹⁵ [Lag \(2010:299\) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet](#), Sveriges Riksdag, 2010.





<p>What do we recommend?</p>	<ul style="list-style-type: none"> • We propose developing an explicit definition of online terrorist content as part of online regulation legislation, which considers the source of the content to ensure official content from designated terrorist groups can be included. This would tie designation to online regulation and thus provide tech companies with clear legal and factual basis for the removal of terrorist content. • Alongside online regulation, the establishment of a regulatory body should be considered to provide more clarity for tech companies on the practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance. • In addition to online regulation and a regulator, we propose considering an independent ‘classification office’ where material from designated groups and content falling under the definition of terrorist content can be considered and classified. Based on the definition of online terrorist content, counterterrorism experts alongside civil society representatives would adjudicate on the legality of specific pieces of content. This would provide additional clarity for tech companies. • Depending on EU/UN progress in this area, we advise developing a national designation process in addition to EU/UN lists to consider entities that threaten national security, with particular reference to far-right violent extremist groups. • We recommend including civil society representatives, counter-terrorism specialists, and human rights lawyers to consult on designating or delisting an entity as well as implementing regular review mechanisms. • We recommend that Sweden consider designating far-right groups or lone actors who have committed an attack by means of online regulation so that manifestos and other associated material become illegal, rather than require tech companies to adjudicate content by reference to vague definitions of terrorism. • We advise keeping records so that the designation of a group, actor, or content happens transparently and making such records available for judicial oversight.
<p>Further information and comments</p>	<p>The use of certain symbols may be punishable as agitation against a population group, when the act threatens or expresses contempt for a population group by allusion to e.g., ethnic origin, religious belief or sexual orientation.⁹⁶ Case law includes convictions relating e.g., to the Swastika. This offence applies to a statement or other communication that is disseminated (i.e., transmitted to more than a few persons) “outside the completely private sphere.” Oral and written verbal messages are covered, as are images and symbols. The offence may be committed online.</p>

⁹⁶ [Prop. 2001/02:59](#), Sveriges Riksdag, 2001.





SPAIN

Does the country or institution have their own list of designated, banned, or proscribed groups?

No.

What type of system does the country or institution use?

Proscription – While Spain has no formal list, it does have the ability to proscribe a political group domestically. Article 6 of the Spanish Constitution states with regard to political groups that “[t]heir creation and the exercise of their activities are free in so far as they respect the Constitution and the law.”⁹⁷ There are two possible ways to proscribe a political group. Firstly, a procedure of criminal law enables groups to be banned for being anti-constitutional (article 6) in conjunction with article 515 of the Spanish Penal Code which prohibits illicit associations with paramilitary/terrorist/violent groups or those that incite hate and discrimination against others.⁹⁸ Secondly, a civil procedure outlined in the Organic Law 6/2002 on Political Parties permits both the government and Prosecution Office to request the Judicial Authorities to initiate the procedure allowed in certain cases and outlined in article 9.2 of the law.⁹⁹ These cases include instances when the group: which prohibits illicit associations with paramilitary/terrorist/violent groups or those that incite hate and discrimination against others.¹⁰⁰ Secondly, a civil procedure outlined in the Organic Law 6/2002 on Political Parties permits both the government and Prosecution Office to request the Judicial Authorities to initiate the procedure allowed in certain cases and outlined in article 9.2 of the law.¹⁰¹ These cases include instances when the group:

- Systematically violates fundamental freedoms and rights by promoting, justifying or exculpating attacks against the life or integrity of persons, or the exclusion or persecution of persons because of their ideology, religion or beliefs, nationality, race, sex or sexual orientation.
- Encourages, propitiates or legitimises violence as a method for the achievement of its political objectives or to eliminate the conditions necessary for the exercise of democracy, pluralism and political freedoms.
- Complements and politically supports the action of terrorist organisations in order to achieve their goals of subverting the constitutional order or seriously altering public peace.
- Attempts to subject public authorities, certain persons or groups of society or the population in general to a climate of terror, or contributes to multiply the effects of terrorist violence and the fear and intimidation generated by the same.

⁹⁷ [The Spanish Constitution](#), Government of Spain, 1978.

⁹⁸ [Spanish Penal Code](#), Spanish Ministry of Justice, 2016.

⁹⁹ [Organic Law 6/2002 of 27 June](#), on Political Parties, Government of Spain, 2002.

¹⁰⁰ [Spanish Penal Code](#), Spanish Ministry of Justice, 2016.

¹⁰¹ [Organic Law 6/2002 of 27 June](#), on Political Parties, Government of Spain, 2002.





<p>What is the definition of “terrorism” the country or institution employs?</p>	<p>Definition of Terrorism – Article 573 Spanish Criminal Code 2019.¹⁰²</p> <ul style="list-style-type: none"> • Terrorism is defined as “[t]he commission of any serious crime against life or the physical integrity, liberty, moral integrity, sexual freedom and indemnity, heritage, natural resources or the environment, public health, of catastrophic risk, fire, document falsification, against the Crown, attack and possession, trafficking and deposit of arms, ammunition or explosives, provided for in this Code, and the seizure of aircraft, ships or other means of collective or merchandise transport.” • To come under the rubric of terrorism, the above offences must be carried out for the following purposes: <ul style="list-style-type: none"> o Subvert the constitutional order, or to suppress/seriously destabilise the functioning of political institutions or the economic or social structures of the State, or to force the public powers to carry out an act or refrain from doing so o Seriously alter the public peace o Seriously destabilise the functioning of an international organisation o Cause a state of terror in the population or in a part of it.
<p>How does the designation process relate to the relevant authority’s definition of terrorism?</p>	<p>In relation to designation, Spain relies on external lists so there is no relationship to the country’s definition of terrorism. Terrorist organisations are considered the same as Criminal Organisations (Article 570 Bis) but with their purpose being the commission of crimes in Articles 572-580 (terrorism). The civil procedure for proscribing political groups can be used in relation to terrorism, if the group supports the action of terrorist organisations or attempts to subject public authorities, certain persons or groups of society or the population in general to a climate of terror, or contributes to multiply the effects of terrorist violence and the fear and intimidation generated by the same. In 2004, the Special Chamber of the Supreme Court criminalised and dissolved Batasuna under the Law of Political Parties, having proved it was an instrument created by and part of the terrorist organisation ETA. Partido Comunista Español (reconstituida) or PCEr was banned under the same law in 2003, as it was considered a single terrorist structure with The First of October Antifascist Resistance Group (GRAPO).</p>
<p>Does the country follow UN or EU (if relevant) designation lists and sanctions?</p>	<p>Yes - Spain relies on the EU framework and UN designations pursuant to resolution 1267/1989/2253 (al-Qaeda and the Islamic State) and resolution 1988 (the Taliban).¹⁰³ The Spanish regulatory framework has made the decision to designate groups that have been also designated by the UN as part of its commitments to the Security Council.</p>
<p>Does designation have an effect on the online realm? Is content created by terrorist groups illegal?</p>	<p>No. However, the online activities and assets (websites, online platform accounts etc.) of proscribed political groups should be suppressed (based on LPP, however online is not specifically mentioned). In the criminal case of Batasuna, the court ordered that web pages should be deleted and internet services used by Batasuna should be notified to the police.</p>

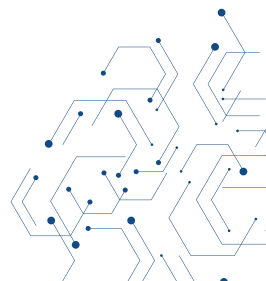
¹⁰² Article 573 Spanish Criminal Code 2019, Government of Spain, 2019.

¹⁰³ [Resolution Adopted on the ISIL \(Da’esh\) and Al-Qaida Sanctions Committee](#), Security Council Report, 2020.





<p>Is online content that incites acts of terrorism illegal?</p>	<p>The Spanish Criminal Code criminalises online content that glorifies terrorist acts (art. 578 subsection 1) or incites terrorism (art. 579).</p>
<p>Is online content that supports designated terrorist groups illegal?</p>	<p>Yes, as long as it glorifies terrorist acts or incites terrorism. This adjudicates on the nature of the content and not the source of the content (whether it's official).</p>
<p>Is there a sufficient balance between far-right and violent Islamist groups and individuals?</p>	<p>Two extreme far-right groups have been proscribed in relation to the offence of unlawful association in relation to illicit activities not linked to terrorism (Article 515.5 of Penal Code). They were Blood & Honour España and Hammerskin España, both proscribed in 2011.</p> <p>However, political proscription only applies to far-right political groups that operate domestically, excluding internationally designated far-right groups such as Atomwaffen Division (AWD). Furthermore, given Spain relies on EU/UN lists, there is a heavy skew towards violent Islamist groups such as al-Qaeda and IS.</p>
<p>Are there human rights-compliant mechanisms in place for delisting a group?</p>	<p>The judicial dissolution of a political group must be decided by the Special Chamber of the Supreme Court and is therefore based on the rule of law and the Constitution. As there is no formal list for dissolved political groups, there is no regular review process for 'delisting'.</p>
<p>What are the weaknesses in the designation process?</p>	<ul style="list-style-type: none"> ● The process of political proscription is based on the constitution and penal code rather than on terrorism legislation. This judicial process explicitly considers political groups on a case-by-case basis (not a list) and is therefore an unsuitable mechanism to use for the designation of terrorist entities. ● Spain relies on EU/UN lists so lacks autonomy in this process and cannot proactively designate. ● Current supranational lists overlook the threat of extreme far-right organisations. ● Spain should be commended for tying proscription to online regulation, through the Law of Political Parties under which the online activities and assets (websites, online platform accounts etc.) of proscribed political parties are illegal. ● However, there is no link between designation and online regulation. Tech companies are provided with no legal clarity on the removal of online terrorist content.





What do we recommend?

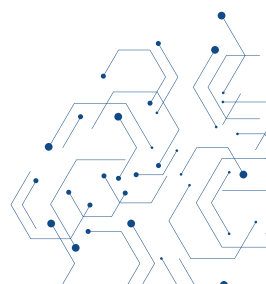
- We recommend clarifying Spain's process for designating terrorist entities and separating it from political proscription.
- Depending on EU/UN progress in this area, we recommend that Spain consider developing a national designation process in addition to EU/UN lists to consider entities that threaten national security. We advise accounting for the threat posed by extreme far-right groups and lone actors, starting with those which have already been politically proscribed.
- We propose developing an explicit definition of online terrorist content, as part of online regulation legislation, which considers the source of the content to ensure official content from designated terrorist groups can be included. This would tie designation to online regulation and thus provide tech companies with clear legal and factual basis for the removal of terrorist content.
- Alongside online regulation, the establishment of a regulatory body should be considered to provide more clarity for tech companies on the practical steps tech companies can take to identify and remove illegal terrorist content. The regulator would also have punitive measures available to enforce compliance.
- In addition to online regulation and a regulator, we propose considering an independent 'classification office' where material from designated groups and content falling under the definition of terrorist content can be considered and classified. Based on the definition of online terrorist content, counterterrorism experts alongside civil society representatives would adjudicate on the legality of specific pieces of content. This would provide additional clarity for tech companies.
- We propose creating a review process for individuals and groups that are designated to protect human rights.
- To respond to the changing threat landscape from terrorist groups, Spain should consider including civil society representatives, counterterrorism specialists and human rights lawyers in the designation process.
- We advise keeping records so that the designation of groups, actors, or content happens transparently and making such records available for judicial oversight.

Further information and comments

Pursuant to article 577 Subsection 2 of the Spanish Criminal Code, a penalty of 5-10 years may be imposed on those who carry out any "recruitment, indoctrination or training activity, which is directed or which, due to its content, is capable of incitement to join a terrorist organisation".

As well as the criminalisation of incitement and support, Article 575 Subsection 2 of the Criminal Code covers:

- The crime of "receiving indoctrination" which incurs a prison sentence on conviction of 2-5 years applicable to anyone who "regularly accesses one or more communication services accessible to the public online or content accessible through the internet or an electronic communications service" whose contents aim to "incite [another] to join a terrorist organisation or group, or to collaborate with any of them or for their purposes". This applies when the offence is committed in Spain and the content is accessible in Spain.
- This crime is also committed when an individual acquires or has in their possession documents that "encourage the incorporation of a terrorist organisation or group or collaboration with any of them."



6.2 Methodology

Scope

In designing our research, we have focused on the designation systems of western democracies. In future research, we intend to explore the designation systems of a greater diversity of political models worldwide.

For this research, we analysed the designation (or similarly but nonetheless differently named) systems of the following nations and supranational bodies:

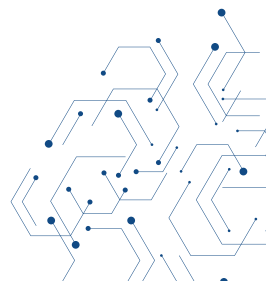
- United Nations
- European Union
- Canada
- United States
- Australia
- New Zealand
- United Kingdom
- France
- Sweden
- Germany
- Spain
- Denmark

Furthermore, this work has focused predominantly on the designation of terrorist groups, not on the regimes of sanctions against individuals that often accompany national or supranational designation lists. However, we do investigate the designation of lone-actor terrorists in this report, as can be and has occasionally been done in the case of a terrorist entity, such as with the Christchurch attack perpetrator, who was designated as a terrorist entity in New Zealand. In addition, this report aims to explore improvements to the designation of far-right terrorist entities, for which lone-actors who have committed attacks are an essential consideration.

Methods:

For this paper we embraced a multi-stage, mixed-methodology approach, which sought to analyse a wide range of original and existing data. A primary legal review was the core data collection avenue, which was paired with a literature review and unstructured interviews with experts in designation.

To conduct this research, Tech Against Terrorism used solely open-source information which is freely and publicly available. Our findings being made on the basis of purely public information about designation systems, they may be incomplete if there is relevant information available in sources that we were unable to consult for reasons of security classification.



We have mitigated this risk by also consulting academics with expertise on a range of jurisdictions to ensure that our analysis is based to the greater possible extent on factual, verifiable data, which accurately represents the designation process in question. We also consulted with governments and governing bodies to ensure the accuracy of our findings. In some instances, this has required some amendment to our conclusions, and we have throughout the report clearly marked where such consultation has warranted an amendment.

Literature review

Our literature review process is focused on two main categories of source:

- Academic papers
- Third-party research

In considering the variety of available literature, we highlighted that there was a significant deficiency in the academic literature concerning the wider understanding of the global designation processes. By expanding the scope of the literature review to also include third-party research by civil society and NGOs, our literature review sought to explore the current understanding of designation further.

Legal review

In analysing the designation processes of numerous democratic nation states and supranational institutions, a variety of sources were consulted to ensure all available data was incorporated into our analysis. These documents include, but were not limited to:

- Official legislation
- Official designation lists
- Green papers
- Interim codes
- Pending legislation
- Government statements
- Court documents

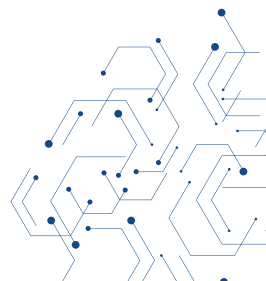
Official legislation provided the basis of our analysis, but these additional avenues of data permitted a more nuanced analysis by providing further insight into how designation processes operate in practice.

Interviews

In the course of our interview process, we spoke with leading scholars in the field to gain further insight into how academics and researchers currently understand global designation processes. These interviews allowed us to better understand how researchers are able to engage with designation processes when conducting scholarly enquiries, which informed our recommendations.

We held interview with the following experts on designation:

- Jason Blazakis, Former Director of the Counterterrorism Finance and Designations Office, Bureau of Counterterrorism, U.S. Department of State.
- Anna Meier, Assistant Professor of Politics and International Relations at the University of Nottingham focussing on terrorism and counterterrorism.



- Gavin Sullivan, Reader in International Human Rights Law at The University of Edinburgh, lead researcher for the UKRI-funded project, *Infra-Legalities: Global Security Infrastructures, Artificial Intelligence and International Law* and lawyer who has provided pro-bono legal representation to people targeted by security lists worldwide, including before the UN Office of the Ombudsperson.
- David Shanks - Chief Censor of the New Zealand Classification Office at the time of writing this report.

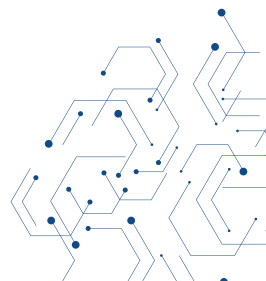
As part of our analysis of designation processes, Tech Against Terrorism also conducted interviews with a range of representatives from the relevant nations and supranational institutions. Within the interviews, Tech Against Terrorism provided our understanding of the relevant designation process, which the representatives were given a chance to thoroughly review and check. The interviews permitted an open dialogue on the strengths and limitations of designation as well as specific processes within the global practice, and the results of these discussions later informed our proposals.

We held interviews with representatives from the following jurisdictions:

- United Kingdom
- Canada

We also received written input from:

- United States
- United Nations
- European Union
- Canada
- Spain
- New Zealand
- Sweden
- United Kingdom
- France



ABOUT TECH AGAINST TERRORISM

Tech Against Terrorism supports technology companies to counter the terrorist use of the internet. It is an independent public-private partnership initiated by the UN Security Council.

Our research shows that terrorist groups - both jihadist and far-right terrorists - consistently exploit smaller tech platforms when disseminating propaganda. At Tech Against Terrorism, our mission is to support smaller tech companies in tackling this threat whilst respecting human rights and to provide companies with practical tools to facilitate this process.

As a public-private partnership, the initiative works with the United Nations Counter Terrorism Executive Directorate (UN CTED) and has been supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of Spain, Switzerland, the Republic of Korea, and Canada.

contact@techagainstterrorism.org



This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>

