tech against terrorism

POSITION PAPER | MARCH 2023

WHO DESIGNATES TERRORISM?

The Need for Legal Clarity to Moderate Terrorist Content Online

This Position Paper lays out the key findings and recommendations on the designation of terrorism. The full report is available on our website.

TABLE OF CONTENTS

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.

ABOUT TECH AGINST 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