RUSI
www.rusi.org
Royal United Services Institute
for Defence and Security Studies

BROOKINGS

Global Research Network on Terrorism and Technology: Paper No. 7

Terrorist Definitions and Designations Lists

What Technology Companies Need to Know

Chris Meserole and Daniel Byman

Key Findings and Recommendations

Many technology companies refer to third-party terrorist definitions and designation lists when moderating potential terrorist accounts. However, those definitions and lists are often produced for specific legal, political or academic purposes and may not be suitable for general use. Technology companies should understand such lists' relative strengths and limitations before relying on them.

Key recommendations:

- Technology companies should define terrorist entities in a way that distinguishes them from non-violent dissidents, state actors, conventional rebel groups, and criminals or criminal syndicates.
- Technology companies should use government designation lists with caution, since even the lists compiled by democratic governments are more likely to include some terrorist groups but not others.
- The technology sector and representatives from civil society, academia and government should work together to develop a global, unbiased and real-time database of possible terrorist entities. The database could be used to produce different designation lists based on various inclusion criteria.

Introduction

Terrorist groups pose a profound challenge for technology companies. The 'blitzscaling' model pioneered by YouTube, Instagram and others has enabled social networks and file-sharing services to gain tens and even hundreds of millions of users globally before they make meaningful revenue, much less profits.[1] By the time technology companies can afford to hire a counterterrorism expert, it is often too late: any application with tens of millions of users worldwide but little oversight is ripe for terrorist exploitation. Worse, even when companies are able to hire counterterrorism experts, they are often unable to do so at a scale commensurate with the problem.[2]

1. 'Blitzscaling' is a business strategy that prioritises rapid growth and that leverages cloud computing. From the mid-2000s on, companies could scale quickly and globally without investing in massive data centres and personnel. For instance, YouTube had 50 million users but only 65 employees when it was purchased for $1.6 billion, while Instagram had 30 million users and 13 employees when it was purchased for $1 billion. Both companies were only two years old when purchased. See Reid Hoffman and Chris Yeh, *Blitzscaling: The Lightning-fast Path to Building Massively Valuable Businesses* (New York, NY: Currency, 2018).
2. The technology platform with the largest known staff of terrorism experts is Facebook, which had hired over 150 terrorism analysts by 2017. Yet even

For the vast majority of technology companies, developing an in-house competence in counterterrorism is thus not a viable strategy for moderating potential terrorist accounts. Instead, most companies must choose between one of two imperfect strategies. The first is to adjudicate possible terrorist accounts on an ad hoc basis. The downside to this approach, as CloudFlare CEO Matthew Prince made clear when he 'woke up one morning and decided' to take the Daily Stormer, a popular online forum for white nationalists, offline after the Charlottesville attack, is that it is arbitrary.[3] By contrast, another strategy is to rely on third-party terrorist definitions and designation lists. Although this approach offers a more principled means of account moderation, it is not without its own drawbacks. Most notably, off-the-shelf definitions and designation lists all contain biases and limitations that may not be obvious to non-experts and that could unwittingly bias a company's efforts at platform governance. Just as companies lack the competence to identify terrorist actors, they also lack the expertise to discriminate between various definitions and lists – often with significant consequences.

Relying on third party definitions and lists is preferable to ad hoc adjudication, but companies that adjudicate terrorist accounts based on such lists should understand how to evaluate them. The aim of this policy paper is to provide such an understanding.

Definitions

Defining terrorist actors is notoriously difficult. A wide variety of academics, technology companies and government agencies have published their own definitions, but there is no universally accepted definition.[4] Indeed, even the UN, which as a global organisation is well positioned to produce one, has yet to do so; despite numerous attempts, UN member states have yet to agree on how to define terrorism and terrorist entities.[5] (Members disagree

Facebook still struggled to moderate potential terrorist accounts on its network. See Jeremy Kahn, 'Facebook Enlists AI, Human Experts in New Push Against Terrorism', *Bloomberg*, 15 June 2017.

3. Will Oremus, 'Cloudflare's CEO Is Right: We Can't Count on Him to Police the Internet', *Slate*, 17 August 2017.
4. The lack of consensus has been a longstanding problem. In the late 1980s, Alex Schmid and Albert Longman reviewed over 100 definitions of terrorism, and found little overlap in them. See Alex P Schmid and Albert J Longman (eds.), *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature* (New Brunswick, NJ: Transaction Books, 1988), pp. 5–6.
5. According to the UN Counter-Terrorism Executive Directorate, the reason for the lack of consensus is that 'an unequivocal definition of terrorism would remove the political distinction that some make between the actions of so-called freedom fighters and terrorists'. See UN Counter-Terrorism Executive Directorate, 'Frequently Asked Questions about UN Efforts to Fight

on whether to include groups associated with liberation movements and popular causes, such as Palestinian nationalism.)

However, the absence of a universal definition of terrorist groups does not imply that the term is devoid of meaning, or that producing a responsible definition of terrorist is not possible.[6] For example, there is some agreement, particularly among experts and institutions within liberal democracies,[7] that terrorists are different from other contentious actors by virtue of the following:

- Use of violence: although terrorist actors often justify their violence in terms of specific beliefs and ideologies, it is the use of violence – or threat of violence – that distinguishes terrorist actors from political dissidents and extremists. Authoritarian states like China will often include references to 'thought' or 'speech' when defining terrorism and terrorist entities, not just violence.[8] Precisely to avoid making moral judgements about which thoughts and political beliefs are acceptable, terrorist activity is generally defined in terms of violence rather than merely disagreement or even hateful speech or thought.
- Non-state actor: since states are defined in terms of their monopoly on violence within a given territory, most definitions of terrorist organisations specify that terrorist groups must be non-state actors. If a state military or security service could also be defined as a terrorist group, then the term would hinge on normative or moral judgements about the legitimacy of a given regime and how it exercises violence.[9] In addition, other categories exist (such as war crimes) for when states illegitimately use violence.

Terrorism', 2005; see also European Parliament Members' Research Service, 'Understanding Definitions of Terrorism', November 2015.

6. Boaz Ganor, 'Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter?', *Police Practice and Research – An International Journal* (Vol. 3, No. 4, 2002), pp. 287–304.
7. For a fuller overview of the arguments and discussions related to the five criteria listed in this paper, see Bruce Hoffman, *Inside Terrorism* (New York, NY: Columbia University Press, 2002), pp. 38–41.
8. For example, see *Human Rights Watch*, 'China: Draft Counterterrorism Law a Recipe for Abuses', 20 January 2015.
9. This, for instance, is precisely the problem with the US Department of State's recent designation of the Iranian military's Islamic Revolutionary Guard Corps (IRGC) as a terrorist group. By virtue of its covert foreign operations, the IRGC can plausibly fall under the 'clandestine agents' term of the State Department's definition of terrorism. Yet because the IRGC also carries out conventional military activities, the designation was widely critiqued as being driven primarily by politics and ideology – and, moreover, establishing a dangerous precedent by which foreign countries could designate branches of the US military as a terrorist organisation.

- Non-combatant targets: to distinguish terrorist violence from military violence, terrorist groups are typically defined as non-state actors whose violence deliberately targets civilians and non-combatants. Although the line is blurry in practice, the distinction serves to separate terrorist actors from rebel groups and insurgents that only attack formal militaries.[10]
- Psychological effect: whereas most criminal violence is often directed solely at the immediate victims of a particular crime or attack, terrorist violence deliberately aims to create a psychological effect among a broader community or population. Terrorist actors are therefore commonly defined not only in terms of violence against non-combatant targets, but also intimidation of a target audience.
- Motivation: terrorist actors are also distinguished from gangs and cartels, each of whom also use violence against civilians for the purpose of intimidation, by virtue of their political motivations. Although what counts as political can be ambiguous[11] – indeed, many definitions now refer to 'political, religious, ethnic, or ideological motivations' in order to encompass hate groups that otherwise lack a coherent political vision – the criterion that terrorist actors carry out their violence on behalf of an explicit political or social cause is a nearly universal one.[12]

As scholar of terrorism Brian Phillips has noted, how exactly to define a terrorist group or entity remains an open question.[13] To the extent that there is a consensus about how to define a terrorist actor, it is that they engage in violence or the threat of violence, and that that violence exists in contradistinction to criminal violence, state-led violence and conventional warfare. Technology companies should adopt any definition of terrorist groups that touches on each of those distinctions. For example, one definition might be a slightly revised version of Facebook's definition:[14] 'a terrorist entity is any non-governmental

10. For more on the distinction between terrorists and insurgents, see Assaf Moghadam, Ronit Berger and Polina Beliakova, 'Say Terrorist, Think Insurgent: Labeling and Analyzing Contemporary Terrorist Actors', *Perspectives on Terrorism* (Vol. 8, No. 5, 2014).
11. Another ambiguity occurs when political statements and manifestos can be taken at face value, and when they reflect mental illness. See Jonas R Kunst, Lisa S Myhren and Ivuoma N Onyeador, 'Simply Insane? Attributing Terrorism to Mental Illness (Versus Ideology) Affects Mental Representations of Race', *Criminal Justice and Behavior* (Vol. 45, No. 12, 2018), pp. 1888–1902.
12. For a good discussion on this point, see J M Berger, 'The Difference Between a Killer and a Terrorist', *The Atlantic*, 26 April 2018.
13. Brian J Phillips, 'What is a Terrorist Group? Conceptual Issues and Empirical Implications', *Terrorism and Political Violence* (Vol. 27, No. 2, 2014), pp. 225–42.
14. Facebook defines a terrorist entity as 'any non-governmental organization that engages in premeditated acts of violence against persons or property to intimidate a civilian population, government, or international organization in order to achieve a political, religious, or ideological aim'. See Monika Bickert

actor that engages in violence or the threat of violence against noncombatant persons or property to intimidate, and create a broad psychological effect among, a population, government, or international organization in order to achieve a political, religious, ethnic or ideological aim'.

Lists

As challenging as it can be to define what terrorists are, compiling a list of terrorist actors can be even more so. For technology firms operating at a global scale, such a list needs to meet three requirements:

1. It should be unbiased, in the sense that all entities that meet a particular definition are equally likely to appear on the list regardless of ideology or identity.
2. It should be global. If a list is unbiased but only covers one country or region, it will be of limited use to social networks and file-sharing platforms with a global userbase.
3. It should be updated in near real time. Since many high-profile attacks, such as the Christchurch shooting, are carried out by actors and individuals that are previously unknown to police,[15] the list should be constantly monitored in order to include new groups and causes.

Unfortunately, producing a list that is unbiased, global and real time is not a trivial task. A single expert or scholar of terrorism can devise a reasonable definition of 'terrorist' in relatively short order. By contrast, a well-vetted, real-time list of terrorist entities requires a team of researchers with a wide range of local and regional expertise to monitor the emergence and behaviour of terrorist actors and groups in every country. The expense of such a team – up to several million dollars per year – can be prohibitive for nearly all technology companies.[16]

---

and Brian Fishman, 'Hard Questions: How Effective Is Technology in Keeping Terrorists off Facebook?', Facebook, 23 April 2018.

15. In addition to Christchurch, the Utoya, Norway and Sousse, Tunisia attacks were also carried out by previously unknown individuals. See Tom Blackwell, 'How a Racial Terrorist Unknown to Police Carried Out a Shocking Massacre in New Zealand', *National Post*, 15 March 2019; Johan Ahlander and Victor Klesty, 'Norway Killer Unknown to Police, Criticized Islam', *Reuters*, 23 July 2011; Jessica Elgot, 'Deadly Attack on Tunisia Tourist Hotel in Sousse Resort', *The Guardian*, 26 June 2015.
16. The winning bid for the most recent Department of Homeland Security grant for a global terrorism database had a proposed budget of over $10 million. See US Government Accountability Office, 'University of Maryland', B-416682, 24 October 2018.

Table 1: Terrorist Designation List Typology

	Unbiased	Global	Real Time
Academia	Yes	Yes	No
Civil Society	No	No	Yes
Government	No	Yes	No

Faced with such a cost, even large companies have turned to designation lists released publicly by academia, civil society and government.[17] Yet those lists were not designed for the needs of a global technology company. Most lists published by academia, civil society and government satisfy one or two criteria for use by a global technology company, but none meet all three. Companies that use off-the-shelf lists should understand the specific limitations of each.

Academic Lists

The advantage of academic datasets of terrorist organisations is their rigour and objectivity. Since both their data and data-collection processes are peer reviewed, academic datasets of terrorist actors are far more likely to be unbiased than those produced by governments or advocacy organisations.[18]

However, for the technology sector academic lists have several drawbacks. The first is the tradeoff between timeliness and global coverage. The most detailed dataset on terrorist organisations worldwide is the recently released Extended Data on Terrorist Groups dataset, which is based on groups cited in the Global Terrorism Dataset (GTD).[19] However, while the Extended Data on Terrorist Groups is both unbiased and global, it is not timely: despite being released in 2019, the Extended Data on Terrorist Groups data only

17. Microsoft, Twitter and YouTube have all publicly stated that they use government lists. Although they are required to use some of these lists – each is legally obliged to ban groups listed on the Foreign Terrorist Organization list, for example – they are not unbiased and are insufficient for global coverage. For more on how each company uses government lists, see Microsoft Corporate Blogs, 'Microsoft's Approach to Terrorist Content Online', 20 May 2016; Twitter, 'Terrorism and Violent Extremism Policy', March 2019; YouTube, 'Transparency Report: Featured Policies', March 2019.
18. For a good overview of available academic datasets, see Neil G Bowie, 'Terrorism Events Data: An Inventory of Databases and Datasets, 1968-2017', *Perspectives on Terrorism* (Vol. 11, No. 4, 2017); Neil G Bowie, 'Terrorism Databases and Data Sets: A New Inventory', *Perspectives on Terrorism* (Vol. 12, No. 5, October 2018).
19. Dongfang Hou, Khusrav Gaibulloev and Todd Sandler, 'Introducing Extended Data on Terrorist Groups (EDTG), 1970 to 2016', *Journal of Conflict Resolution* (June 2019). DOI:10.1177/0022002719857145.

runs to 2016; technology companies that rely on it will not identify the many terrorist groups and actors that have emerged since then. By contrast, the Armed Conflict Location and Event Data Project, which produces weekly data on conflict events worldwide, offers timely data that can be used to monitor the emergence of terrorist groups. However, it does not yet cover North and South America and much of Asia.[20]

A second drawback of academic datasets concerns their sustainability over time. As discussed above, global datasets of terrorist groups can be expensive to produce, and academic datasets often rely on government funding, which is typically distributed via short-term contracts that may not be renewed. For example, the GTD, arguably the most well-known and widely used terrorism dataset, was recently informed that its primary funding would not be renewed.[21] Technology companies seeking to build a long-term solution to terrorist account moderation should evaluate the sustainability of a given dataset before incorporating it into their own moderation processes.

Civil Society Lists

Civil society organisations often do an excellent job of tracking particular forms of terrorism and extremist groups. In the US, for example, the Anti-Defamation League (ADL) and the Southern Poverty Law Center (SPLC) both house leading terrorism researchers and consistently produce rigorous data on terrorist and extremist attacks and groups.[22]

One advantage of civil society organisations is that they often have the resources and incentive to monitor attacks in real time.[23] However, civil society groups are not suitable for exclusive use by technology companies for two reasons. The first is that no civil society organisation produces a

20. The Armed Conflict Location and Event Data Project (ACLED) also illustrates another problem with academic datasets: many of them are focused on political violence in general, rather than terrorism specifically. Technology companies that rely on data from ACLED and similar projects, such as the Social Conflict in Africa Dataset or the Uppsala Conflict Data Project, will still need to decide which groups in the dataset meet their definition of terrorist entities.
21. See US Government Accountability Office, 'University of Maryland'. An additional concern with government funding of academic datasets is that the funding may depend on political considerations. For instance, the GTD may have been defunded for revealing a rise in far-right terrorism domestically. See Emily Atkin, 'A Database Showed Far-Right Terror on the Rise. Then Trump Defunded It', *New Republic*, 3 January 2019.
22. See Anti-Defamation League (ADL), 'ADL H.E.A.T. Map- Hate, Extremism, Anti-Semitism, Terrorism'; Poverty Law Center, Extremist Files, 'Groups'; Southern Poverty Law Center, 'Hate Map'.
23. For example, see the ADL H.E.A.T. Map cited above, which tracks extremist and anti-Semitic incidents in the US and is frequently updated as incidents occur.

comprehensive terrorist organisation list at a global scale: most civil society organisations instead have a local or national focus, which is of limited use for companies with global networks of users. The second reason is that when civil society organisations compile lists of violent actors, they will invariably reflect the mission and advocacy of the organisation and its donors. Befitting their history and aim, both the ADL and SPLC focus on extremism as well as terrorism, and release data on groups and individuals that espouse extremist rhetoric but do not necessarily call for or carry out violent attacks.[24]

Civil society organisations' datasets can offer a valuable resource for technology companies in need of real-time monitoring of extremist violence. However, they are generally too geographically constrained to offer a turnkey solution for global technology companies seeking to identify terrorist accounts across their platform or service.

Government Lists

The main advantage of government lists is that they are both transnational and well resourced.[25] In contrast to academic and civil society organisations, governments are not dependent on outside sources of funding and therefore have greater resources to vet terrorist organisations. In addition, many have access to classified information that can provide valuable information on the purpose of a group and its activities.

However, that does not mean the lists are unbiased.[26] Most notoriously, authoritarian and illiberal regimes often use designation lists to target dissidents and human rights activists under the pretext of counterterrorism. During the Syrian uprising in 2011 and 2012, for instance, the Assad regime frequently described legitimate opposition protestors as terrorists.[27] Likewise, in China, the government has leveraged the actual terrorism of the

24. The subjective nature of what qualifies as 'extremist' rhetoric can also lead to allegations of bias. The SPLC list, for example, became the subject of considerable controversy when it included Maajid Nawaz, a former Islamist turned counter-extremist, on a list of anti-Muslim extremists. See David A Graham, 'The Unlabelling of an "Anti-Muslim" Extremist', *The Atlantic*, 18 June 2018.
25. Technology companies are also legally obliged to comply with many of the designation lists produced by the countries in which they operate. As a result, another advantage of government lists is that the cost of global compliance with each list should be relatively low.
26. For more on the biases involved, see Colin Beck and Emily Miner, 'Who Gets Designated a Terrorist and Why?', *Social Forces* (Vol. 91, No. 3, 2013), pp. 837–72.
27. See *Al Jazeera*, 'Scores Killed on Syria's "Day of Rage"', 20 April 2011; Khaled Yacoub Oweis, 'Assad: Syria Won't Stop Fight Against "Terrorists"', *Reuters*, 9 August 2011; Anthony Shadid, 'Syrian Leader Vows "Iron Fist" to Crush "Conspiracy"', *New York Times*, 10 January 2012.

East Turkestan Islamic Movement and other Uighur terrorist groups to target non-violent Uighur dissidents too. For example, in addition to designating the East Turkestan Islamic Movement as a terrorist group, Beijing has also designated the World Uighur Congress, an NGO of exiled Uighurs that is critical of the Chinese Communist Party, as a terrorist organisation.[28] Within autocratic regimes, terrorist designation lists are a key instrument in the authoritarian toolkit; they will often skew or even manufacture data to support their capacity for repression.[29] As a result, it is often difficult – if not impossible – to ascertain which designations are legitimate and which are the result of illiberal motivations.

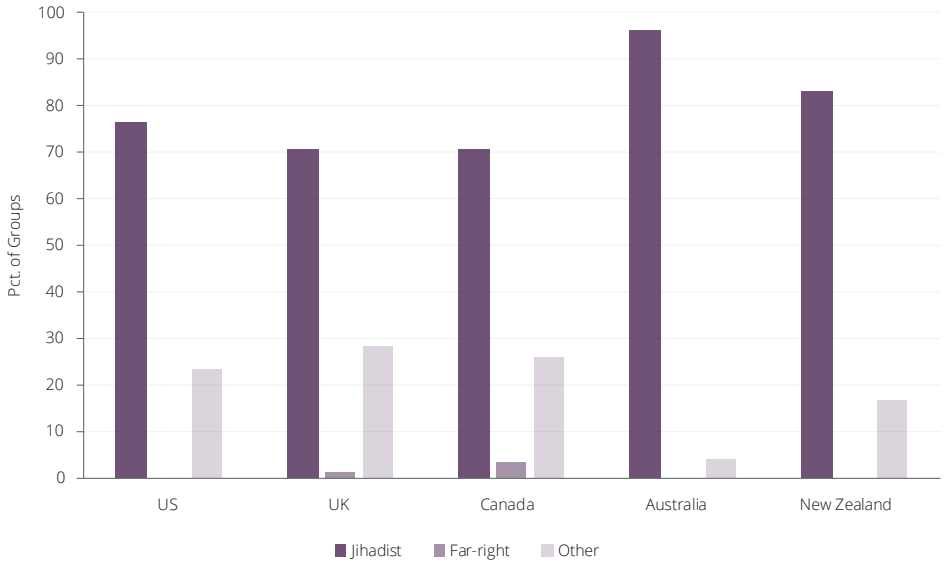
By contrast, democratic governments typically have oversight mechanisms in place to ensure that groups designated as terrorist entities actually engage or support terrorism. However, that does not mean the resulting designation lists are unbiased. Since the terrorist designation process involves considerable transaction costs, ushering a group through that process requires a strong political incentive or motive. The result is that not all actors and organisations that meet the definition of a terrorist group are equally likely to appear on a designated terror group list.[30]

For example, consider the main designation lists of the UK, the US, Canada, Australia, and New Zealand.[31] Known as the Five Eyes, the countries all have similar values, political institutions and definitions of terrorist groups. Their intelligence services also routinely share information about terrorist groups worldwide. If the designation process was globally unbiased, one would expect to see very similar lists. Further, one would also expect that the number of groups with a given ideology should be roughly proportionate to the level of violence perpetrated by adherents to that ideology.

---

28. Murray Scot Tanner with James Bellacqua, 'China's Response to Terrorism', *CNA*, June 2016.
29. *Ibid*.
30. For more on the non-representative nature of different designation lists, particularly the US's Foreign Terrorist Organization (FTO) list, see Phillips, 'What is a Terrorist Group?', pp. 234–36.
31. Several countries maintain multiple designation lists and use them for different purposes. The US, for instance, produces both the FTO list pursuant to the Nationality and Immigration Act, as well as the Specially Designated Terrorist Groups list pursuant to Executive Order 13244. The former is maintained solely by the State Department and includes only organisations, while the latter is maintained by both the State Department and the Treasury Department and includes both individuals and organisations. For the sake of comparison, only organisational lists were compared. See Terrorist Designations, 'Five Eyes Comparison', <https://www.terroristdesignations.org/five-eyes/>, accessed 18 July 2019.

Figure 1: Five Eyes Terrorist Designations by Ideology

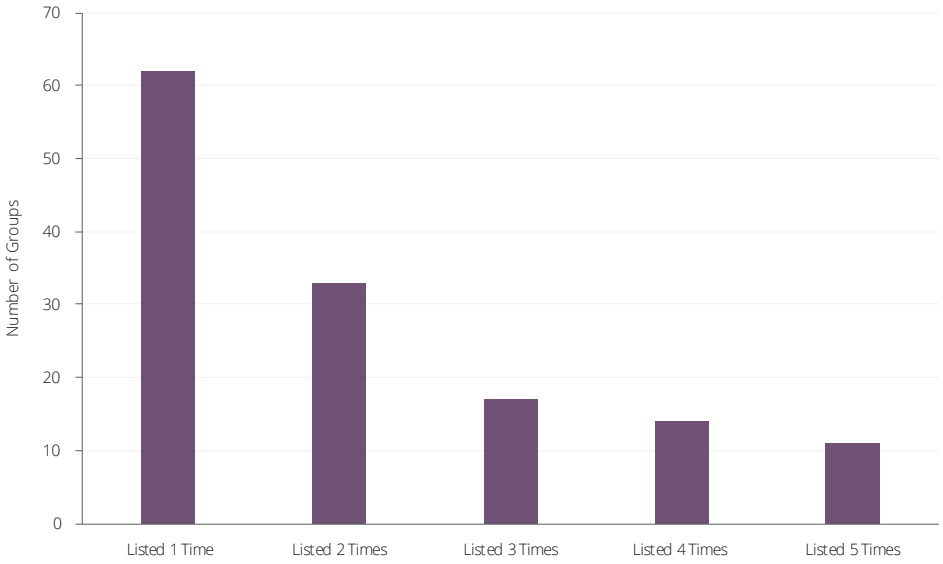


Source: The Authors.

Yet the lists do not comport with either expectation. As Figure 1 shows, despite the global prevalence of far-right terrorism,[32] far-right groups comprise a tiny fraction of designated terrorist groups.[33] In fact, there are only three far-right groups across all the lists – two of which were only added by Canada in June 2019.[34] Technology companies that rely exclusively or primarily on government designation lists will thus miss most of the far-right groups using their platforms and services.

32. For a roundup of empirical data on far-right terrorism, see Ben Butcher and Micah Luxen, 'How Prevalent is Far-Right Terrorism?', *BBC*, 19 March 2019.
33. Data on far-right and jihadist/Islamist groups was compiled by the authors and is available at Terrorist Designations, 'Five Eyes Comparison'.
34. Daniel LeBlanc, 'Canada Adds Two Neo-Nazi Groups to List of Terrorist Organizations', *Globe and Mail*, 26 June 2019.

Figure 2: Joint Designations Across Five Eyes Lists



Source: The Authors.

Even more, the lists are not nearly as similar as they should be. Figure 2 shows how many groups are listed once, twice or more across all Five Eyes lists. A list that was comprehensive and unbiased should skew to the right. Instead, Figure 2 skews to the left, with nearly half of all groups appearing on only one list and only 11 groups appearing across all five lists.[35]

Further, several of the groups that do appear on all five lists illustrate how the lists can be driven by political concerns. Consider Hamas, Palestinian Islamic Jihad (PIJ), and the Kurdistan Worker's Party (PKK). Although each group has carried out a major terrorist attack and thus should be designated, so too have numerous other groups, such as Abu Sayyaf in the Philippines or the East Turkestan Islamic Movement in China, which are not jointly designated. What Hamas, the PIJ and the PKK likely share in common is the efficacy with which their adversary governments were able to negotiate their inclusion on terrorist designation lists. For instance, the US recently

35. There are 11 joint groups only if New Zealand is coded as having designated Al-Qa'ida, the Islamic State, Al-Nusrah, Boko Haram, Hizbullah and Jemaah Islamiya by virtue of their inclusion on the UN sanctions list pursuant to Resolutions 1267, 1989 and 2253. If those groups are not included, the number of jointly designated groups drops to five: Hamas; Palestinian Islamic Jihad (PIJ); Kurdistan Workers Party; Al-Shabaab; and ISIL-Sinai. Including the UN designated groups is a conservative coding decision because New Zealand explicitly designated Hamas and the PIJ, even though they are also on the UN list, which implies that its designation process is independent of the UN's. For more on the New Zealand case, see Terrorist Designations, 'Five Eyes Comparison'.

re-designated the PKK as a terrorist organisation during negotiations with Ankara over several related security issues, including US support for PKK-linked forces in northern Syria and the sale of a Patriot missile system.[36] Far from being a purely academic exercise, designation on a terrorist list is a political act that can be used as leverage in bilateral negotiations. The resulting designation lists reflect in part the political interests and incentives that guide those negotiations.

Finally, just as national governments struggle to produce global and apolitical lists, so too do international governmental organisations like the UN. The UN has produced two designation lists that technology companies already rely on. The first is a sanctions list of entities affiliated with Al-Qa'ida, the Taliban and the Islamic State, which the UN compiles pursuant to Resolutions 1267, 1989 and 2253.[37] By definition, this list is explicitly biased towards those three groups. The second is the United Nations Security Council Consolidated Sanctions List, which includes but is not limited to terrorist actors.[38] Exclusive use of either list for terrorist designation by technology companies creates problems: the former because it is biased towards three specific organisations, the latter because it includes many groups that have never engaged in terrorism.

Conclusion and Recommendations

For technology companies with global reach, responding to terrorist groups online remains a daunting challenge. Very few have the competence to produce a rigorous definition of what a terrorist is, much less a terrorist designation list that is unbiased, global in scope and updated in real time. Yet there are also no third-party terrorist definitions and designation lists that meet those criteria either.

36. Joyce Karam, 'US Renews Designation of PKK as Terrorist Organization', *The National*, 2 March 2019.
37. Technically, these are now separate lists, pursuant to UN Security Council Resolution 1989 (2011). However, since the Al-Qa'ida and Taliban lists were originally compiled together, they are commonly referred to as one list. For more background on them, see United Nations Security Council, Sanctions Committee, 'Security Council Committee Pursuant to Resolutions 1267 (1999) 1989 (2011) and 2253 (2015) Concerning ISIL (Da'esh) Al-Qaida and Associated Individuals Groups Undertakings and Entities'.
38. United Nations Security Council, 'United Nations Security Council Consolidated List'.

The following policies are therefore recommended:

- Technology companies should define terrorist entities in a way that distinguishes them from non-violent dissidents, state actors, conventional rebel groups, and criminals or criminal syndicates.
- Technology companies should use government designation lists with caution, since even the lists compiled by democratic governments are more likely to include some terrorist groups but not others.
- The technology sector and representatives from civil society, academia and government should work together to develop a global, unbiased and real-time database of possible terrorist entities. The database could be used to produce different designation lists based on various inclusion criteria.

Chris Meserole is a Fellow in the Foreign Policy Program at the Brookings Institution.

Daniel Byman is a Professor and Vice Dean in the School of Foreign Service at Georgetown University and a Senior Fellow at the Center for Middle East Policy at the Brookings Institution.

The authors would like to thank Israa Saber and Malika Mehrotra for research assistance.

About RUSI

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

About The Global Research Network on Terrorism and Technology

The Global Research Network on Terrorism and Technology is a consortium of academic institutions and think tanks that conducts research and shares views on online terrorist content; recruiting tactics terrorists use online; the ethics and laws surrounding terrorist content moderation; public–private partnerships to address the issue; and the resources tech companies need to adequately and responsibly remove terrorist content from their platforms.

Each publication is part of a series of papers released by the network on terrorism and technology. The research conducted by this network will seek to better understand radicalisation, recruitment and the myriad of ways terrorist entities use the digital space.

The network is led by the Royal United Services Institute (RUSI) in the UK and brings together partners from around the world, including the Brookings Institution (US), the International Centre for Counter-Terrorism (Netherlands), Swansea University (UK), the Observer Research Foundation (India), the International Institute for Counter-Terrorism (Israel), and the Institute for Policy Analysis of Conflict (Indonesia).

The research network is supported by the Global Internet Forum to Counter Terrorism (GIFCT). For more information about GIFCT, please visit https://gifct.org/.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)