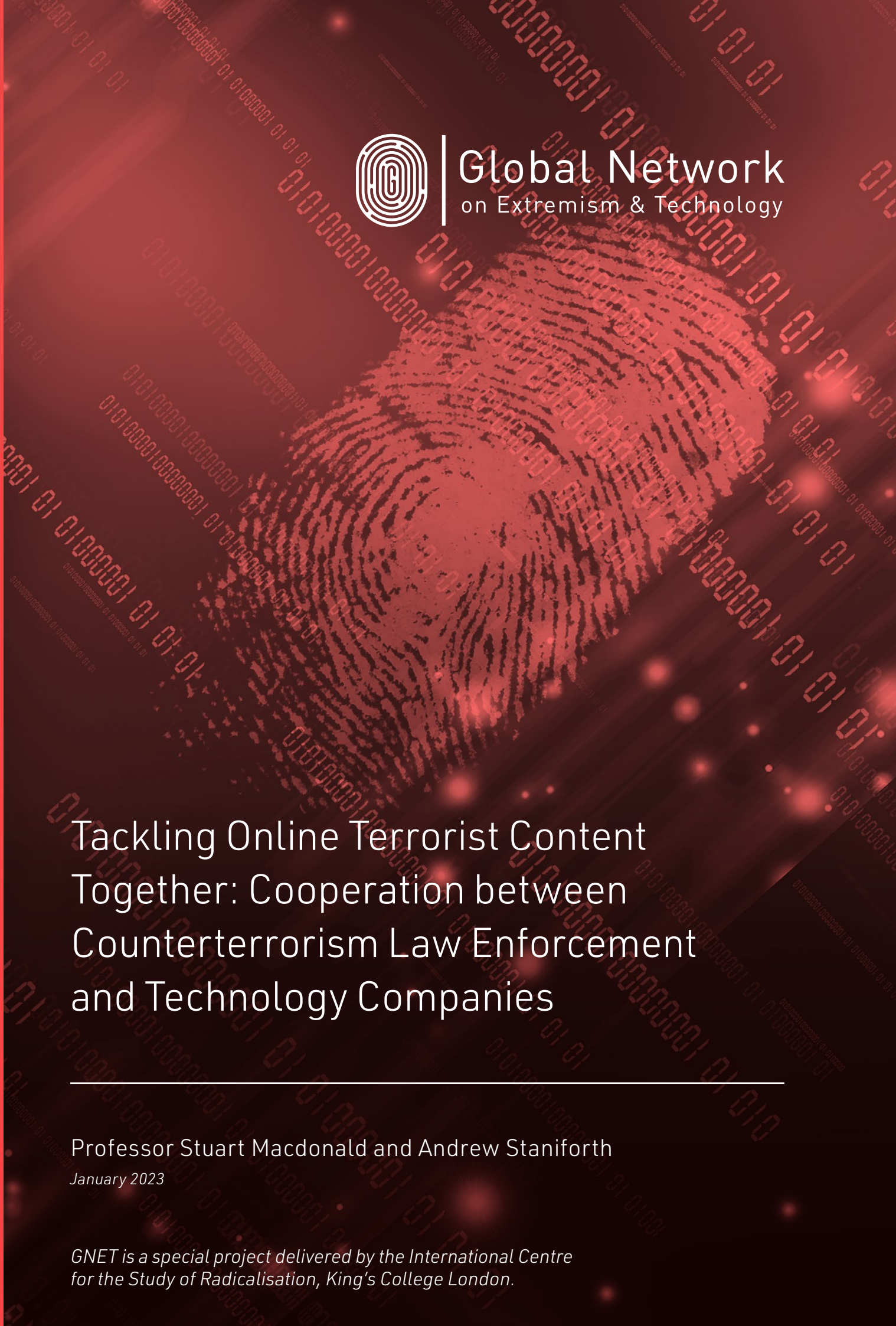

Global Network
on Extremism & Technology

Tackling Online Terrorist Content Together: Cooperation between Counterterrorism Law Enforcement and Technology Companies

Professor Stuart Macdonald and Andrew Staniforth

January 2023

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The authors of this report are Professor Stuart Macdonald and Andrew Staniforth

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Recommended citation:
Macdonald, Stuart, and Andrew Staniforth. "Tackling Online Terrorist Content Together: Cooperation between Counterterrorism Law Enforcement and Technology Companies." London: Global Network on Extremism and Technology (GNET), January 2023. https://doi.org/10.18742/pub01-110.

Executive Summary

Cooperation between law enforcement and tech companies is widely regarded as necessary to tackle online terrorist content. Both sectors have publicly stated their commitment to working together and there are examples of mutual cooperation. Yet there are also impediments to such collaboration, including different cultures and operating practices, and there have been high-profile instances of non-cooperation. The informality of existing collaborations has also led to concerns about censorship, mission creep and a lack of accountability and oversight.

The focus of this report is on how to resolve the impediments to closer cooperation between law enforcement and the tech sector in order to realise the benefits of mutual collaboration, while simultaneously addressing concerns about due process and accountability. The report utilises an interview-based methodology to examine the experiences and opinions of personnel from both sectors who have first-hand experience of mutual cooperation. It provides empirically grounded insights into this under-researched topic.

The report's findings are organised around four themes:

- Shared appreciation of the threat: Participants from both sectors emphasised the importance of tackling online terrorist content. From a law enforcement perspective, this stemmed from a conviction that such content has an important influence in practice, whereas tech sector participants emphasised the growing range of online services and the increasing sophistication and secrecy of the online activities of terrorists.

- Progress to date: Interviewees described how initial attempts at cross-sector collaboration had been difficult. Reasons for this included different ideological cultures, an absence of established channels for communication or cooperation, and differing expectations. The key catalysts for change were the significant presence on Twitter of Islamic State during the period between 2013 and 2015 and the Christchurch attacks of 2019. Participants described how major tech companies began to invest more heavily in the removal of terrorist content, including the recruitment of personnel from a policing background, while law enforcement began to deliver specific training on cooperation with social media companies.

- Current challenges: Participants stressed that tensions remain. Law enforcement interviewees expressed frustration at the length of time it can take for requests to be resolved and at a perceived failure by tech companies to incorporate safeguards into the design of new technologies. The chief concern expressed by tech sector interviewees was the process by which law enforcement referrals were and are made and the tenuous link to terrorism of some of the referrals received.

- Next steps: Given the different objectives and challenges faced by law enforcement and the tech sector, our participants felt that the most important priority in advancing cross-sector cooperation was increasing mutual understanding. Three specific measures were suggested to achieve this: clear channels of communication; greater information-sharing; and dedicated training and recruitment.

The report concludes with four recommendations aimed at resolving the impediments to closer cooperation between law enforcement and the tech sector while simultaneously addressing concerns about due process and accountability. These are: the development of an experience exchange programme; the implementation of a takedown-shutdown counterterrorism policing protocol; a joint upstreaming programme founded on a proactive preventative ethos; and the development of joint strategic research requirements.

Contents

1 Introduction

The dissemination of propaganda online is a strategic priority for terrorist groups.[1] Terrorist groups and their sympathisers post an enormous volume of content, such that in the year up to September 2022 Facebook had removed a total of 54 million items of terrorist content.[2] In the same time period, YouTube removed 273,016 videos that promoted violence and violent extremism,[3] while in 2021 Twitter suspended a total of 112,360 accounts for the same reason.[4] The dissemination of terrorist content is not confined to the biggest platforms nor is terrorist exploitation of online platforms limited to social media. A variety of other services are also exploited.[5] For example, from December 2020 to November 2021, Tech Against Terrorism alerted 65 different tech companies to terrorist content on their platforms. These spanned 13 different service types, including file-sharing, archiving, link shortening, book subscriptions and web hosting.[6]

For more than a decade, stakeholders have emphasised the importance of public-private partnership in tackling terrorists' use of the Internet, particularly cooperation with tech companies.[7] Tech companies have publicly stated their commitment to cooperation with law enforcement and vice versa.[8] Law enforcement in several countries has established specialist units,[9] who work to identify online terrorist content and refer it to the host platform for removal.[10] The UK's Counter-Terrorism Internet Referral Unit (CTIRU), established by the UK Metropolitan Police in 2010, contributed to the removal of 310,000 pieces of content during its first eight years.[11] Following the CTIRU model, the EU's Internet Referral Unit (EU IRU) was established in 2015.[12] Europol describes

1 Anne Aly, Stuart Macdonald, Lee Jarvis, and Thomas Chen, eds., *Violent Extremism Online: New Perspectives on Terrorism and the Internet* (Abingdon: Routledge, 2016).
2 "Dangerous Organizations: Terrorism and Organized Hate," Community Standards Enforcement Report, Facebook, accessed 9 December 2022, https://transparency.fb.com/data/community-standards-enforcement/dangerous-organizations/facebook/#content-actioned.
3 "YouTube Community Guidelines Enforcement," Google Transparency Report, Google, accessed 9 December 2022, https://transparencyreport.google.com/youtube-policy/removals?hl=en_GB&videos_by_reason=period:2021Q4&lu=videos_by_reason.
4 "Rules Enforcement," Transparency, Twitter, accessed 9 December 2022, https://transparency.twitter.com/en/reports/rules-enforcement.html#2021-jan-jun.
5 Stuart Macdonald, Kamil Yilmaz, Chamin Herath, J M Berger, Suraj Lakhani, Lella Nouri and Maura Conway, *The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German & French Far-Right Online Ecosystems* (Washington, DC: RESOLVE Network, 2022), https://doi.org/10.37805/remve2022.
6 "Transparency Report: Terrorist Content Analytics Platform, Year One: 1 December 2020 – 30 November 2021" (London: Tech Against Terrorism, 2022), https://www.techagainstterrorism.org/wp-content/uploads/2022/03/Tech-Against-Terrorism-TCAP-Report-March-2022_v6.pdf.
7 See, for example, United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes* (Vienna: UNODC, 2012); Mubaraz Ahmed, "Impact of Content," in *Extreme Digital Speech: Contexts, Responses and Solutions*, edited by Bharath Ganesh and Jonathan Bright (VOX-Pol Network of Excellence, 2019), 41–52, https://www.voxpol.eu/download/vox-pol_publication/DCUJ770-VOX-Extreme-Digital-Speech.pdf.
8 "How Meta works with law enforcement", Meta, accessed 13 December 2022, https://transparency.fb.com/en-gb/policies/improving/working-with-law-enforcement; Monika Bickert and Brian Fishman, "Hard Questions: How We Counter Terrorism", Meta, accessed 13 December 2022, https://about.fb.com/news/2017/06/how-we-counter-terrorism/.
9 Zoey Reeve, "Repeated and Extensive Exposure to Online Terrorist Content: Counter-Terrorism Internet Referral Unit Perceived Stresses and Strategies", *Studies in Conflict & Terrorism* (2020), https://doi.org/10.1080/1057610X.2020.1792726.
10 Across GIFCT member companies, there is no common approach to defining terrorist content (Katy Vaughan, *The Interoperability of Terrorism Definitions* (Washington, DC: GIFCT, 2022), https://gifct.org/wp-content/uploads/2022/07/GIFCT-22WG-LF-TVEC-1.1.pdf). While the human rights impact assessment of GIFCT's strategy, governance and operations stopped short of recommending the adoption of a shared definition, it did recommend the development of a "common understanding" of the term terrorist and violent extremist content (BSR, *Human Rights Assessment: Global Internet Forum to Counter Terrorism* (BSR, 2021), https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf, 35).
11 "Together we're tackling online terrorism," Counter Terrorism Policing, accessed 9 December 2022, https://www.counterterrorism.police.uk/together-were-tackling-online-terrorism/.
12 "EU Internet Referral Unit – EU IRU: Monitoring terrorism online," Europol, accessed 9 December 2022, https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru.

cooperation with tech companies as a strategic priority, the aim being to exchange best practices and specific measures to improve the referral process and content moderation.[13] One example of cooperation is EU IRU Referral Action Days, which have been organised in collaboration with various companies including SoundCloud,[14] Internet Archive,[15] Telegram,[16] Google and Facebook.[17]

Nonetheless, there are impediments to close cooperation. Tech companies and law enforcement have very different cultures and operating practices. There have been high-profile instances of non-cooperation.[18] Concerns have also been raised about the informality of existing collaborations.[19] To guard against the possibility of censorship, mission creep and a lack of accountability and oversight, there have been calls for all requests submitted to tech companies from state authorities to be subjected to rigorous scrutiny, accompanied by detailed reporting requirements to ensure transparency.[20]

The policy challenge is to address the impediments to cooperation between law enforcement and the tech sector in order to achieve the collaboration that is widely accepted as necessary to tackle online terrorist content, while ensuring that such cooperation meets the demands of due process and accountability. This challenge is the focus of this report. Utilising an interview-based methodology, the report explores the experiences and opinions of key personnel from the law enforcement and tech sectors who have first-hand experience of collaboration between the two communities. By doing so, the report offers a unique, empirically grounded contribution to the relatively thin existing academic research on this topic.

The report begins with a description of the research methodology, followed by a presentation of the findings, organised into four themes: shared appreciation of the threat; progress to date; current challenges; and next steps. Following discussion, the report concludes by advancing a set of mutually beneficial recommendations, focused on: embedding personnel from law enforcement and the tech sector within each other's counterterrorism operational functions; improving the oversight and transparency of current referral processes; enhancing the value of threat assessments and intelligence insights; and the identification of strategic research requirements.

13 EU Internet Referral Unit, "2021 EU Internet Referral Unit Transparency Report", Europol, accessed 13 December 2022, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_IRU_Transparency_Report_2021.pdf.

14 "Terrorist and extremist chants used to woo recruits – focus of latest Europol Referral Action Day", Europol, accessed 13 December 2022, https://www.europol.europa.eu/media-press/newsroom/news/terrorist-and-extremist-chants-used-to-woo-recruits-%E2%80%93-focus-of-latest-europol-referral-action-day.

15 "Jihadist content targeted on Internet Archive platform", Europol, accessed 13 December 2022, https://www.europol.europa.eu/media-press/newsroom/news/jihadist-content-targeted-internet-archive-platform.

16 "Europol and Telegram take on terrorist propaganda online", Europol, accessed 13 December 2022, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

17 "EU law enforcement and Google take on terrorist propaganda in latest Europol Referral Action Days", Europol, accessed 13 December 2022, https://www.europol.europa.eu/media-press/newsroom/news/eu-law-enforcement-and-google-take-terrorist-propaganda-in-latest-europol-referral-action-days; "EU law enforcement joins together with Facebook against online terrorist propaganda", Europol, accessed 13 December 2022, https://www.europol.europa.eu/media-press/newsroom/news/eu-law-enforcement-joins-together-facebook-against-online-terrorist-propaganda.

18 Most notably, the Apple-FBI encryption dispute: Lev Grossman, "Inside Apple CEO Tim Cook's Fight with the FBI", *Time*, 17 March 2016, https://time.com/4262480/tim-cook-apple-fbi-2/.

19 "Europol: Delete criminals' data, but keep watch on the innocent", EDRi, accessed 13 December 2022, https://edri.org/our-work/europol-delete-criminals-data-but-keep-watch-on-the-innocent/; "Europol: Non-accountable cooperation with IT companies could go further", EDRi, accessed 13 December 2022, https://edri.org/our-work/europol-non-accountable-cooperation-with-it-companies-could-go-further/.

20 Danielle Keats Citron, "Extremist Speech, Compelled Conformity, and Censorship Creep," *Notre Dame Law Review* 93, no. 3 (2018): 1035–72; Evelyn Douek, "The Rise of Content Cartels", Knight First Amendment Institute at Columbia University, accessed 13 December 2022, https://knightcolumbia.org/content/the-rise-of-content-cartels.

2 Methodology

To understand how law enforcement and tech companies coordinate to tackle online terrorist content, we conducted semi-structured interviews of professionals from four key sectors: law enforcement; tech companies; NGOs; and subject experts. This section outlines the three core stages of our research methodology: participant selection; interview structure; and data coding and analysis.

Before embarking on the research, full ethical approval was received from Swansea University. Issues addressed as part of this process included: potential risks to the participants and researchers; arrangements for ensuring participants' informed consent; and data storage and security. One-to-one interviews were conducted and recorded online. Informed consent was obtained beforehand and confirmed at the start of the interview. In order to ensure that potential interviewees felt able to participate and to speak openly and freely, we undertook steps to ensure anonymity – unless participants chose to be explicitly named (which none did).

Participant Selection

We selected participants who could offer unique access and insights from different perspectives of tackling online terrorist content from four sectors: law enforcement, tech companies, NGOs and subject experts. To produce authoritative outcomes, it was important to include a mix of law enforcement agency practitioners working in the field from different jurisdictions and across hierarchical structures. The law enforcement personnel who we interviewed spanned six counterterrorism roles: senior national leaders; heads of intelligence and referral units; team leaders; analysts; investigators; and training coordinators.

To capture the views of tech companies, a range of experts from the tech sector was considered a priority. Moreover, professionals with legislative, regulatory and public policy expertise were considered to have important insights that might inform the research. These interviews were augmented by others with representatives from non-governmental organisations (NGOs) that provide support, guidance and training to stakeholders across the specialist online harms landscape.

In total we interviewed 21 participants. Table 1 outlines the breakdown of participants by sector. Participants were located in seven countries, adding an important international dimension reflecting the borderless, transnational nature of the threat from online terrorist content. The cohort consisted of ten law enforcement interviewees from five countries, five professionals from tech companies, three NGO representatives and three subject experts from academia and public policy with experience of national counterterrorism strategy and legislation.

Table 1: List of interviewees

Identifier	Sector	Duration
LE1	Law enforcement	58 minutes
LE2	Law enforcement	46 minutes
LE3	Law enforcement	54 minutes
LE4	Law enforcement	56 minutes
LE5	Law enforcement	47 minutes
LE6	Law enforcement	56 minutes
LE7	Law enforcement	46 minutes
LE8	Law enforcement	57 minutes
LE9	Law enforcement	55 minutes
LE10	Law enforcement	46 minutes
TS1	Tech sector	45 minutes
TS2	Tech sector	59 minutes
TS3	Tech sector	59 minutes
TS4	Tech sector	48 minutes
TS5	Tech sector	52 minutes
NGO1	NGO	57 minutes
NGO2	NGO	51 minutes
NGO3	NGO	46 minutes
S1	Subject expert	50 minutes
S2	Subject expert	46 minutes
S3	Subject expert	58 minutes

Interview Structure

Given the sensitive operating environment of interviewees, including demands on their time and coronavirus restrictions in place at the initial phases of the project, interviews were conducted online. A set of interview questions was designed to cover participants' experiences of cooperation between law enforcement and the tech sector, the benefits of such cooperation, obstacles to cooperation and suggestions for the future.[21] The questions were provided to all interviewees in advance to aid planning and preparation, as well as

21 The complete interview schedule can be found in the appendix. Where interviewees are referenced in the footnotes, we have chosen to refer to the interviewee by their code, omitting a date of interview for anonymity's sake.

providing the necessary reassurance of the purpose of the interview and the intended reporting of outcomes from their responses. The interview approach and format were designed as an informal discussion, set within a semi-structured framework designed not only to ensure consistency of approach and to elicit the responses required to inform the research but also to allow flexibility and autonomy for the interviewer and interviewee to delve deeper into matters that concerned them from their own experience. The interviews lasted between 45 and 59 minutes.

Data Analysis

All interviews were recorded and later transcribed by the research team. To begin data analysis, both members of the research team analysed the 21 interview transcripts to construct a thematic coding framework inductively. The interview transcripts were then coded by theme. This report focuses on four of these themes: the importance of tackling online terrorist content; the evolution of cooperation between law enforcement and the tech sector; frustrations and challenges; and practical suggestions.

3 Findings

From our interviews, we identified four core themes of relevance to cooperation between law enforcement and the tech sector. The first focused on the importance participants attached to tackling online terrorist content, and the reasons advanced for this, in order to examine the extent to which this was a shared priority. The second was the evolution of cooperation between law enforcement and the tech sector. Most of the participants had worked in this field for a number of years and so were able to discuss changes that had occurred over time and catalysts for these changes. The third focused on frustrations that participants had experienced when engaged in cross-sector collaboration and the challenges that had been overcome, or needed to be. The final theme focused on practical suggestions. Participants offered opinions and ideas on how to enhance further the cooperation between law enforcement and the tech sector. Each of these themes will be examined in turn.

Shared Appreciation of the Threat

Our participants were unanimous in emphasising the importance of tackling online terrorist content. While academic research has warned against simplistic and monocausal explanations for radicalisation,[22] law enforcement interviewees stated that, in their opinion, online terrorist content has an important influence in practice. Comments included: "There isn't much that goes on these days when it comes to serious crime or terrorism that doesn't have a significant technology component, whatever that looks like";[23] "I think social media has a lot to answer for in the radicalisation of individuals in this country and in the world";[24] and "Almost every single individual that we charge and prosecute has a mountain of this material on their devices when they are arrested".[25] This last interviewee acknowledged that "proving a causal link between media and actual violence is very, very difficult", but said that "professional intuition" points to the important practical influence of online terrorist content.[26]

Participants from other sectors also stressed the importance of tackling online terrorist content but offered different underlying reasons. These included the growing range of online services that can be utilised and the increasing sophistication and secrecy of terrorists' online activities:

> *The threat is growing, and the problem is becoming more acute. There are several factors driving this, including the expansion of the Internet and related services, the adoption and adaption of new technology by extremists and terrorist groups leading*

22 Joe Whittaker, "The online behaviors of Islamic state terrorists in the United States", *Criminology & Public Policy* 20, no. 1 (2021): 177–203.
23 LE8.
24 TS1.
25 LE1.
26 LE1.

> *to ever more sophisticated campaigns, and the unintended consequence of successful operations removing harmful content, serving to drive extremists to the deeper and darker corners of the web and to be more creative in how they disguise, upload and reuse content.*[27]

As far as the tech sector is concerned, it is important to add two caveats. First, it is not necessarily the case that our interviewees' organisations are representative of the tech sector in general. It might plausibly be suggested that many other tech companies do not attach as much weight to tackling online terrorist content. In fact, one of our participants suggested that many smaller platforms are unaware of the extent to which their platforms are exploited by terrorist organisations, stating that when they discover the volume of such content, "they always get surprised".[28] Second, as professionals tasked with tackling online terrorist content, it is perhaps unsurprising that our participants emphasised the scale and importance of this task. There were some suggestions from our interviewees that members of the biggest tech companies who do not work in this field may view combating online harms as less of a priority, as shown below.

Progress to Date

A consistent theme in the interviews was the progress that has been made in building cooperation between law enforcement and tech companies. Comments included "in the best place it's ever been",[29] "most of our relationships are good to excellent",[30] "we have a good relationship",[31] "we've developed a much better working relationship",[32] "a very, very good working relationship"[33] and "a huge amount of progress".[34] Interviewees acknowledged that the picture has not always been so positive. They identified various reasons for this, with both sectors bearing some responsibility.

The first reason was different ideological cultures. Within law enforcement, there was "the old culture of counterterrorism where you don't engage with anybody".[35] Meanwhile, the tech sector was resistant to intervention. This stemmed from its "ideological underpinning that they were about free speech and that they were giving the voice to the citizen".[36] The second reason was procedural. There were not established channels for communication or cooperation. One law enforcement interviewee commented, "My recollection is that there was quite a lot of uncertainty about how even to make contact with the companies and generally very little understanding of what could be possible".[37] According to a tech sector interviewee, these difficulties caused tension, resulting in a relationship that was "adversarial … I actually think it wasn't adversarial by choice. It was a product of processes and systems and relationships that were frankly underdeveloped".[38] The third reason was differing expectations.

27 NGO3.
28 NGO2.
29 LE1.
30 LE4.
31 LE5.
32 LE7.
33 LE8.
34 TS2.
35 LE6.
36 LE6.
37 LE7.
38 TS2.

At that time, "law enforcement had a relationship with telcos [telephone communication companies], and they were confused when that relationship wasn't just replicated by technology companies".[39] Together, these three factors combined to produce "two groups of people speaking different languages, not understanding each other, very little empathy and processes that were out of date".[40]

Cooperation between tech companies and law enforcement began to change between 2013 and 2015. This period has been described as Islamic State's "Golden Age" on Twitter.[41] Tech companies and law enforcement began to "realise they can no longer tackle this problem on their own",[42] that cooperation is "really, really useful for both sides"[43] and, most fundamentally, "it's in the interest of everyone to take down terrorist content from their platforms".[44] Our interviewees highlighted two key developments during this time. First, the major tech companies began to "scale up" their efforts to remove terrorist content from their platforms.[45] As well as increasing investment in automated tools, there was also investment in relationship-building with external organisations, including law enforcement,[46] and in the recruitment of personnel with subject matter expertise.[47] The latter included recruiting people with law enforcement or military backgrounds.[48] Second, law enforcement started to deliver training on "the processes that actually set us up to" succeed.[49] One interviewee described a specific training package on cooperation with social media companies:

> *We get together with social media companies where we try to understand their procedures, their point of view on their relationship with law enforcement. We integrate their feedback in our processes and systems, and then we offer this in a more digestible form to go to law enforcement investigators.*[50]

A further catalyst was the 2019 Christchurch attacks. Interviewees recounted how "a senior technical person from Facebook Australia flew to New Zealand and ended up working within the major operations centre within, I think, 36 hours of the event".[51] Having a tech company representative working "under the same roof … made the world of difference to the investigators. They got what they needed and much, much faster … When you're dealing with someone virtually or via email, it just simply isn't the same relationship."[52] According to this interviewee, this close cooperation "shifted our relationship from one that was transactional to one that was transformational".[53]

Participants from both sectors applaud the closer cooperation that has developed. A tech sector interviewee stated: "These relationships have been something that we both invested in over a period of very many years now."[54] Similarly, a law enforcement interviewee said that

---

39 TS2.
40 TS2.
41 Maura Conway, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weir, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts", *Studies in Conflict & Terrorism* 42, nos. 1-2 (2019): 141–60, 150.
42 NGO3.
43 TS3.
44 LE2.
45 TS3.
46 TS3.
47 LE6; TS3.
48 S1.
49 TS2.
50 LE2.
51 LE7.
52 LE8.
53 LE8.
54 TS3.

"the amount of effort social media companies are now putting into improving their technology to take more content down, and the fact that they're open to discussions on regulation and legislation, are tremendous achievements".[55]

The overall sense was thus that significant progress has been made. Central to this was the establishment of working relationships, practices and processes that were underpinned by an ethos that did not initially sit easily with the culture of either sector. It is also telling that the two essential catalysts for greater cooperation involved widespread political, media and public concern about terrorists' exploitation of social media platforms. The impression is that outcry on this scale was necessary to overcome institutional inertia.

Current Challenges

While our participants opined that significant progress has been made, several also emphasised that tensions remain and there is still room for improvement. Interviews revealed that the current challenges for cooperation, when viewed from the perspective either of tech companies or law enforcement, were distinct. This section first details the two key issues that were identified by law enforcement participants: delays in resolving requests; and a perceived failure to incorporate safeguards into the design of new technologies. It then describes the chief concern identified by tech sector interviewees: the content of the referrals they sometimes receive from law enforcement and the process by which these are made.

The first frustration expressed by several of the law enforcement interviewees was the length of time that it can take for requests to be resolved. One described a process of "negotiation" that they found quite frustrating, offering as an example discussion over whether a threat to life was sufficiently imminent.[56] Another interviewee offered a similar example:

> *They genuinely do want to help. But it is then the requests for justification for the action that we're asking to be taken. That's when it becomes challenging and difficult. And in this particular case, we got the impression they wanted to move fast. They really wanted to do it. They saw our point completely. But then the next day, still not deleting the content, and the requests start coming through. What's the legal position on this one? Where are you getting this information from? Can you share the actual intelligence that supports this point of view … That rumbled on for weeks. And eventually we actually withdrew the request because it wasn't going anywhere and had gone beyond the point of being useful to the investigation.*[57]

According to this interviewee, this problem is particularly acute in cases involving terrorism: "I don't think that barging in with counterterrorism suddenly actually gives it any more impetus. In some cases, I think maybe it brings a bit more scrutiny from the company on specific cases. They can be very slow because of that."[58]

55 LE1.
56 LE1.
57 LE3.
58 LE3.

The law enforcement participants who expressed this frustration at delays did also show some empathy, commenting that tech companies have to balance competing considerations. For one interviewee, the desire to scrutinise referrals carefully stemmed from the need to safeguard the reputation of the company: tech organisations "have far less latitude at times to do things … I think they are as sympathetic as they can be. But ultimately … they have to think about the company, the reputation of the company and how that affects the whole business."[59] Others explained that errant takedowns or shutdowns could result in further action being taken: "They have their internal policies and procedures, and they are just as liable that someone could make a claim against them if they start taking people's content down."[60]

As well as scrutinising requests, two further reasons were suggested for companies being slow to respond or failing to do so at all. The first was capacity: the size of content moderation teams in relation to the volume of online content. One interviewee explained that "the turnaround time is often either very, very slow or non-existent, purely because of the volume of things that they get referred to them and they don't have the capacity".[61] While interviewees stated that this is particularly the case for small and medium sized companies (for example, "most of them, except for the really well-established companies, do not have the resources to look at it. They are for profit enterprises and for them, any additional step in production that adds to the cost should be given a lot of thought"[62]), some felt that it was also true of the biggest companies:

> *If we look at the scale of investment in the law enforcement liaison teams, it's tiny. They are overstretched, they're overworked. It takes sometimes weeks for them to respond to you by email for anything other than a standardised request, because the people who are doing it are running all over Europe … It's crazy compared to their investment in other parts of the business.*[63]

The second reason was lack of motivation. According to one interviewee, some companies are "just not interested in cooperating on a voluntary basis … In the US context, they were using the argument that the First Amendment protects freedom of speech and anything that goes on the Internet should be protected".[64] Another suggested that some tech companies do not regard tackling online terrorist content as a priority. This stems from the view, which this interviewee claimed is espoused by academic researchers, that "actually the propaganda wasn't harmful".[65]

The second frustration with the tech sector that law enforcement interviewees expressed was the perceived failure to incorporate safeguards into the design of new technologies. One NGO interviewee commented, "There hasn't been a lot of risk assessment built into the foundation of companies. It's been very reactive traditionally."[66]

---

59 LE4.
60 LE5.
61 LE4.
62 LE2.
63 LE3.
64 LE2.
65 LE9.
66 NGO1.

An example offered by a law enforcement interviewee was "fully end-to-end encrypted services":

> *Why would you want to do that when you know you have the technical capability not to do that? … Why would you still go ahead and do that? It's like allowing a hotel to open up in your hometown in which the only people allowed through the door are criminals and the only people who are not allowed in are law enforcement. Why would you do that to your community?*[67]

Meanwhile, the principal concern that interviewees from the tech sector raised was about the requests they receive from law enforcement. There was a feeling that Internet referral units sometimes make referrals for content that is only tenuously connected to terrorism or is not connected to it at all. According to one interviewee, "Internet referral units can sometimes be diluted because it's an easy way to send a lot of links to tech companies to see what comes down and what stays up".[68] This was attributed to a lack of proper training and skills development. One interviewee suggested that there is a "huge skills and training need if law enforcement is going to become more involved in this kind of content policing, understanding how that is done in a way that is both respectful of British values and freedom of speech, but also, frankly, doesn't waste their time".[69] In the absence of such training, interviewees warned of potential mission creep: "When the Counter-Terrorism Internet Referral Unit was established, as the name suggests, it was meant to be counterterrorism."[70] But now, they claimed, when a person complains that a social media post is offensive, the police will open an investigation: "there seems to have been this kind of culture shift where I think law enforcement don't feel empowered to tell people that just because you don't like it doesn't mean the police should do something about it."[71]

As well as the content of some referrals, tech sector participants also expressed concern about the process by which law enforcement make takedown and shutdown requests:

> *We have had requests to remove content that have, for example, involved individuals in the UK who have not been convicted of any criminal offence. We would sort of sit there saying, 'Well, hang on a minute, if this is a UK person, why are you asking us to shut their account down? Why are you not prosecuting?' And so I think one definite need is to clarify what is the scope of your power to send requests? Like, what are the thresholds they work under?*[72]

For this interviewee, this raised the question whether there should be a "double lock" system, so that judicial approval would be required to submit a request to have an account shut down (similar to the process found in the Investigatory Powers Act 2016). Tech companies are uncomfortable, they suggested, with "law enforcement agencies themselves making determinations of legality without judicial process".[73] Relatedly, another interviewee stated that, while tech companies have invested heavily in transparency reporting, this hasn't been matched

67 LE1.
68 TS3.
69 TS2.
70 TS2.
71 TS2.
72 TS2.
73 TS2.

by law enforcement or governments: "as a direct result of wanting to work more with law enforcement, but not wanting to be crippled by accusations that we were doing this in the dark, we've invested in transparency. What we realise is there isn't equitable transparency on the government side, so there isn't transparency about how many referrals they are making, how they're defining their referral parameters. That's one area where I think we can grow together."[74]

It is important to note the connection between law enforcement concerns about the time taken to respond to referral requests and tech sector concerns about the content of some referrals and the process by which referrals are made. The follow-up requests for information and justification that follow, sometimes slowing the response to some referrals, appear to be a product of the informality of the process and wider concerns about mission creep. Our interviews thus provide empirical support for the concerns about due process and accountability that have been expressed by some commentators. A clearer and more stringent referral process has the potential not only to alleviate such concerns, but also to improve tech sector response times to such requests.

Next Steps

Interviewees identified a number of future priorities in the effort to tackle online terrorist content. In this section we focus on the importance of increasing mutual understanding between the law enforcement and tech sectors, as this was identified as a priority by the greatest number of participants.[75] Three specific measures were suggested to increase mutual understanding: clear channels of communication; greater information-sharing; and dedicated training and recruitment.

From all interviewees, there was a consistent emphasis on the value of increased cooperation between law enforcement and the tech sector. One interviewee remarked that "Both sides have to see the advantage of the collaboration and that both sides can win".[76] At the same time, interviewees pointed out that law enforcement and the tech sector have different objectives and face different challenges. As a result, interviewees emphasised the importance of mutual understanding. In particular, there was a feeling among law enforcement interviewees that tech companies lack an understanding of policing, as the following illustrates:

> *I think that the challenge for certain social media platforms or any online platform really is that they don't necessarily understand what the police's point of view is, where they're coming from, how a request may fit into the bigger picture or even understanding how the content that they're hosting could be used for a terrorist purpose.*[77]

74 TS3.
75 Other priorities identified included:
- Greater investment in AI tools and the provision of technical tools to smaller companies to improve their capacity to comply with regulations on such content (TS4; NGO2).
- Imposing a formal obligation on tech companies to report to law enforcement suspicious activity on their platforms, similar to the system in place in the banking industry (TS1).
- Supporting academic research, since law enforcement personnel lack the time to conduct in-depth analysis. One area of particular interest is evidence of what types of content are most likely to engage and influence people (LE5; LE9).

76 LE10.
77 LE4.

This was echoed by other interviewees, who suggested that tech companies may not understand the "societal impact of what their platforms are … accelerating, amplifying".[78] For this interviewee, "tech companies could learn a lot from law enforcement agencies by listening to them".[79] At the same time, other law enforcement interviewees acknowledged that improvements are needed in how they communicate with the tech sector. One interviewee stated that the police "need to sell a little bit more about what they do and why they do it without giving secrets away or anything like that. But they do need to be more open."[80] Another remarked:

> *More exchanges and more collaboration in terms of understanding one another's business, I think, would be a good thing. I think law enforcement needs to be very clear what it's asking for, why it's asking for it, and probably to do that in ways which make it easier for social media companies to respond, because we can sometimes have a bit of a habit of asking for the universe.*[81]

Interviewees offered several suggestions for how to improve this mutual understanding. First, they urged the importance of clear channels of communication. One interviewee stated, "The biggest thing for me is communication. And if you can either have a named contact or at least a named department to have those conversations with, then that makes that conversation much, much easier."[82] This interviewee explained that over time they had built up good working relationships with the tech sector, such that either side could now simply "pick up the phone".[83]

Second, interviewees from both law enforcement and the tech sector stated that greater sharing of information would improve mutual understanding, in particular shared threat assessments and intelligence insights. According to one interviewee, at present the briefings that law enforcement provide to tech companies "offer little" and are "not much different than what they already know themselves, or may receive from other players in this field, whether from GIFCT, academic research or other NGOs operating in and monitoring this space".[84] This interviewee stated:

> *Tech companies would be better informed if law enforcement authorities shared more in-depth sensitive information and intelligence about what they are seeing and forecasting … To develop true collaboration and cooperation moving forward, authorities need to provide more open access to intelligence and ongoing operations. Of course, this may require individuals to receive higher vetting status to view such material. But this is simply a matter of trust and the way to improve this is to share more, from which I believe will result a more dynamic, collaborative partnership moving forward.*[85]

78 S3.
79 S3.
80 TS1.
81 LE7.
82 LE4.
83 LE4.
84 NGO3.
85 NGO3.

Greater sharing of information is also required from the tech sector, they added: "Of course, tech companies and tech developers should also be more open and upfront about new and emerging technologies and the potential security threats of their use by bad actors."[86]

The final suggestion concerned training and recruitment. Interviewees suggested that companies' trust and safety teams would benefit from more training,[87] including specific training on how to interact and cooperate with law enforcement.[88] The value to tech companies of recruiting individuals from a law enforcement or military background was also emphasised. According to one interviewee, the biggest tech companies need computer scientists, but they also "need cohorts of investigators, some of whom will be former police officers".[89] An additional suggestion was to embed law enforcement colleagues in (or second them to) tech companies. One law enforcement interviewee commented, "Personally, I would like to send a data scientist there to work with them. That is something that we would love to do. It would have real benefits to us."[90] Another agreed, stating that "It would just strengthen the relationships at a strategic level if we were able to do that … Maybe the next level is to actually put somebody who's still employed by the police into those organisations. It's pretty radical, but I don't see why it can't happen."[91]

86 NGO3.
87 NGO2.
88 LE2.
89 S1.
90 LE3.
91 LE8.

4 Discussion

The findings of this research provide unique insights into the context and operating environment of members of law enforcement and tech companies engaged in the highly specialised counterterrorism field of online terrorist content removal. From a law enforcement perspective, it is clear that the rapid pace of social and technical innovation has resulted in an increasingly interconnected and interdependent world, in which many new hazards have a transnational dimension. This has necessitated a significant shift in approach to counterterrorism. Tech companies are the driving force behind this dynamic change in society, sometimes with unintended consequences for safety and security. But while the tendency has been to highlight the differences between tech companies and law enforcement agencies, this research report provides evidence of an understanding of the common vision shared by both sides to keep people safe online.

The processes and professional partnerships that have been developed are, in part, the product of tech companies' investment in establishing dedicated teams to remove terrorist content. This investment has included the recruitment and buy-in of much needed knowledge and expertise, including hiring personnel with law enforcement backgrounds. The establishment of these teams, coupled with the development and delivery of bespoke training, has led to an improved understanding of each other's roles. The findings also reveal positive working practices of tech companies providing direct and fast access to data at times of critical threat, as well as making personnel available to work within and alongside police counterterrorism operations in response to major terrorist events. These developments provide evidence of a real commitment to tackle terrorism and reveal existing models of cooperation upon which future collaboration can be founded.

It is noteworthy that the research findings did not contain any demands from law enforcement for a more robust regulatory or legislative framework for the removal of online terrorist content. On the contrary, what emerged was a more nuanced, practical and pragmatic approach by police officers who have invested time and resources into developing positive relations with individual tech companies. Our law enforcement interviewees expressed concerns about the utility of new legislation, particularly at a national level, with the most common concern being that such legislation could impede voluntary cooperation and mark a return to the "transactional" relationship of the past.[92] Perhaps it is unsurprising that police officers wish to protect the professional partnerships that they have built over time with their counterparts in tech companies. Nonetheless, the only justification that our law enforcement interviewees offered for new legislation was that it might increase public confidence in how this issue is being tackled.

92 Stuart Macdonald and Andrew Staniforth, "The Tech Industry and the Regulation of Online Terrorist Content: What do Law Enforcement Think?", Hedayah, accessed 9 December 2022, https://hedayah.com/blog-post-the-tech-industry-and-the-regulation-of-online-terrorist-content-what-do-law-enforcement-think/.

In contrast, it was our tech sector participants who had misgivings about the informality of the existing referral process, citing concerns about mission creep and transparency. From their perspective, response times can be slowed as a result of insufficient information being provided and because some requests are not terrorism-related and so have to be redirected within the organisation. There was also a sense that the tech sector's improvements in transparency reporting should be mirrored by state authorities requesting takedowns or shutdowns. This has particular force where an informal referral process is utilised in preference to a formal statutory procedure for content takedown, such as in the UK.[93]

93 Terrorism Act 2006, section 3.

5 Conclusions and Recommendations

While the cultures and operating practices of law enforcement and tech companies are very different, strides have been made towards an increasingly open and cooperative relationship in recent years. Nonetheless, such cooperation remains in its infancy and tensions remain. From a policy perspective, the challenge is to resolve these tensions, given the value of cooperation to tackling online terrorist content, while simultaneously addressing the concerns about due process and accountability that stem from the informality of current arrangements.

The following recommendations are highlighted and offered in an attempt to meet this policy challenge with measures that can be implemented with immediate effect:

- The development of an **experience exchange programme** affording the opportunity for identified personnel within counterterrorism policing and tech companies to be embedded within each other's counterterrorism operational functions. The purpose of the exchange is to fully embed, immerse and expose personnel with the required security vetting and clearances to the operating cultures and practices of each other's organisations, serving to share knowledge, expertise and opportunities to identify better alignment of priorities and more productive ways of working together.

- The implementation of a **takedown-shutdown counterterrorism policing protocol**, providing clarity following review of current practices for content takedown and account shutdown referrals. The protocol will reset and reform current practices with the primary purpose of achieving greater transparency between counterterrorism policing and tech companies, including clearly defined referral parameters and the introduction of independent oversight for takedown and shutdown requests. The protocol serves to ensure counterterrorism powers and partnerships are used only for counterterrorism purposes, while protecting policing from determining legality without independent oversight of takedown and shutdown referrals.

- The development of a joint **upstreaming programme**, which seeks to deliver a fundamental shift in emphasis from the removal of terrorist content online to preventing its initial publication. The upstreaming is founded upon a proactive preventative ethos. This must include increased access and visibility of each other's threat assessments, intelligence insights and future risk forecasting, including meaningful briefings of operational value that offer far greater granularity of detail.

- The development of joint **strategic research requirements**, identifying and prioritising areas of mutual concern for further development and investigation through research. The research

requirements can then be made available to the research and innovation community, offering a unique opportunity to design, develop and deliver research meeting the identified needs of tech companies and counterterrorism agencies better to tackle online terrorist content. These research requirements may include the provision of new AI tools, techniques and technologies, and in-depth analysis providing an evidence base to inform policy, practice and procedure directly.

As the sustained threat from terrorism in all its forms persists, a more progressive, cooperative and collaborative partnership between law enforcement agencies and tech companies must be encouraged. Adopting these recommendations will support transforming this partnership.

Policy Section

This policy section has been authored by Nicola Mathieson, Research Director, at the Global Network for Extremism and Technology (GNET) at the International Centre for the Study of Radicalisation (ICSR) at King's College London. This section provides policy recommendations and is produced independently from the authors of this report. Recommendations do not necessarily represent the views of the authors.

The key findings of this report carry corresponding policy implications for technology companies and policymakers. This report has provided an overview of the status and challenges of cooperation between technology companies and law enforcement in addressing online terrorist content. This report presents an opportunity for both sectors to review their current processes and protocols and implement shared policy changes that support this cooperation.

This policy section ensures that GNET reports provides actionable research outcomes that can inform and support technology companies and policymakers to identify and prevent extremist and terrorist exploitation of digital platforms. The policy section fulfils GIFCT's core pillar of learning to improve prevention and responses to terrorist and extremist violence. This policy section is unique in that, because the report itself is explicitly about cooperation, I will begin with shared recommendations before moving on to sector-specific policy recommendations.

1. Shared Recommendation

Cooperation and coordination between technology companies, more specifically social media platforms, and law enforcement has been reactive rather than a proactive creation of shared protocols and understandings. Drawing on the findings in this report, I identify three core areas for improving cooperation that I envision being implemented by a shared taskforce.

Law Enforcement and Social Media Counterterrorism Taskforce

To date, cooperation between technology companies and law enforcement has been largely ad hoc and reactive. Consequently, this report has identified challenges in what law enforcement requests and what technology companies are able to provide legally, as well as actions that they can reasonably undertake without judicial authority. These issues could be addressed through the establishment of a taskforce that was responsible for systematically developing protocols and processes for cooperation. The three core aims of the taskforce would be to 1) establish dedicated channels of communication for crisis situations; 2) determine a shared language and the parameters of law enforcement requests and technology company compliance; and 3) establish a regular panel between sector experts to assess high-risk cases and share information on recent trends relevant to the jurisdiction.

The challenge of implementing a dedicated taskforce relates to the sheer number of jurisdictions of law enforcement and the regional expertise that it would require. Each of the policy recommendations presented here could be made without the implementation of a formal taskforce. However, without a formal body, the role of facilitating cooperation would still be the responsibility of individual law enforcement jurisdictions and individual technology companies.

- A dedicated channel of communication: a taskforce could act as the dedicated communication channel for law enforcement and technology companies. A single channel to access the relevant actors within different social media companies, for example, would help better coordinate requests, as well as acting as a means of tracking and measuring outcomes.

- The parameters of requests: the report made clear that counterterrorism law enforcement officers and technology companies were often frustrated by the processes of either side. Law enforcement expressed frustration with the speed and different interpretations of "threat to life." Technology companies were frustrated by the lack of judicial authorities, the lack of specificity in requests for content removal and the lack of transparency of government requests. A joint taskforce could be responsible for building a protocol for requests that improve the technology companies' capacity to respond to requests and make clear to law enforcement what technology companies can and cannot do based on their own internal policies.

- High-risk panel: regular panel meetings between sector experts – including actors beyond law enforcement and technology companies – could be designed to address high-risk cases that pose an imminent threat. Cases may be related to individual actors or groups that are displaying concerning behaviour or sharing terrorist content online. High-risk multi-sector panels are an established practice in other sectors, specifically domestic or family violence spaces. These panels would allow for the collaborative sharing of information among panel members so immediate decisions could be made and actions taken. These panels would be a means of ensuring high-risk cases are treated separately from regular protocols and provide all involved a defined time for the issue to be addressed or resolved.

2. Technology Companies

In addition to the joint efforts with law enforcement, there is an additional policy recommendation specific to technology companies:

- Personnel: this report noted the challenge of obtaining timely responses from technology companies for requests and referrals and the competing demands of staff members working on law enforcement liaison teams. Technology companies need to ensure that there is sufficient investment in teams that facilitate cooperation for them to function effectively.

3. Policymakers

In addition to the report findings and their implications for technology companies, this report has also identified three core areas for action by policymakers:

- Harmful but legal content: policymakers have yet to establish a working definition and approach to harmful but legal content online. When it comes to content moderation, the posting of illegal material identified as terrorist content does not pose the same challenges as extremist content that causes harm but is not illegal. States and law enforcement need to be able to define and legislate this content better so that there is a legal basis for requests to technology companies to remove it from their platforms.

- Threshold guidance: interviewees from the technology sector noted that law enforcement Internet referral units lack specificity and the expertise necessary to be participating in this work. Law enforcement personnel in the counterterrorism space need specific training to understand how to report content and when thresholds relevant to technology companies have been reached so that they are able to act on referrals.

- Transparency: this report noted that law enforcement referrals and processes are not subject to the same transparency requirements of technology companies. Often the outcome of implementing transparency requirements is as much an exercise in developing specific protocols and processes that streamline internal organisational behaviour as producing transparency reports themselves. For example, by implementing transparency protocols, law enforcement would be required to determine and define its referral parameters. Implementing greater transparency requirements could help to develop consistency and predictability that enhance the cooperation between technology companies and law enforcement.

Appendix: Interview Schedule

1. Could you please describe your current role and responsibility?

2. [*For law enforcement interviewees*] As part of your role, at any time have you had cause to work, partner, liaise or collaborate with tech companies? Or at any time managed, directed or supervised colleagues who have worked, partnered, liaised or collaborated with tech companies in relation to any aspects of counterterrorism police operations, investigations or general duties or, more specifically, to aspects related to matters of online extremist or terrorist-related content on their platforms?

   [*For tech sector interviewees*] As part of your role, at any time have you had cause to work, partner, liaise or collaborate with law enforcement? Or at any time managed, directed or supervised colleagues who have worked, partnered, liaised or collaborated with law enforcement in relation to any aspects of counterterrorism operations, investigations or general duties or, more specifically, to aspects related to matters of online extremist or terrorist-related content on your platform?

3. Could you please describe the nature of your experience of collaborating with tech companies/law enforcement? Can you recall a specific experience? When was it? How long was it? What was the purpose of this work? What was the outcome of the work?

4. From your experience of working or collaborating with tech companies/law enforcement, did the collaboration meet your expectations? Did this collaboration achieve what you had originally intended? Did the response of tech companies/law enforcement meet the urgency or seriousness of your reasons for making contact?

5. Did your experience of working or collaborating with tech companies/law enforcement require working from their or your place of work? How was this managed? Did this work well?

6. What have you learned from your experience of working and collaborating with tech companies/law enforcement? How would you describe your relationship with tech companies/ law enforcement? Would you describe it as a shared partnership?

7. Were there or are there any barriers and obstacles to your work and collaboration with tech companies/law enforcement? And if so, what did you do or are you doing to address them? And how can these barriers or obstacles be overcome in future collaborations?

8. What are the key benefits of working and collaborating with tech companies/law enforcement?

9. How do you believe your work with tech companies/law enforcement could have been made easier, more efficient or more effective?

10. What are the key challenges of working and collaborating with tech companies/law enforcement? And how do you believe these challenges can be overcome to better achieve your aims?

11. What can tech companies/law enforcement do to develop more effective collaboration for mutual benefit?

12. Is there anything further you wish to add?

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.