Tech Against Terrorism in 2019:
End of Year Report

tech against terrorism

Table of Contents

Executive Summary

The year 2019 saw a number of examples that showcase the ways in which terrorist use of the internet is a constantly evolving threat. The most high-profile case was the Christchurch attack in March 2019, where the perpetrator live streamed his murder of 51 people at two mosques. As shown in research conducted by Tech Against Terrorism, 2019 also saw terrorist groups like the so-called Islamic State (IS) and other violent extremist far-right groups continue their experimentation with new technologies, including the decentralised web and open source licensing.

Both tech companies and governments have responded to many of these challenges. Following the Christchurch attack, industry bodies like the Global Internet Forum to Counter Terrorism (GIFCT), Europol, and the Christchurch Call to Action (an initiative launched by the governments of New Zealand and France) all initiated protocols aimed at stifling the viral proliferation of terrorist content in relation to terrorist attacks. These initiatives were then deployed in the Halle attack in Germany, where the live stream of an attack on a synagogue failed to reach the same level of virality as the Christchurch attack – in large part thanks to the cross-industry responses around crisis coordination that had been put in place.

While terrorist use of the internet continues to evolve, smaller tech platforms remain at high risk of exploitation. Several smaller companies being used by terrorist groups – whether they be messaging, fintech, e-commerce, or content-sharing apps – do not have the resources necessary to tackle this threat. At Tech Against Terrorism, our focus lies on supporting these smaller platforms in tackling terrorist use of their services whilst respecting human rights. In 2019, we expanded our programme of work to include a more diverse set of approaches in supporting the tech industry to include:

- Direct consultation with more than 80 tech companies
- Introduction of the Tech Against Terrorism Mentorship programme to support the GIFCT Membership scheme and provision of one-on-one mentorship to eight companies in the areas of content standards, transparency, human rights, and content moderation
- Introduction of a password protection system on Jihadology.net to protect the site from use by terrorists whilst preserving the site's status as the central hub for terrorist content for academic research purposes
- Funding and commencement of planning for the Terrorist Content Analytics Platform, the world's first free centralised database of verified terrorist content aiming to support smaller tech companies improve content moderation
- Four global workshops (in Europe, South Asia, North America, and the Middle East) on behalf of the GIFCT, attended by at-risk tech companies, senior government officials, leading civil society organisations

- Five webinars for smaller tech companies
- The Tech Against Terrorism Podcast
- Increased research output (see section B.5 in this report)
- Increased investment in open source intelligence (OSINT) – a core part of Tech Against Terrorism's work
- Participation in high-level stakeholder processes, including the Christchurch Call to Action, the EU Internet Forum, and Europol's development of a crisis coordination protocol

In this report, we have provided a detailed summary of our activities in the past year across our three workstreams: outreach, knowledge sharing and operational support. We welcome feedback on our work from our stakeholders including tech companies, civil society groups, governments and inter-governmental organisations, as well as the public.

We can be reached at contact@techagainstterrorism.org.

Background to Tech Against Terrorism

Tech Against Terrorism is an initiative launched in April 2017 by the United Nations Counter Terrorism Executive Directorate (UN CTED), pursuant to four UN Security Council Resolutions[2],[3],[4],[5] as well as the Comprehensive International Framework to Counter Terrorist Narratives[6] that calls for improved public-private cooperation regarding tackling the use of the internet for terrorist purposes whilst respecting human rights.

Tech Against Terrorism focuses on supporting the global technology sector in responding to terrorist use of the internet whilst respecting human rights. The initiative is tech-agnostic and works with companies across all types of technologies, with an explicit focus on supporting smaller tech companies with less resources to adequately address the urgent threat of terrorist exploitation. As a public-private partnership, Tech Against Terrorism works to foster constructive and improved working relationships between the tech sector and the governmental sector.

The workshops took place in Europe, the Middle East, Asia and America, encouraging a broad geographic participation. These discussions enabled Tech Against Terrorism to design a programme of knowledge sharing that led to the launch of the Knowledge Sharing Platform at a special meeting of the UN Counter-Terrorism Committee in New York in November 2017.

In 2018, we directly engaged with over 150 tech companies, organised five training workshops, and attended 77 international conferences in 25 different countries. In its first year, Tech Against Terrorism worked closely with larger tech companies such as Facebook, Google, Microsoft, and Twitter, and in August 2017 supported their launch of the Global Internet Forum to Counter Terrorism (GIFCT).[11],[12] In five months and across nine cities, Tech Against Terrorism, in partnership with the GIFCT, organised nine high-level workshops to bring together representatives from academia, civil society, government, and more than 65 platforms of all sizes.

Funding

Tech Against Terrorism's funding model is based on an equal split between companies and governments. This balance is important as it assures that the project can maintain its neutral position. Tech Against Terrorism has received support from Public Safety Canada, Facebook, Microsoft, Google, Telefonica and the Governments of Spain, Switzerland and the Republic of Korea.

Implementation

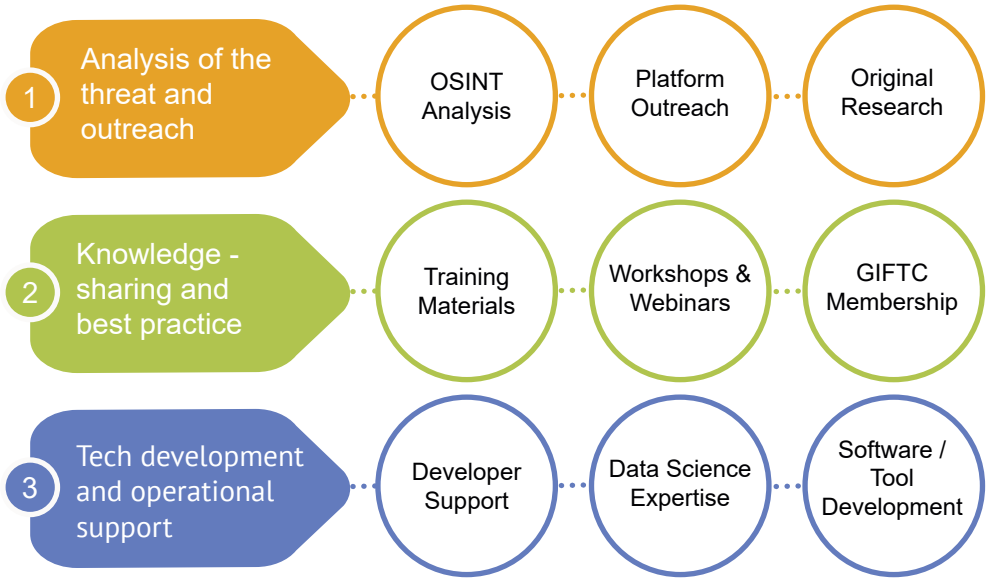
Since November 2018, Tech Against Terrorism is being implemented by QuantSpark Foundation (QSF). QSF is a UK-based foundation aiming to create social impact through data science and product development.

Improving Tech Against Terrorism's governance structure

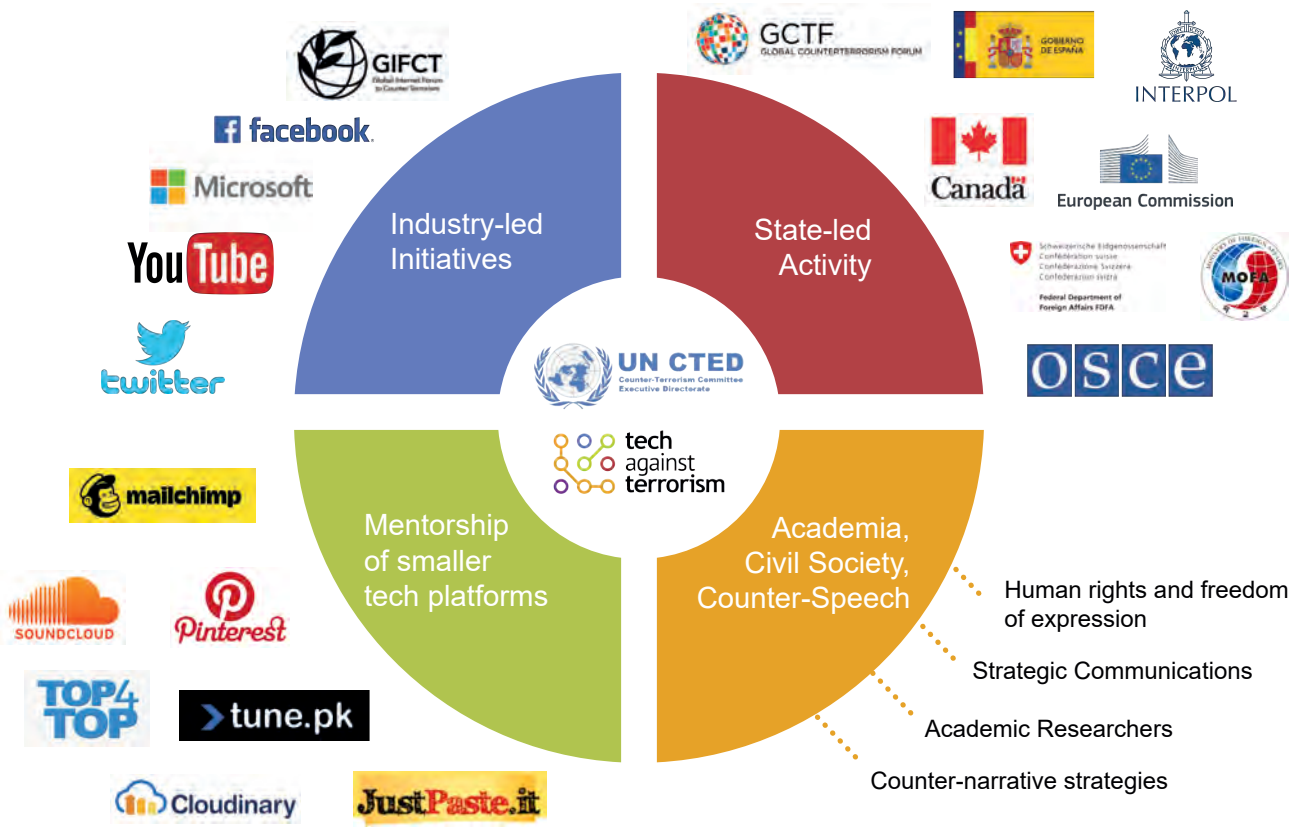
During United Nations General Assembly Week in September 2019, Tech Against Terrorism organised a meeting with core stakeholders to reconvene its Advisory Group and Experts Committee at the UN CTED offices in New York. During this meeting, the issue of governance over Tech Against Terrorism was discussed. Governance is noted as a key tenet by the United Nations Special Rapporteur for the Protection and Promotion of Human Rights while Countering Terrorism Fionnuala Ní Aoláin in her 2019 report to the Human Rights Council of the UN. Tech Against Terrorism is committed to developing a governance structure that allows it to operate in a transparent and accountable manner, for example through ensuring our participatory processes for external stakeholders are consistent, open, and in due consideration of human rights. Tech Against Terrorism is currently working on updating its governance structure, and will publicly publish further information on progress and implementation when more is known over the course of the coming months.

[1] "Launch of 'Tech Against Terrorism' – a partnership between technology companies, governments, and UN CTED" retrieved from https://www.un.org/sc/ctc/news/2017/03/31/launch-tech-terrorism-partnership-technology-companies-governments-un-cted
DISCLAIMER: This report does not necessarily reflect the views of the United Nations and Counter-Terrorism Executive Directorate
[2] Resolution 2129 (2013) notes the evolving nexus between terrorism and the internet, and directs UN CTED to help address this
[3] Resolution 2354 (2017) mandates UN CTED to recommend ways for Member States regarding counter terrorist narratives
[4] Resolution 2395 (2017) recognises the development of Tech Against Terrorism and its efforts to foster collaboration between the tech industry, academia, and governments to disrupt terrorists' ability to use technology for terrorist purposes
[5] Resolution 2396 (2017) recognises the development of Tech Against Terrorism and its efforts to foster collaboration between industry, academia, and governments to disrupt terrorists' ability to use technology for terrorist purposes
[6] S/2017/375 Security Council proposal for a comprehensive international framework to counter terrorist narratives with focus on public-private partnership - describing the Tech Against Terrorism initiative as good practice
[7] See our 2016 report "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust" retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf
[8] The Universal Declaration of Human Rights: Article 19
[9] The Universal Declaration of Human Rights: Article 12
[10] More details of the Tech Against Terrorism Pledge please refer to: https://www.techagainstterrorism.org/membership/pledge
[11] Global Internet Forum to Counter Terrorism to Hold First Meeting in San Francisco, Facebook, 13 July 2017 retrieved from https://newsroom.fb.com/news/2017/07/global-internet-forum-to-counter-terrorism-to-hold-first-meeting-in-san-francisco
[12] "Update on the Global Internet Forum to Counter Terrorism", Global Internet Forum to Counter Terrorism, 4 Dec 2017 retrieved from Facebook, YouTube, Microsoft, and Twitter: https://blog.twitter.com/official/en_us/topics/events/2017/GIFCTupdate.html, https://newsroom.fb.com/news/2017/12/update-on-the-global-internet-forum-to-counter-terrorism

Our three pillars: We focus on Outreach, Knowledge Sharing, and Operational Support



Tech Against Terrorism is a public-private partnership focused on knowledge sharing and providing support to tech platforms



Activities in 2019

A OUTREACH

The foundation to any successful partnership is trust. In order to build trust with the global tech industry, since our inception in 2017 Tech Against Terrorism has devoted a lot of time towards industry outreach. As part of this, we present our work at a range of different international conferences organised by intergovernmental organisations, states, academia and the tech industry. We also build trust and confidence with the tech sector through face-to-face meetings and our own events. We prioritise smaller tech companies identified to be at risk in our data.

1. Geographical presence

In 2019, Tech Against Terrorism attended 41 conferences across the world and delivered a presentation at 26 of these events. Participation in these events allowed us to further consolidate our collaboration with organisations that we have been working with for the past few years and develop new working relationships.

The events we attended and organised in 2019 allowed us to further expand our presence across the world, reaching new markets and regions. Through our global workshops in partnership with the Global Internet Forum to Counter Terrorism (GIFCT), we increased our engagement in the Middle East and Asia, engaging with new tech companies and organisations and addressing new threats and terrorist ideologies.

Our international presence is reflected by the range of organisations with which we partner. Amongst the events we took part in 2019, 15 were held by international organisations and international law enforcement agencies. Notably, we engaged with the OECD on their transparency reporting project, and increased our collaboration with Europol and the EU Internet Referral Unit as we participated in table-top exercises and the EU IRU Referral Action Day *(see section on Participation in stakeholder processes for more on this)*.

We participated in a number of high-level processes helmed by cross-sector and public-private partnerships, notably the Christchurch Call Crisis Response Protocol Workshop organised in Paris following the Christchurch attack, as well the GCTF Policy Toolkit Recommendations led by the Governments of Australia, UK, Switzerland in partnership with the Institute for Strategic Dialogue (ISD).

2. Collaboration with tech platforms

In order to build trust with the global tech industry, we devoted a lot of time towards industry outreach in 2019, engaging with tech companies across the entire tech ecosystem. Our outreach strategy is underpinned by our research and quantitative analysis of terrorist use of internet platforms, and aims to build trust and confidence with the tech sector through face-to-face meetings, workshops and webinars. We prioritise smaller tech companies who might lack resources to tackle terrorist use of their platforms but have the will to engage with this issue.

Overall, in 2019 we have had direct engagement with more than 80 tech companies through our workshops, webinars, partnerships, and bilateral discussions. These companies represent a diverse range of technologies including social media, file-sharing, messaging apps, fintech, gaming, and e-commerce platforms.

Central to our outreach strategy to tech companies is our mentorship programme for content-sharing platforms in collaboration with the GIFCT. We are proud to say that over the course of 2019, we mentored eight tech companies, three of which completed the process to become members of the GIFCT *(see section B.2)*.

3. Open source intelligence (OSINT)

In 2019 we scaled up our open source intelligence (OSINT) capabilities and efforts to underpin all three of our pillars. OSINT is the collection, verification and analysis of information that is gathered from public, or "open", sources. It therefore allows us to monitor and identify at-risk platforms to which we can offer our support. From here, our OSINT analysis can also help to predict or gauge how terrorists may operate online in the future – and, accordingly, where resources should be directed.

In 2019, OSINT was an essential part of Tech Against Terrorism's knowledge sharing strategy, as we took part in multiple events centred on open source intelligence – including participating in Europol OSINT Workshop and providing training at the National Police Chiefs Council Conference on Internet Investigations.

In order to strengthen our OSINT network and share knowledge, we launched a series of OSINT breakfasts aiming to bring together local OSINT researchers to share knowledge, tools, and best practices. These breakfasts are the opportunity to learn more about the use of OSINT through insightful case studies and to build a strong community of practitioners. Our breakfasts, held in July and November 2019, notably touched upon the collection and analysis of Telegram metadata at scale, researching far-right entities, and other insightful case studies by practitioners.

4. Tech Against Terrorism in the media

We are proud to say that in 2019 we saw a significant increase in public interest in the work that Tech Against Terrorism does. This was demonstrated by the important rise in media coverage of our work, which was featured in over 30 articles and publications from global media throughout the year. The work of Tech Against Terrorism was notably mentioned in the following articles, amongst others:

- "Christchurch attacks: Should Facebook be commended or condemned?", Al-Jazeera English interview with Tech Against Terrorism Director Adam Hadley 18 March 2019
- "Is There a Growing Far-Right Threat Online?", BBC News, 7th July 2019
- "Creative Intelligence and Anti-Terrorism", Noteworthy - The Official Journal Blog interview with Tech Against Terrorism Director Adam Hadley, 25 July 2019
- "Germany terror attack livestreamed: What is the tech industry doing?", France24 interview with Tech Against Terrorism Director Adam Hadley, 10th October 2019
- "The German Synagogue Shooter's Twitch Video Didn't Go Viral Here's Why", Vice News, 11th October 2019

Tech Against Terrorism's Director Adam Hadley was interviewed by France24 in the aftermath of the Halle, Germany attack.

B KNOWLEDGE SHARING

1. Global workshops

Global workshops allow us to reach a more diverse range of stakeholders across the world. In 2019, we organised four workshops with the Global Internet Forum to Counter Terrorism in Amman, Delhi, and London as well as a masthead event in Silicon Valley.

These are designed to facilitate knowledge sharing between cross-sector stakeholders and increase smaller platforms' understanding of and capability to tackle terrorist use of their platforms. They are typically split into two parts. The first part convenes expert researchers, academics, government officials, and civil society organisations to provide a state of play threat assessment of how terrorists are currently exploiting the internet. Subsequently, experts explore models for collaboration and how various sectors can work together to tackle the threat in a manner that respects fundamental human rights.

In the second part of the workshop, we hold informal, in-depth discussions and breakout sessions for tech companies, researchers and CT experts. The sessions, run by Tech Against Terrorism, allow an unprecedented opportunity for smaller companies to share their concerns and experiences with this problem – and to solicit advice from larger tech companies. These sessions have been invaluable for Tech Against Terrorism in terms of increasing our understanding of how smaller platforms approach implementing mechanisms around Terms of Service and content moderation.

Local representation is integral to the success of these events. Apart from private tech companies, we are always delighted to see representation from local and regional government officials and law enforcement at each of these workshops, as well as from a range of leading academics, counterterrorism researchers, civil society groups, and intergovernmental organisations.

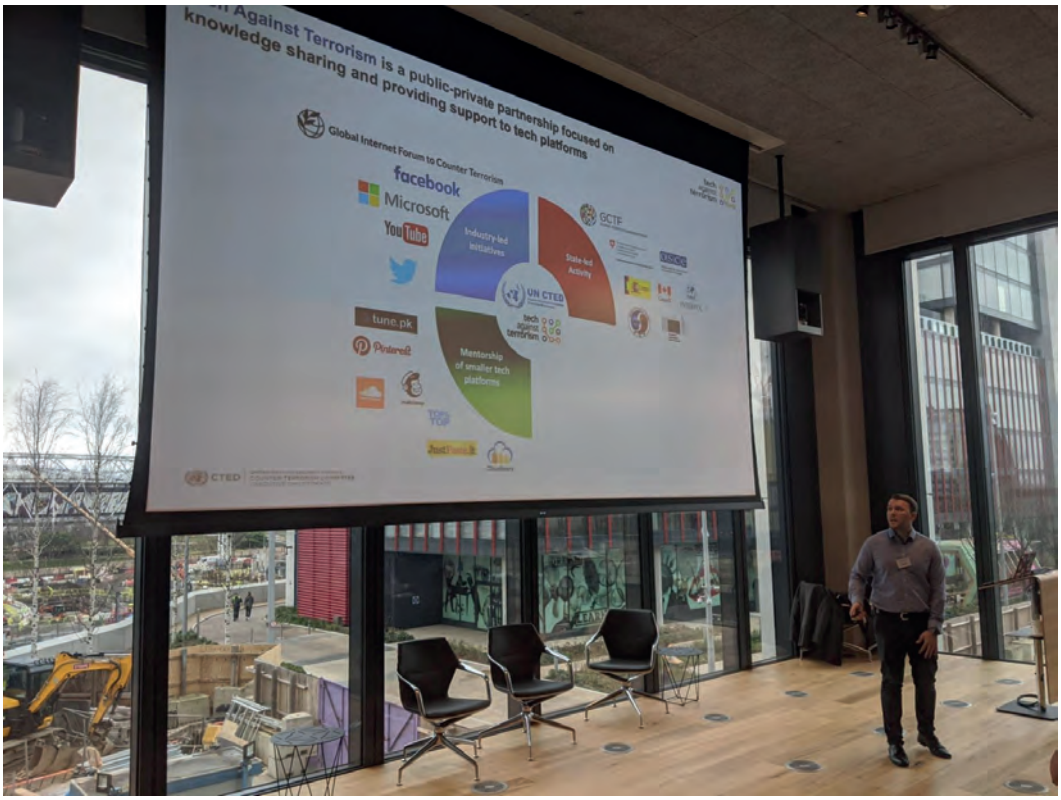
1.1 Amman Workshop (June 2019)

- In attendance: 100 participants, of whom over 40% were Jordan based, with a further 30% from the MENA region. Overall, 35% of our panellists were also Jordan based.
- Notable speakers: There were 15 panellists from various sectors including government officials, OSINT analysts, civil society leaders, specialised academics, and policymakers from tech companies. Notable speakers include Sharri Clark, Counter-Terrorism Bureau of the US Department of State; Dr Mohanned Arabiat, President from Generations for Peace; and Dr Khawla Alhasan, Inclusion and Gender Advisor of Municipal Services and Social Resilience Project.

1.2 San Francisco GIFCT event (July 2019)

In July, we supported the GIFCT at their annual summit in Silicon Valley.

- In attendance: around 100 attendees including all GIFCT CT leads, Europol, Interpol, ORF, the German government, US Department of Homeland Security, US State Department, companies such as Wikimedia, Pinterest, Western Union, prominent civil society groups including the Center for Democracy and Technology and the Internet Jurisdiction and Policy Network, and a range of academics including Aaron Zelin, founder of Jihadology.
- Notable speakers: Nick Clegg, Vice-President of Global Affairs and Communications, Facebook; Monika Bickert, Head of Global Policy Management, Facebook; Department of Prime Minister and the Cabinet of New Zealand; and Ministry of Digital Affairs of France.



1.3 Delhi Workshop (November 2019)

Our Delhi workshop was the first of its kind in India, as well as the first two-day workshop that we have organised. The longer format allowed us to increase space for expert discussion, including hosting a new panel that explored existing programmes to counter terrorism. For the first time, we had a breakout session explicitly for law enforcement officials that was run concurrently to the tech and the research sessions.

- In attendance: 90 participants in counterterrorism, counter-extremism, and localised resilience work from across India, Afghanistan, Sri Lanka, and Bangladesh.
- Notable speakers: Ankhi Das, Facebook's Public Policy Director (India, South & Central Asia); Samir Saran, President of the Observer Research Foundation (ORF); alongside leading officials from the Indian Army and Indian National Security Council Secretariat, Lt General (Retd.) Syed Ata Hasnain and Mr. Shiv Sahai.
- Notable conclusions: The key term for the Delhi event was a "whole of society" approach. Although technology is an enabler when it comes to violent extremism and terrorism, approaches to tackling these issues must bear in mind that technology does not create terrorists and there is no substitute for on the ground, in-community CVE work.

1.4 London Workshop (December 2019)

Building on the success of the two-day format of our Delhi Workshop, the London event was also held over two days. However, London's second day was dedicated entirely to a declassified threat assessment day led by the Federal Bureau of Investigation, including presentations from all Five Eyes countries. The first day also included a prioritisation/severity training exercise for a select few attendees.

- In attendance: 90 participants, over 40% of whom were from the tech sector.
- Notable speakers: Counter-terrorism leads from Five Eye countries, Dr Shiraz Maher, Director of ICSR, and Edward Bowles, Director of Facebook Public Policy Northern Europe; counterterrorism leads for Five Eyes countries; Europol.

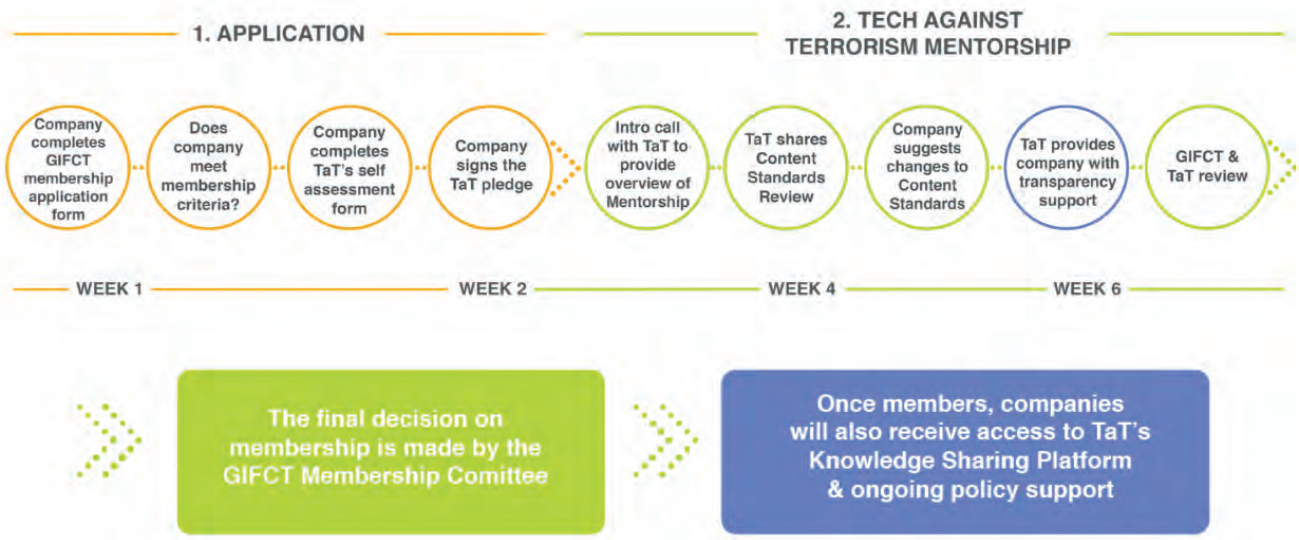
2. Mentorship

At the end of 2018, the GIFCT announced a membership programme for content-sharing platforms, including social media, content storage, and file-sharing companies, aiming to set a baseline standard across the tech industry for addressing terrorist content online. It was agreed that Tech Against Terrorism, expanding on its work supporting the GIFCT's knowledge-sharing activities, would act as a mentor for companies applying to the membership programme. To this end, Tech Against Terrorism supports the companies that do not meet the membership criteria stipulated by the GIFCT, and advises them as to how some of these challenges might be addressed.

In 2019, Tech Against Terrorism mentored eight tech companies. Our mentorship has focussed on four main areas: content standards, human rights compliance, transparency and content moderation.

1. Content standards: Having accurate yet robust content standards are vital to effectively tackling terrorist use of a service. We complete a forensic review of a company's content standards, including their Terms of Service, Community Guidelines, and other policies. We highlight areas in these content standards that are strong, and provide policy recommendations for areas that might need consideration. This year, all of the companies for which we provided assessments have explored adapting their content standards in accordance with our suggestions, the majority of which have actually published updates in their content standards thereafter.
2. Human rights compliance: We provide guidance to platforms to help them ensure that their policies and processes are created and enforced to preserve and enhance users' rights. Companies are also asked to sign the Tech Against Terrorism Pledge, which consists of six guiding principles based on internationally recognised norms and resolutions on counter-terrorism and human rights. The Pledge provides a framework to ensure that companies will actively consider freedom of expression and human rights in their counter-terrorism measures.
3. Transparency: We support companies to either introduce or improve on their transparency reporting, providing policy advice around standards to report on and, if necessary, support in data collection processes.
4. Content moderation: Companies are asked to complete Tech Against Terrorism's self-assessment tool, a series of questions and problems to help us understand existing content moderation procedures, as well as outline areas where a company might require further support. We provide tools and resources that support content moderation policy and takedown decisions.

The diagram below shows the steps involved in the membership process, and Tech Against Terrorism's role within it:



2.1 Mentorship Booklet

We have also compiled a 20-page booklet designed to provide prospective and onboarded smaller platforms with insight into what Tech Against Terrorism Mentorship and the GIFCT Membership actually entails. The booklet details the steps involved in the mentorship process, as well as further information on each of the components including a task list, the GIFCT Membership criteria, the Tech Against Terrorism Pledge, and self-assessment tool. Once Tech Against Terrorism has completed an assessment of the company's content standards, this review is included in the booklet. If you are interested in receiving a copy of this guide, please email us.

3. E-learning Webinars

In 2019, we introduced e-learning sessions to be carried out in partnership with the GIFCT. These sessions are aimed at scaling knowledge and capacity-building across the wider tech industry and include presentations on a variety of topics by representatives from Tech Against Terrorism and GIFCT, as well as leading industry experts. The sessions close with a Q&A session, which allows participants to ask questions or share thoughts about what they have just learnt. The main aim is to explore practical ways to support smaller tech companies in tackling the terrorist use of the internet whilst respecting human rights.

We also organised webinars separately from the GIFCT, for example in December 2019 with Europol.

3.1 E-learning session: Using hashing technology to counter terrorist use of the internet (June 2019)

- Summary: After introductory remarks from Tech Against Terrorism and Facebook, two presentations were given by representatives from Facebook and Camera Forensics. Each explored how image and video hashing technology can be used to combat both terrorism use of the internet and other online harms, such as child abuse. Facebook also provided the participants with information about the GIFCT's hash-sharing consortium and how tech companies can be included in it.
- Speakers: Dina Hussein, Policy EMEA Facebook; John Kerl, Facebook engineering team; and Dave Ranner, Camera Forensics.

Given the level of interest in the topic of hashing, we hosted a repeat session for the APAC time zone later on in the year.

3.2 E-learning session: Defining terrorism and terrorist organisations on tech platforms (October 2019)

- Summary: This webinar explored the issue of defining terrorism and terrorist organisations on tech platforms. Dr. Krisztina Huszti-Orban and Lina Cepeda gave presentations that explored the international legal framework for definitions of terrorism and the UN approach on this topic, as well as some of the human rights considerations involved in defining terrorism. Facebook discussed their approach to creating its own definition, and Chris Meserole laid out the strengths and drawbacks of using designation lists as reference points for moderating content.
- Speakers: Jacob Berntsson, Research Manager, Tech Against Terrorism; Dr. Erin Saltman, Policy Manager EMEA, Facebook; Dr. Krisztina Huszti-Orban, Senior Legal Advisor to the UN Special Rapporteur on Counter-terrorism and Human Rights; Lina Cepeda, Legal Officer & ICT Coordinator, UN CTED; and Chris Meserole, Research Fellow at Brookings.

3.3 E-learning session: Drafting Terms of Service & Community Guidelines (October 2019)

- Summary: This webinar looked at how drafting robust Terms of Service and Content Standard Guidelines can help in protecting a platform from terrorist exploitation. Experts from Tech Against Terrorism, GIFCT, and leading researchers shared their insights on how platforms can ensure that their standards are effective whilst simultaneously safeguarding freedom of speech and human rights.
- Speakers: Adam Hadley, Director, Tech Against Terrorism; Dina Hussein, Policy EMEA, Facebook; Daphne Keller, Director of Intermediary Liability, The Center for Internet & Society at Stanford Law School; Alex Feerst, former Head of Legal and Head of Trust & Safety, Medium; and Sebastian Koehler, Organic Content Policy, Facebook.

3.3 E-learning session: Mental health and content moderation (November 2019)

- Summary: This fourth e-learning session in partnership with GIFCT took a look at the mental health risks faced by those who work in content moderation and are being exposed to terrorist content each day. Experts shared their insights on the scale of the issue itself, as well as offered ideas on best practices that better protect those on the front line of the fight against terrorist use of the internet.
- Speakers: Jacob Berntsson, Research Manager Tech Against Terrorism; Dina Hussein, Policy EMEA, Facebook; Prof. Maura Conway, School of Law and Government, Dublin City University & VOX-Pol Principal Investigator; Dr. Zoey Reeve, Lecturer, Research Methods, Newcastle University & VOX-Pol Research Fellow; and Gustavo Basualdo, Senior Program Manager, Online Safety, Microsoft.

3.4 Tech Against Terrorism & Europol Webinar: Law enforcement and tech sector collaboration (December 2019)

- Summary: Hosted by Tech Against Terrorism in partnership with Europol, this webinar was targeted at sharing knowledge with the tech sector about ways of collaborating with law enforcement. Topics covered included: the mandate and set-up of the European Union Internet Referral Unit (EU IRU), overview of the process used by the EU IRU to refer content to tech companies, ways that the EU IRU supports smaller platforms in identifying terrorist content, referral action days, cross-border requests to access electronic evidence, and the SIRIUS program.
- Speakers: Experts from Tech Against Terrorism, Europol, and the SIRIUS program.

4. The Tech Against Terrorism Podcast

In 2019, Tech Against Terrorism launched its own podcast series, the Tech Against Terrorism podcast, that takes a deep dive into many of the different elements surrounding the response to terrorist use of the internet. Last year, we recorded the first five episodes, convening top experts to unpack some of the complex and contentious topics in the field.

4.1 How do terrorists use the internet?

- Summary: This introductory episode explored how terrorist groups are exploiting an entire tech ecosystem, and what is being done to combat it.
- Guests: Matthew Feldman, Director of the Centre for Analysis of the Radical Right; and Audrey Alexander, researcher and instructor at West Point's Combating Terrorism Center.

4.2 How we fight terrorism while protecting human rights

- Summary: In this episode we looked at how governments and tech platforms are attempting to strike a balance between tackling terrorism online whilst safeguarding human rights and freedom of expression.

- Guests: Emma Llanso, Director of the Free Expression Project at the Center for Democracy and Technology; and Dr. Krisztina Huszti-Orban, Senior Legal Advisor to the UN Special Rapporteur on Counter-Terrorism and Human Rights.

4.3 The power and responsibility of open source intelligence

- Summary: This episode explores how effective analysis of publicly available information is critical in countering terrorist use of the internet; intrigue and curiosity help these experts infiltrate online extremist networks, where messages of propaganda and hate and being spread.
- Guests: Benjamin Strick, an open source investigator for BBC Africa Eye; Nico a.k.a. 'DutchOSINTGuy', a former police officer in the Netherlands; and Terry Pattar, who runs the intelligence unit at the security analysis firm Jane's 360.

4.4 How terrorism is financed

- Summary: This episode delves into the myriad of means used by terrorists to fund operations and recruitment. Although terrorist groups largely use traditional methods to fund their activities, the anonymity cryptocurrency affords is becoming an increasingly attractive alternative.
- Guests: Nick Furneaux, author of 'Investigating Cryptocurrencies'; Florence Keen, research fellow at the International Centre for the Study of Radicalisation at King's College London; and retired police officer Andrew McDonald, who served as head of specialist investigations of the UK National Terrorist Financial Investigation Unit at New Scotland Yard.

4.5 How mainstream media can spread terrorist propaganda

- Summary: Focusing on the UK landscape, this episode explores how news media can inadvertently provide some of the most effective PR for terrorists by amplifying their messages by spreading videos and images. It particularly focuses on the importance of imposing stringent and robust rules on UK newspapers, which currently lack independent regulation.
- Guests: Kyle Taylor, executive director of Hacked Off, a group which campaigns for a free and accountable press in the UK; and Abdirahim Saaed, a journalist for BBC Monitoring, who tracks and analyses the propaganda output of Salafi-jihadist groups like ISIS and Al-Qaeda.

5. Research & Analysis

In 2019 we ramped up our regular research output and quantitative analysis of terrorist use of internet platforms. Below is a selection of the research and analysis we produced.

5.1 Analysis: New Zealand attack and the terrorist use of the internet

We analysed tech sector responses to the exploitation of their services by the Christchurch terrorist sympathisers before, during, and after the attack on 15 March, 2019. In particular, we focused on the so-called "manifesto" and the dissemination of the real-time video of the attack. We found that the global tech sector responded quickly in taking down the terrorist's so-called manifesto and videos of the attack. Even the majority of smaller tech platforms hosting the video and manifesto quickly removed them from their platforms. Despite criticising tech companies for a perceived failure to quickly remove content related to the attack, several news outlets published the attack video and the so-called manifesto on their websites.

5.2 Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content

Tech Against Terrorism's analysis of more than 45,000 URLs dating back to 2014 across more than 330 platforms shows that smaller platforms are heavily targeted by the so-called Islamic State (IS) and that 49% of all URLs were found on just eight of these platforms. We found that IS experimentation with small social media platform Koonekti is the most recent case of the group experimenting with new and small-sized platforms in an attempt to find a viable alternative to Telegram. Moreover, the decentralised web (DWeb) – an alternative to the current world wide web – appears to have proved a stable alternative to Telegram and the smaller platforms in some cases. Nevertheless, we are unlikely to see a transition from Telegram to DWeb services unless Telegram becomes substantially more hostile towards IS and its supporters or DWeb services more user-friendly.

5.3 Analysis: The use of open source software by terrorists and violent extremists

This analysis assesses the need to broaden current debate around terrorist and violent extremist use of the internet to include a much-needed discussion about the decentralised web and open source licenses, its abuse by various entities, and appropriate human rights-compliant measures to counter this trend. Increasingly terrorists and violent extremists are building their own software applications, and much of this depends on reusing existing code and software that were originally developed under the open source model and published for everyone to re-use and modify.

5.4 Analysis: What can we learn from the online response to the Halle terrorist attack?

Following the Halle attack, we assessed the tech sector's response to the attack and in preventing the viral spread of content related to the attack, including a "manifesto" and a live stream of the attack. We concluded that, since the Christchurch attack, great efforts were made to coordinate tech sector responses to "online crises" related to terrorist attacks. Such initiatives, like the GIFCT hash-sharing consortium and the GIFCT Content Incident Protocol, were shown to be effective in dealing with the Halle crisis as the video and manifesto not spread as virally as the Christchurch video and manifesto. In sum, both smaller and larger platforms were prompt in dealing with the proliferation of the video. It was only circulated widely with little or no moderation on smaller fringe platforms.

C OPERATIONAL SUPPORT

Tech Against Terrorism has devoted increasing effort to operational support and capacity building in its programme to support the global tech industry. Specifically, our focus in this regard has been on supporting platforms through the development and implementation of tech solutions in a way that solicits deep subject matter understanding of terrorism and respects freedom of expression and human rights. In our view, this is the most effective and practical way to support the global tech sector in tackling terrorist use of the internet.

1. Jihadology

In April 2019, we announced that we had been working with academic blog Jihadology.net to implement a user registration system ensuring that researchers can access important primary research material whilst preventing terrorists and those vulnerable to recruitment from viewing and downloading the most sensitive content on the site. This system requires account and password creation, where only those with a legitimate research interest will be allowed to use the site. Jihadology is highly regarded as the internet's most comprehensive "clearing house for jihadi primary source material and original analysis". As such, Jihadology is an essential resource for academia and terrorism researchers.

Initial indications suggest that the user registration system has been successful in preventing illicit use of Jihadology. There have been registration requests from suspicious individuals attempting to register, but ultimately failing thanks to the rigorous registration process. To date, we have received more than 100 suspicious requests, the most serious of which we have brought to the attention of the relevant security agencies. Whilst we cannot confirm that suspicious registration attempts have been made by individuals with serious ill intent, it proves that illicit usage of the site is now restricted. We have also noted signs of frustration amongst violent Islamist sympathisers on various online platforms about the updates preventing them from gaining access to the site.

Since the launch of the updated version of Jihadology:

- 100+ suspected terrorists prevented from using the service
- 0 downloads of videos, images, PDFs, and audio files by suspicious users
- 1,400+ accounts created by academic researchers
- 470 research institute domains whitelisted

2. Terrorist Content Analytics Platform (TCAP)

At the end of June 2019, the Government of Canada announced that they would provide funding towards the development of our Terrorist Content Analytics Platform (TCAP). In 2019, we commenced pre-development preparation, including hiring of an academic advisory board and launching a public consultation process. We will share more details on the TCAP in 2020.

2.1 Summary of the TCAP

The TCAP is the first free unified intelligence-sharing database for online terrorist material. It is a repository of verified terrorist content (imagery, video, PDFs, URLs, audio) collected from open sources and existing datasets to facilitate secure intelligence sharing between platforms. The purpose of the TCAP is fourfold:

1. To support tech companies in detecting terrorist content on their platforms, helping inform and manage company moderation procedures as companies will also be able to securely examine verified terrorist content on the TCAP
2. To facilitate affordable intelligence sharing for smaller internet platforms, and help smaller tech companies to expeditiously address terrorist use of their platforms through an alert function
3. To facilitate secure intelligence sharing between expert researchers and academics by giving vetted academics and expert researchers access to the platform, this centralised dataset will instigate improved quantitative analysis of terrorist use of the internet and inform the development of accurate counter-measures
4. To facilitate the coordination of data-driven solutions to counter terrorist use of the internet by making content on the platform available as a training dataset for development of automated solutions

2.2 TCAP side event at UN General Assembly Week in New York (September 2019)

During UNGA week, Tech Against Terrorism convened a side event in partnership with UN CTED. The side event was an introductory consultation meeting on the TCAP. The meeting was attended by members of civil society, academia, the tech sector, as well as government and intergovernmental organisations, whose feedback will help guide the development of the platform. During the event, we gained some initial key recommendations for users and content moderators, for example around the welfare of users, ensuring the diversity of the academic advisory board, and around privacy concerns.

2.3 Public consultation on the TCAP

In laying the groundwork for the development of the TCAP, four key concerns were taken into consideration:

1) Rule of law
2) Accuracy and transparency
3) Privacy and security
4) Tech platform autonomy

To fully understand these and other potential areas of concerns, Tech Against Terrorism launched an online public consultation process in the latter half of 2019 to solicit feedback from experts within the tech sector, civil society, and academia and expert researchers.

Answers gathered during this consultation will inform the TCAP risk mitigation process, which is still ongoing, and will be further discussed during meetings and webinars to be held in 2020 with representatives from the tech sector, academia and civil society. A report with key conclusions from this process will be shared in 2020.

PARTICIPATION IN STAKEHOLDER PROCESSES

Last year, Tech Against Terrorism continued its engagement with many ongoing processes and projects geared toward CT and CVE efforts. Below are some examples of where Tech Against Terrorism was invited to influence the direction of the program by providing evidence, research insights, or training. This list, however, is by no means exhaustive. We would like to thank our partners and stakeholders for their consideration, and commend them for their dedication to creating space for cross-sector collaboration to counter terrorist use of the internet.

The Aqaba Process

In 2019 Tech Against Terrorism participated in two high-level meetings under the auspices of the Aqaba Process, organised by the King of Jordan.

Christchurch Call

Tech Against Terrorism is proud to be mentioned in the Christchurch Call as a good example of industry collaboration. We have also been involved in providing input throughout the consultation process, including through participating in a civil society consultation with New Zealand Prime Minister Jacinda Ardern in Paris, another consultation workshop in Paris, and a research workshop in New York.

Commission for Countering Extremism

We submitted evidence to a report on hateful extremism published by the UK's Commission for Countering Extremism in October 2019.

EU Internet Forum

Tech Against Terrorism participated in several EU Internet Forum meetings over the course of 2019. These meetings bring together member states and prominent tech companies to foster cross sector collaboration and finding ways forward to mitigate terrorist use of the internet.

Europol Open Source Intelligence Conference

Our OSINT staff provided OSINT training in researching terrorist and violent extremist entities as well as how to derive actionable intelligence from large quantitative datasets.

Europol Table-top Exercise

Tech Against Terrorism contributed to a table-top exercise organised by the EU Internet Referral Unit under the auspices of the EU Internet Forum at Europol's headquarters in the Hague. These exercises are aimed at informing the development of a coordinated continent-wide response to the dissemination of viral online terrorist content connected to terrorist attacks.

Internet Intelligence and Investigations Conference

We conducted an open source intelligence training workshop and taught techniques for research purposes on Telegram, as well as how to derive actionable insights from Telegram channels and chats at scale.

Interpol & Project KALKAN Conference: The Transnational Terrorist Threat in The Project

We supported an Interpol-led capacity building exercise for regional law enforcement agencies in Tashkent, Uzbekistan.

The OECD TVEC and Transparency Project

We participated in the introductory meeting of OECD's new transparency reporting initiative, which is set to continue in 2020.

UK Online Harms White Paper

Tech Against Terrorism participated in a closed civil society consultation with DCMS on the interim code of the Online Harms White Paper.

OSCE National Table-top Exercise in Central Asia

We supported a table-top exercise organised by the OSCE in Tajikistan and Kyrgyzstan aimed at building law enforcement capacity in tackling terrorist use of the internet whilst respecting human rights.

UN General Assembly week

Tech Against Terrorism participated in various events during 2019 UN General Assembly week in New York, including: a Christchurch Call High-Level Meeting and Leaders' Dialogue, organised by New Zealand, Jordan, and France; the Global Counter Terrorism Forum (GCTF) and Institute for Strategic Dialogue side event and the Policy Toolkit on the Zurich-London Recommendations; and the Global Rise of Radical Right Wing Extremism, organised by the Soufan Center.

The Tech Against Terrorism team would like to extend our gratitude to all of our key partners, associates, and stakeholders for their support, collaboration, and vision in tackling terrorist use of the internet throughout the year of 2019. We will work to carry the significant level of momentum gained and the lessons learnt into the coming year, and endeavour to support the various projects and hard work being done to this end.

tech
against
terrorism