tech against terrorism

# TECH AGAINST TERRORISM
## ANNUAL REPORT 2020-2021

# CONTENTS


Background to Tech Against Terrorism 1
Executive Summary 4
Our Work in Response to the 2020 Landscape 5
Key Trends in Terrorist Use of the Internet in 2020 8
Activities in 2020 12
- Outreach 12
- Tech Sector Engagement 12
- Podcasts 12
- Weekly Reader's Digest 16

TAT in the media 17
- Recognition of our work 18

Events and webinars 19
Knowledge Sharing 21
- Original Research & Publications 21
- Online Regulation Series 23
- Webinars organised 24

TAT Mentorship and Membership Programmes 31
Operational Support 38
- Terrorist Content Analytics Platform (TCAP) 38
- TAT's Catalogue of services and bespoke support 41

Participation in Stakeholder Processes 42
- Events 42
- Consultations 44

Extending our Knowledge 46
- Online Regulation 46
- End-to-end-encryption 46

Terrorist Operated Websites 47
Gamification 47
2021: Q1 & Q2 48
Events 48
Media 50
E-learning Webinar Series 53
Responses to Regulations and Consultation Processes 54
Publications 54
Terrorist Content Analytics Platform (TCAP) 55
Knowledge Sharing Platform (KSP) 56
Online Regulation Series 57
Open-Source Intelligence (OSINT) 58
Designation – Proscribed Organisations 59
Transparency Reporting Guidelines for Governments and Platforms 59
TAT Mentorship and Membership Programmes 59

# TECH AGAINST TERRORISM | BACKGROUND

Tech Against Terrorism is an initiative supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED), and was launched in April 2017. The official launch followed a first phase convened in April 2016, entitled 'Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust.'[1] Since 2019, Tech Against Terrorism is implemented by the Online Harms Foundation.[2] Tech Against Terrorism is a public-private partnership and is funded by both the tech industry via the Global Internet Forum to Counter Terrorism (GIFCT) and by governments. To date, the governments of Spain, Republic of Korea, Switzerland, Canada and United kingdom have provided financial support to Tech Against Terrorism.

The Tech Against Terrorism initiative is pursuant to four UN Security Council Resolutions[3] as well as the Comprehensive International Framework to Counter Terrorist Narratives[4] 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 tech sector in responding to terrorist use of the internet whilst respecting human rights. Tech Against Terrorism is a tech-agnostic initiative 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.

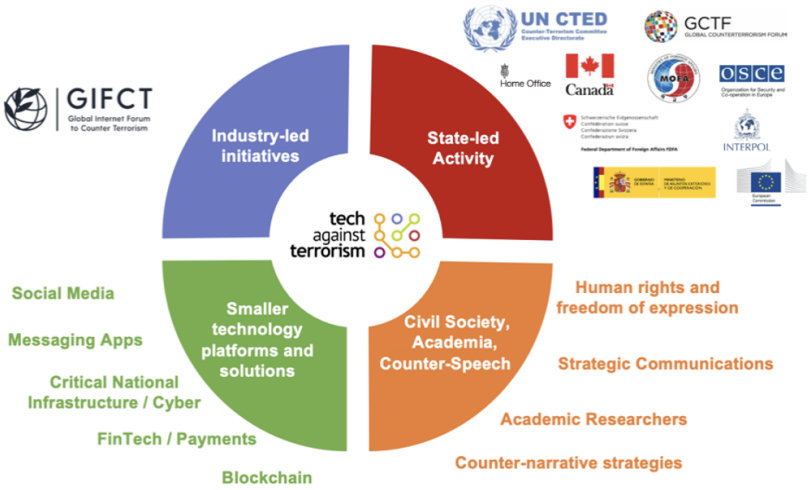
1. A report on this phase can be downloaded here: https://www.techagainstterrorism.org/research/
2. https://beta.companieshouse.gov.uk/company/11656320
3. Resolution 2129 (2013) notes the evolving nexus between terrorism and the internet, and directs UN CTED to help address this; Resolution 2354 (2017) mandates UN CTED to recommend ways for Member States regarding counter terrorist narratives; 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; 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.
4,. 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

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).[5] 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 tech companies and governments. This balance is important as it assures that we can maintain our neutral position. Tech Against Terrorism has received support from the Global Internet Forum to Counter Terrorism and the governments of Canada, the United Kingdom, Spain, Switzerland, and the Republic of Korea.




5. 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; "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

## Implementation

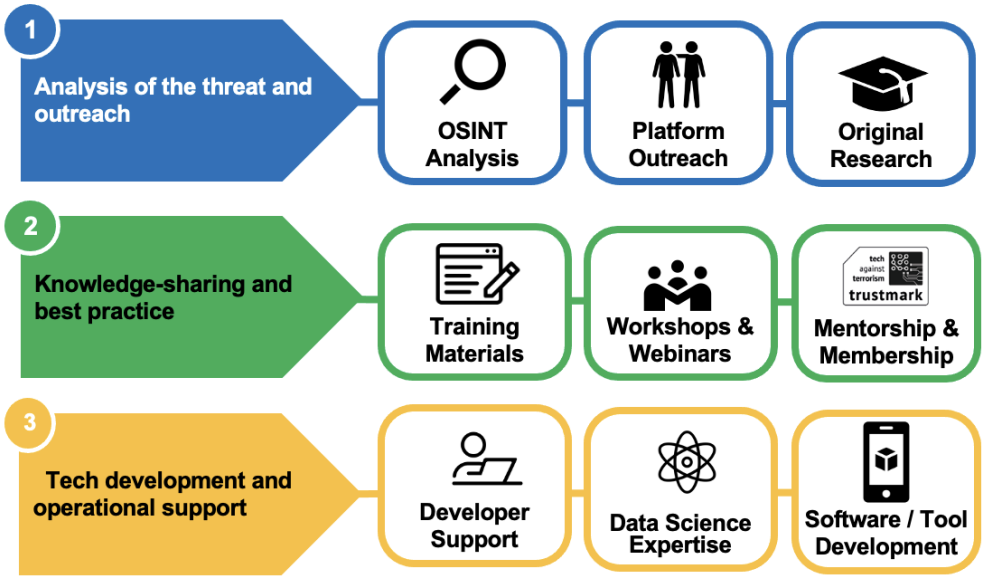
Since November 2018, Tech Against Terrorism is implemented by QuantSpark Foundation (QSF). QSF is a UK-based foundation aiming to create social impact through data science and product development. In 2020, QuantSpark Foundation changed its name to the Online Harms Foundation (OHF).

## Launch of the Online Harms Foundation

The Online Harms Foundation was launched in order to offer broad practical support to smaller tech platforms to include countering the terrorist use of the internet, child sexual abuse material (CSAM), hate speech, online scams, and disinformation whilst respecting human rights.

## Improving Tech Against Terrorism's governance structure

During the 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. 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.



# EXECUTIVE SUMMARY

The year 2020 was largely characterised by the Covid-19 pandemic, its lockdown measures, as well as the spread of related mis- and disinformation online. This environment, coupled with civil and political unrest in several parts of the world, represented an almost ideal opportunity for malevolent actors to exploit. Terrorists and violent extremists were quick to exploit the opportunity offered by the crises to spread their hateful ideas online and recruit new members.

Whilst manifesting itself mostly online, this exploitation was not limited to the online sphere but materialised in real world events as violent extremists blended themselves into anti-lockdown protests and as terrorists' plans were eventually thwarted. Though the tech sector was generally quick to respond to the mis- and disinformation spreading online, the rapid changes in content moderation policy and processes hold important consequences for the future of content moderation and more importantly for freedom of expression online.

The rapid changes in content moderation policy and processes hold important consequences for the future of content moderation and more importantly for freedom of expression online.

In addition, 2020 and 2021 witnessed many developments in terms of regulation of online speech and content, in relation to countering the spread of terrorist content online. Over the past year, more than 20 new laws have been passed or proposed to parliament in several countries including Australia, Brazil, France, India, the United Kingdom, Morocco, Pakistan, Singapore, Turkey, and the European Union.

# OUR WORK IN RESPONSE TO THE 2020 LANDSCAPE

Facing this fast-changing landscape in 2020, we adjusted our knowledge-sharing activities to adapt to the external changes, such as by focusing on our e-learning webinars series, podcasts, as well as participating in a number of virtual stakeholder events. We additionally responded by adjusting our outreach in terms of open-source intelligence as well as through the Terrorist Content Analytics Platform. We expanded our programme of work to include a more diverse set of approaches in supporting the tech industry. Highlights of our work in 2020 includes:

- Organised 5 webinars on topics ranging from the far-right extremist landscape to online regulation, as well as 6 webinars in partnership with the GIFCT on topics including open-source-intelligence, transparency reporting and accountability mechanisms.
- Published 8 podcasts on a range of topics, including on far-right violent extremism and terrorism, gamification, online regulation, accelerationism, as well as incels, online misogyny and gender-based terrorism.
- Participated in high-level stakeholder processes, including presentations at virtual events hosted by the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), the International Criminal Police Organisation (INTERPOL), United Nations Interregional Crime and Justice Research Institute (UNICRI), United Nations Office on Drugs and Crime (UNODC), as well as the European Union Internet Forum.
- Engaged with 20 tech companies through our Mentorship Programme, totalling to 25 mentees in our programme since it was established in 2018. Please see the section below on Mentorship for the key results yielded by the Mentorship and platforms' engagement.
- Alerted 38 tech companies of terrorist content on their platforms, through the Terrorist Content Analytics Platform. 105 tech companies were contacted and are ready to receive alerts for future terrorist content on their platforms.

- Reached out to 11 different tech companies and flagged over 300 pieces of content or accounts which are violent extremist, through our open-source intelligence (OSINT) work. This reporting of violent extremist content is outside of the scope of the TCAP and alerted via email to tech companies.
- Extended our knowledge in multiple areas of research:
    - Over the course of 2020, we have extended our knowledge regionally as well as technically to stay ahead of the evolving threat landscape. We have and will continue to extend our research on the risks of terrorists and violent extremist exploitation of emerging technologies and online services – such as gaming platforms, end-to-end-encryption, and terrorist operated websites. The aim of this extensive research is to ultimately help the tech industry understand the evolving terrorist and violent extremist threat landscape, both online and offline. We have also furthered our research into new areas including online regulation. This is exemplified through our Online Regulation Series, which we will continue to expand upon throughout 2021.

As we started 2021, we continued to build on the work done in 2020. Since the beginning of 2021, Tech Against Terrorism has focused on the following recent work and areas of research all of which have informed our support to smaller platforms:

- Continuing our E-learning Webinars Series, in partnership with the Global Internet Forum to Counter Terrorism (GIFCT)
- Further developing our Terrorist Content Analytics Platform
- Updating and re-launching the Knowledge Sharing Platform
- Expanding our open-source intelligence capabilities and investigations
- Publishing responses to regulations and consultation processes
- Publishing position papers
- Publishing transparency reporting guidelines for tech companies as well as governments
- Continuing our bespoke company support
- Strengthening our support for tech platforms through the Mentorship and Membership Programmes

## Areas of Research

- End-to-end-encryption
- Online regulation
- Terrorist Operated Websites
- Designation – Proscribed Organisations
- Gamification
- Government Transparency Reporting Initiatives

For a further in-depth look at our recent work, see our latest publication on our work in 2021 here.

## Feedback

In this report, we have provided a detailed summary of our activities in 2020 and first two quarters of 2021 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.

# KEY TVEC TRENDS IN 2020 & EARLY 2021

Below is a brief summary of some of the trends that our Open-Source Intelligence (OSINT) team has been tracking and responding to over 2020 and into 2021: Most trends outlined below have arisen partly as a consequence of improved content moderation by tech platforms in recent years, alongside the continued resilience and adaptability of terrorist networks online.

## Persistence of multi-platform approach by violent Islamist actors

Islamist terrorists and violent extremists have persisted in 2020-21 with a multiplatform approach to disseminating content across the web, utilising outlinks posted on core beacon channels or pages that lead to content hosted on predominantly small file sharing, paste and video sharing platforms. The strategy is highly likely to utilise file mirroring services, which enable internet users to upload content simultaneously across multiple platforms. It is intended to maximise the availability and reach of content, ensuring that it remains online for as long as it takes the slowest platform to remove it.

This long-standing trend was likely exacerbated by the Europol-led operation on Telegram in late 2019. That action temporarily decimated violent Islamist networks on Telegram and scattered them across the web onto smaller, more niche alternatives. We saw a gradual return to Telegram by networks affiliated with IS and al-Qaeda in 2020, but they maintain presence on a wider, more diffuse selection of messaging apps and platforms. Telegram has also become more effective at removing public violent Islamist channels and groups. This likely contributes to a violent Islamist extremist threat to other applications and platforms.

## Increased use of “cloud platform” websites

Islamist terrorist organisations including al-Qaeda, Islamic State (IS),and their supporter networks are increasingly exploiting open-source software to create “cloud platform” websites to store their content. These are password-protected websites that enable terrorist actors to share content via URLs. Many of these contain an extensive and regularly updated archive of terrorist material.

This trend is likely due in part to a broad improvement in moderation of terrorist content by mainstream tech platforms. Cloud platforms currently provide terrorist actors with a comparatively stable, centralised location in which to store their material. This is because the process of taking down cloud platforms is extremely challenging. As a result, content stored on cloud platforms can stay active without significant threat of being removed. Most cloud platforms monitored by Tech Against Terrorism exploit open-source software developed by Germany-based company NextCloud.

## Increased and diversified use of the decentralised web

The exploitation of the decentralised web –or Dweb –by terrorist and violent extremist (TVE) actors in recent months has both expanded and diversified. Messaging apps and social media platforms built on Dweb technology are serving critical roles in the online TVE ecosystem, ensuring the ongoing availability of terrorist content online. Decentralised web hosting software and file storage systems like Skynet and the InterPlanetary File System (IPFS), are also increasingly being exploited for the hosting of terrorist content. The administrators of a prominent pro-IS propaganda archive website, for example, have been using a Dweb browser plugin since at least late 2020 to circumvent frequent takedowns.. The plugin enables users to locate a stable landing page on which the latest link for the website can be found.

This shift is likely the result of a combination of improved moderation by centralised platforms and of a flawed perception among TVE actors that Dweb services cannot be moderated. We anticipate that TVE actors are likely to further expand their exploitation of Dweb services in the coming months, particularly if centralised platforms continue to make improvements in moderating terrorist content.

## Resurgence of terrorist operated websites

Tech Against Terrorism has been tracking a resurgence of the use of terrorist operated websites (TOWs) over the last year. TOWs are websites that are run by terrorist actors and have been created solely  to further the goals of a terrorist organisation or network. This may be through the dissemination or archiving of content, recruitment of members, or dissemination of official TVE correspondence or literature.

We assess that the resurgence of TOWs is likely a side-effect of broad improvements in social media platforms' content moderation efforts. As terrorist content moderation by mainstream platforms has strengthened, and the deplatforming of terrorist actors has become more widespread over the past few years, terrorist actors have been pushed onto increasingly niche platforms where the reach of their messaging is limited. As a result, terrorist actors and their supporters have increasingly supplemented accounts on smaller platforms with their own sites and platforms. TOWs are often still indexed on search platforms and are often more easily discoverable in comparison to private channels on niche messaging apps.

TOWs present significant challenges to counterterrorism practitioners, namely as the process of removing them is often more complex and time-consuming than the removal of content or actors from social media platforms. Engagement with infrastructure companies on suspected TOWs must be based on the principles of rule of law and freedom of expression, and any recommended action must be supported by a strong evidence base.

## Far-right extremist actors migrating to increasingly niche alt-tech platforms

We are seeing an ongoing migration of violent far-right actors to increasingly niche alt-tech video sharing platforms, as medium-sized platforms increase their capability to moderate and remove terrorist or violent extremist content. We have identified tens of violent far-right terrorist videos across a growing number of small new alt-tech platforms since the start of the year, some of which are likely to be violent extremist-run, based on our research.

Alt-tech platforms are often created in defiance over perceived notions of censorship on mainstream platforms that usually have high content standards. As alt-tech platforms champion themselves as advocates of "free-speech" and regularly boast that they host content that has been removed elsewhere online, these spaces become havens for TVE actors seeking to evade the strict parameters of mainstream platforms.

## Pro-IS content becoming more prevalent amid decline in official output

The output of IS'central propaganda channels has broadly dropped in both volume and frequency since at least early 2020. Currently, official IS channels mostly publish text-based communique claims of attacks, with one propaganda video on average being disseminated every month.

As there has been a decrease in official IS video and photo media in recent months, supporter-generated content has simultaneously diversified and become more prominent in the wider IS'online ecosystem. Multiple IS-supporter media channels publish a consistently high volume of multilingual pro-IS propaganda across different messaging apps and platforms, including pro-IS groups focused on specific regions or IS "provinces". IS itself has repeatedly recognised and encouraged this trend, most recently hailing the importance of support networks in its al-Naba newsletter in early June 2021.

.

## TVE supporter networks pose as news channels

Terrorist networks are increasingly attempting to operate on mainstream social media platforms by masquerading as legitimate news organisations. We have seen several coordinated efforts by supporter networks of designated terrorist organisations to disseminate content on mainstream platforms under the guise of"reporting" on current events.

The content posted by these networks is usually sanitised of direct references to terrorist organisations. Incriminating logos and images are obfuscated, and special characters are inserted into words to evade automated moderation. Content of this nature largely focuses implicitly on the operational successes of terrorist organisations, and instead subtly disseminates violent extremist narratives in support of the group.

A specialist and up-to-date understanding of terrorist use of the internet across platforms is therefore increasingly required for effective moderation of these networks, whose behaviour often adapts according to the platform on which they are operating. Their sophisticated understanding of platforms'Terms Of Service and content standards often results in terrorist content remaining available for several months at a time.

# ACTIVITIES IN 2020

As the Covid-19 pandemic caused lockdowns and travel bans, we focused on adjusting our work, knowledge-sharing, and outreach to the virtual landscape. In doing so, we increased our webinars, podcasts, as well as outreach to platforms.

## Outreach

The foundation to any successful partnership is trust. In order to build trust with the global tech industry, Tech Against Terrorism has devoted a lot of time towards industry outreach since our inception in 2017. 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.

## a. Tech Sector Engagement

Our tech company engagement can be broken down by the following workstreams: Tech Against Terrorism Mentorship and Membership programmes, the Terrorist Content Analytics Platform (TCAP), open-source intelligence, and knowledge sharing – such as our e-learning webinars.

As part of our open-source intelligence (OSINT) capabilities, we report violent extremist content which is found outside of the scope of the TCAP. In doing so, we reached out to 11 different tech companies – beyond our TAT mentees and members– flagging over 300 pieces of content or accounts which are violent extremist.

## b. Podcasts

In 2020, Tech Against Terrorism continued its podcast series. The Tech Against Terrorism podcast takes a deep dive into many of the different elements surrounding the terrorist and violent extremist online threat landscape and response to this exploitation.

Throughout the year, we produced 8 podcasts:

How Mainstream Media Can Spread Terrorist Propaganda (January 2020)

This episode explores how news media can provide some of the most effective PR for terrorists, by giving tremendous reach to their messages of hate and 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.
- Abdirahim Saaed, journalist for BBC Monitoring.

How Nordic neo-Nazis use the Internet (April 2020)

This episode explores how Nordic neo-Nazis are exploiting online platforms as a "safe haven" and how they exploit mainstream trends, such as memes, to spread their message and aid radicalisation on a global scale. This podcast also looks at some of the most prominent individuals in the Nordic neo-Nazi scene.

Guests:

- Jonathan Leman, researcher at Expo.
- Dr. Louie Dean Valencia-García, Assistant Professor of Digital History at Texas State University.

Far-right Violent Extremists and Meme Culture (April 2020)

This episode discusses how far-right violent extremists take advantage of the intrinsic virality of seemingly harmless online jokes to reach out to new audiences, penetrate mainstream culture and evade content moderation.

Guests:

- Maik Fielitz, researcher at the Jena Institute for Democracy and Civil Society, and fellow at the Centre of Analysis of the Radical Right.
- Lisa Bogerts, expert of visual communication
    - Both of them are contributors to the 2019 book, 'Post-Digital Cultures of the Far Right'.

How Are Terrorists and Violent Extremists Using Gamification? (May 2020)

This episode discusses how terrorist and violent extremists exploit gaming culture for their own ends. We look at how terrorists and violent extremists exploit gaming platforms to serve their own ideologies and purposes.

Guests:

- Linda Schlegel, senior editor at The Counterterrorism Group and regular contributor for the European Eye on Radicalization.
- Dr. Nick Robinson, associate professor in politics and international studies at the University of Leeds.

Regulating the Online Sphere (May 2020)

This episode discusses the ways in which online regulation is being pursued by companies, governments, and multi-lateral organisations. It also explores the implications of Facebook's new Oversight Board and what this really means for governance and accountability processes. It concludes by discussing whether we should use international human rights law as a framework for ruling the internet, and why terrorist content is such an important topic in regulatory discourse.

Guests:

- Evelyn Douek, lecturer in law and SJD candidate at Harvard Law School, and affiliate at the Berkman Klein Center for Internet & Society, studying international and transnational regulation of online speech.
- Daphne Keller, Director of Platform Regulation at Stanford's Cyber Policy Center – formerly Assistant General Counsel at Google and Director of Intermediary Liability at Stanford's Center for Internet and Society.

A Gender Approach to Women's Role in the Online Extremist Sphere (July 2020)

This episode considers the broader socio-cultural context of how gender is viewed in extremist ideology participation. In particular, it dwells on how understanding of gender identity, individuals' experiences, age, and social class influence the reasons one might join an extremist group.

Guests:

- Dr. Joana Cook, Assistant Professor on Terrorism and Political Violence at Leiden University, Senior Project Manager and an Editor in Chief at the International Centre for Counterterrorism.
- Dr. Elizabeth Pearson, lecturer at the Cyber Threats Research Centre at Swansea University who specialises in gender, extremism, and counter extremism.

Trend Alert: Accelerationism (September 2020)

In this episode, our guests discuss why accelerationism has become a flagship doctrine of far-right violent extremism, and the emergence of accelerationist subcultures. In particular, the guests focus on how accelerationist used the Covid-19 pandemic to "initiate the collapse of society", and the rise in media attention on accelerationism in the US.

Guests:

- Professor Matthew Feldmann, Director of the Centre for Analysis of the Radical Right (CARR), and an expert on fascist ideology, neo-Nazism and "lone actor" terrorism.
- Ashton Kingdon, PhD student at the University of Southampton and fellow at CARR, whose research focuses on how far-right extremists use technology for recruitment and radicalisation.
- Ben Makuch, national security reporter with Vice News, who investigates far-right violent extremism, particularly neo-Nazism.

Incels, Online Misogyny and Gender-based Terrorism (October 2020)

In this podcast, the speakers consider what measures technology companies can take to counter incel groups on their services – such as partnering with entities that have expertise in countering these forms of extremism. They underline how incels and wider misogyny are a problem both offline and online, and how countering these issues requires collective action from both spheres. They also argue that some forms of incel violence should be seen as gender-based terrorism.

Guests:

- Dr. Debbie Ging, Associate Professor in the School of Communications at Dublin City University.
- Alex DiBranco, the Co-Founder and Executive Director of the Institute for Research on Male Supremacism.

## Weekly Reader's Digest

In early 2020, Tech Against Terrorism introduced its Reader's Digest, a weekly selection of top stories and review of insightful articles about terrorist and violent extremist use of the internet, counterterrorism, and tech policy. We also include updates on Tech Against Terrorism's work and media appearance.

The Reader's Digest is shared every Friday. You can find past editions of the digest and newsletters on our website. You can subscribe to our Digest and Newsletter here.

# TAT IN THE MEDIA

In 2020, media coverage of our work was featured in interviews, news articles and publications from global media throughout the year. Below is a selection of media that cited our work:

A sorry site: 8chan gets the axe, raising questions about internet censorship: In this article on Cloudflare's decision to stop its service provision to 8Chan, the New Economy spoke with Tech Against Terrorism's Flora Deverell and Jacob Berntsson about the lack of global consensus when it comes to terrorist and violent extremist content online.

Combatting Online Extremism: Global Defence interviewed Jacob Berntsson, to discuss the challenges in tackling terrorist use of the internet, Tech Against Terrorism's work with smaller tech companies, and on facilitating cross-sector collaboration.

3 Questions to Jacob Berntsson: Renaissance Numérique interviewed Jacob Berntsson to discuss the work of Tech Against Terrorism and how we can support tech platforms, notably through the Terrorist Content Analytics Platform.

'Alt-tech' attracts growing number of extremists in Britain: In July 2020, Tech Against Terrorism was quoted in the Telegraph on the rise of "alt-tech" platforms as a result of mainstream social media platform removing extremist and terrorist content from their platforms.

Asking the big social media companies to remove extremist content more quickly will do little to fight terrorism: Tech Against Terrorism's Director Adam Hadley, in an op-ed in the Independent, cautioned that asking big platforms to take down extremist content more quickly is not a solution to either terrorism or terrorist use of the internet.

Following a terrorist attack in Vienna on Monday, 2 November, our Director, Adam Hadley, discussed terrorist use of the internet, in particular of social media, and the related challenges of identifying terrorist content at scale with John Pienaar on Times Radio.

Social media firms must face sanction for 'anti-vax content', demands Labour: Our director, Adam Hadley, as founder of our parent organisation the Online Harms Foundation, was quoted in an article on a proposal made by the UK Labour Party to introduce fines for tech companies failing to act to "stamp out dangerous anti-vaccine content".

Online harms bill: firms may face multibillion-pound fines for illegal content: Our Director, Adam Hadley, commented on behalf of our parent foundation the Online Harms Foundation on the UK regulatory framework for online harms, which sets out new guidelines for tech companies removal of terrorist and other "harmful" online content.

## Recognition of our work

Tech Against Terrorism's work in supporting the tech industry in countering terrorist use of the internet was highlighted by the 2019 US Department of State's Country Reports on Terrorism.

## Events and webinars

In 2020, Tech Against Terrorism attended and presented at various virtual conferences. Participation in these events allowed us to further consolidate our collaboration with organisations we have been working with for the past few years and develop new working relationships.

- In January, our Director, Adam Hadley, presented at UN CTED's and the UN Counter Terrorism Committee's open meeting on countering terrorist narratives in New York.

- In January, we continued our engagement with the Mayor of London's Civic Innovation Challenge, giving a presentation around best practice in tackling terrorist use of the internet for the companies taking part in the challenge at TechUK.

- In February, Jacob Berntsson participated in the "Foreign Terrorist Fighters – Addressing the Current Challenge" conference in Vienna. During this high-level event – jointly organised by UNOCT, the OSCE and Switzerland – he presented on the issue of online recruitment of foreign terrorist fighters, and the need for cross-sector collaboration to counter it.

- On 5 May, Tech Against Terrorism contributed to a virtual EU Internet Forum meeting on far-right violent extremist and terrorist use of the internet, sharing insights from our research on far-right terrorist use of online platforms. This meeting was the first EU Internet Forum meeting addressing far-right violent extremism and terrorism.

- On 23 July, Tech Against Terrorism presented at GIFCT's Multi-Stakeholder Summit, which took place under the leadership of newly appointed executive director Nicholas Rasmussen. This was the fourth GIFCT summit, the first one having been organised by Tech Against Terrorism in 2017, and the first summit for the GIFCT as an independent organisation. The summit saw presentations from a range of stakeholders, the recordings of which you can find here. During the Summit, the different GIFCT working working groups were also introduced. Tech Against Terrorism is delighted to chair the working group on technical approaches, which you can read more about here.

- Adam Hadley spoke at the first conference organised by the Safety Tech Innovative Network, an initiative set up by the UK's Ministry for Digital, Culture, Media and Sports (DCMS), Nominet and KTN on mental health considerations in content moderation, and the potentially negative effects experienced by content moderators.

- Tech Against Terrorism also spoke at a webinar on money muling organised by ComplyAdvantage and FINTRAIL, highlighting the role of social media and financial services in crime and terrorist financing. To watch the recording of this webinar, please click here.

- On 14 October, Adam Hadley joined the discussion on "Counter-terrorism strategy in a post-COVID environment", organised by Wilton Park, to talk about the cyber terrorist threat.

- On 26 October, Jacob Berntsson took part in the EU Internet Forum workshop on "Right-wing terrorist groups and symbols online", giving opening remarks on the importance of supporting smaller platforms to counter the spread of terrorist and violent extremist content online.

- On 30 October, Adam Hadley gave opening remarks during the expert group meeting on "Recently developed operational notes to assist service providers with requests from overseas criminal justice officials for electronic evidence". This meeting gathered 21 service providers, and was organised by the UNODC, in consultation with the UNCTED and Tech Against Terrorism.

- In late November, Adam Hadley took part in the third INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement, presenting during a panel dedicated to "Tapping into AI to Fight Crime – Terrorist Use of the Internet and Social Media".

- On 18 December, our OSINT Analyst, Arthur Bradley, presented on the novel digital terrorist modus operandi in the Middle East and North Africa Region at a workshop organised by the UNODC for Lebanon on "The use of electronic evidence and sensitive intelligence in cross-border investigations of emerging terrorist threats"

# KNOWLEDGE SHARING

## Original Research & Publications

In 2020 we ramped up our regular research output and quantitative analysis of terrorist use of internet and tech sector's response. Below is a selection of the research and analysis we produced.

### Transparency reporting for smaller platforms (March 2020)

We published a blogpost on the challenges of transparency reporting faced by smaller tech platforms, including our recommendations for government and tech companies. Whilst transparency reporting is an important way for the tech sector to increase awareness of its internal content moderation decision-making processes and to increase transparency around information and takedown requests made by external entities, smaller tech platforms might lack the capacity to regularly capture the relevant data and publish transparency reports.

### The designation of the Russian Imperial Movement by the US State Department: why it matters for tech companies (May 2020)

In April, the US Department of State proscribed the Russian Imperial Movement as a specially designated global terrorist entity – the first time the US gave such a designation to a far-right violent extremist entity. Tech Against Terrorism welcomed this designation as it will help facilitate an improved tech sector response to online manifestations of far-right terrorism. We encourage states to use legal powers to promote rule of law through comprehensive terrorist designation lists. You can read our blogpost on this designation here.

### The EU's Terrorist Content Regulation: Concerns about Effectiveness and Impact on Smaller Tech Platform (July 2020)

Tech Against Terrorism commented on the EU draft regulation on preventing the dissemination of terrorist content for VOX-Pol.[10] In this piece, we highlighted concerns we have with the regulation, particularly with regards to smaller and newer tech platforms. In our view, smaller companies will likely struggle to comply with the regulation's requirements, such as the one-hour removal deadline. We also shared some concerns we have about the regulation's potential impact on freedom of expression and the rule of law.

### Covid-19: far right violent extremism and tech platforms' response (November 2020)

The Fondation pour L'Innovation Politique (Fondapol) published our analysis of the online exploitation of Covid-19 by violent far-right extremists and tech platforms' response to the increase in misinformation, conspiracy theories and extremist content in the early months of the pandemic. You can find the report in English here.

### The Terrorist Content Analytics Platform and Transparency by Design (November 2020)

In November, we published an article on Vox-Pol about the TCAP, detailing how it is being developed in a "transparency by design" approach. Our piece was a response to an article by the Electronic Frontier Foundation's (EFF) outlining concerns with automated moderation tools.

### Terrorist Use of the Internet (December 2020)

In December, we wrote in the Counter Terror Business Magazine on terrorist use of the internet, and what we at Tech Against Terrorism are doing to tackle the threat. The article highlights the exploitation of smaller platforms as well as the lack of resources that such companies face. It underlines the need for support as well as specific solutions to tackle this threat to smaller platforms

10. This draft regulation was recently passed. To read our statement on it, please see here.

## Online Regulation Series

In October 2020, we conducted the first edition of the Online Regulation Series, our latest knowledge sharing endeavour aimed at shedding light on the state and future of online regulation globally, in particular with regard to terrorist and extremist content. Throughout the series, we provided regular blogposts on different countries'regulatory frameworks, covering a different region each week. We also provided an overview of tech sector's initiatives for content governance, and insights from academic and expert perspectives on online regulation.

During the Online Regulation Series we published 17 country-specific blog posts as well as 3 blog posts on tech sector initiatives and insights from academia:

- Asia-Pacific: Singapore, Pakistan, The Philippines, Australia, India
- North America: US, Canada
- Europe: EU, France, Germany, UK, Turkey
- MENA and Sub-Saharan Africa: Morocco, Kenya
- South America: Brazil, Colombia
- Tech sector initiatives
- Academia perspectives: Insights from Academia I, Insights From Academia II – The future of online regulation

We concluded the Online Regulation Series with a webinar on The State of Global Online Regulation, welcoming tech policy and digital rights experts to share insights on key regulations around the world that might shape the future of online regulation. If you would like to access a recording of this webinar, you can reach out to us at contact@techagainstterrorism.org.

In 2021, we will continue our research and analysis on the global state of online regulation, both by tracking ongoing regulations as well as through drafting and launching our Online Regulation Series Handbook. The Online Regulation Series Handbook was launched in July 2021, and provides insight and analysis of over 60 regulations and legislative proposals in 17 countries, and includes our recommendations for policymakers. You can access the handbook here.

## 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, 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.

### E-learning session: OSINT introduction to the current Islamist terrorist landscape (March 2020)

In this webinar, we took a closer look at the Islamist terrorist landscape online. We highlighted the latest trends and challenges, and discussed strategies and tactics to tackle this problem whilst respecting human rights.

Speakers:

- Adam Hadley, Director of Tech Against Terrorism.
- Lorand Bodo, OSINT analyst at Tech Against Terrorism.

### Transparency reporting for smaller tech platforms (April 2020)

This webinar welcomed Reddit's Policy Lead Jessica Ashooh, Facebook's Former Head of Counterterrorism and Dangerous Organisations Policy for EMEA, Dr. Erin Saltman, and Emma Llanso, Director of the Free Expression Project at the Center for Democracy and Technology. The panel discussed the importance and role of transparency reporting, as well as shared resources and best practice for smaller tech companies looking to create their own transparency reports. For a full summary of this webinar, please see here.

Speakers:

- Flora Deverell, Research Analyst at Tech Against Terrorism.
- Dr. Erin Saltman, Former Head of Counterterrorism and Dangerous Organisations Policy for EMEA at Facebook.
- Jessica Ashooh, Director of Policy at Reddit.
- Emma Llanso, Director of the Free Expression Project at the Center for Democracy & Technology.

### Tech sector and law enforcement engagement in countering Terrorist Use of the Internet (May 2020)

The webinar aimed to increase understanding of each sector's online counterterrorism practices, with the tech sector representatives sharing insights on their companies' work on law enforcement collaboration and digital evidence.

Speakers:

- Jacob Berntsson, Research Manager at Tech Against Terrorism.
- Courtney Gregoire, Chief Safety Digital Officer at Microsoft; Experts from EU IRU, Europol.
- Jessica Marasa, Law Enforcement Response Manager at Twitch.
- Stephanie McCourt, Trust & Safety Outreach Lead at Facebook.

### Accountability Mechanisms for Tech Platforms (July 2020)

During this webinar, we explored accountability practices within the tech sector, how they have evolved, and where they will go next. The speakers provided insights into the importance of accountability for tech platforms and the challenges such mechanisms entail. You can read a full summary of the webinar here.

Speakers:

- Maygane Janin, Research Analyst, Tech Against Terrorism.
- Zoe Darme, Business Programme Manager, Microsoft (GIFCT).
- Jillian York, Director, International Freedom of Expression, Electronic Frontier Foundation.
- Dina Hussein, Counter Terrorism and Dangerous Orgs, Facebook.
- Sean Li, Director, Trust & Safety, Discord.

### Tech Against Terrorism Mentorship Programme and Support for Smaller Platforms (October 2020)

During this session, we discussed the Mentorship process, the requirements for Tech Against Terrorism Membership, and the different benefits that platforms can get by joining our Mentorship and Membership Programmes. We were joined by our partners at the GIFCT to present on the GIFCT membership.

Speakers:

- Adam Hadley, Director, Tech Against Terrorism.
- Nicholas Rasmussen, Executive Director, GIFCT.
- Johannah Lowin, Chief of Staff, GIFCT.
- Maygane Janin, Research Analyst, Tech Against Terrorism (Moderator).

### Content Moderation: Alternatives to Content Removal (December 2020)

For this webinar, we took a deeper look at content moderation practices within the tech sector, the objectives they serve and desired outcomes. We focused on strategies deployed by tech companies to ensure an efficient and appropriate moderation of their platforms without solely relying on content removal. In doing so, we questioned the efficiency and challenges related to content removal and deplatforming for terrorist and violent extremist material and actors, weighing this up in relation to other moderation strategies.

Speakers:

- Jacob Berntsson, Research Manager, Tech Against Terrorism.
- Johannah Lowin, Chief of Staff, Global Internet Forum to Counter Terrorism.
- Alex Feerst, GC, Neuralink & Advisor, Trust and Safety Professional Association.
- Bill Ottman, CEO, Minds.
- Rachel Wolbers, Public Policy Manager, Facebook Oversight Board.

## Tech Against Terrorism Webinars

In addition to the e-learning series, we organised a number of Tech Against Terrorism webinars.

### Virtual OSINT Breakfast (March 2020)

In this virtual breakfast, we discussed location intelligence, Twitter analytics tools, accelerationist far-right violent extremists and the Covid-19 crisis.

Speakers:

- Chris Poulter, Founder & CEO, OSINT Combine.
- Francesco Poldi, OSINT expert.
- Amine Ghoulidi, Researcher, Kings College London.
- Lorand Bodo, OSINT Analyst, Tech Against Terrorism.

### OSINT Introduction to the online far right violent extremist landscape (March 2020)

In this session, we discussed international far-right violent extremism and terrorism trends and best practise to monitor terrorist behaviour. We also explored how to respond to threats and disrupt terrorist use of the internet.

Speakers:

- Matthew Feldman, Director of the Centre for the Analysis of the Radical Right.
- Emily Thompson, Research Assistant at Museum of Tolerance.
- William Allchorn, Associate Director of the Centre for the Analysis of the Radical Right.
- Professor Megan Squire, Professor of Computer Science at Elon University and a Senior Fellow at the Centre for the Analysis of the Radical Right.
- Lorand Bodo, OSINT Analyst at Tech Against Terrorism.
- Miro Dittrich, Project Lead at Amadeu Antonio Stiftung.

### Terrorist Content Analytics Platform: Update call for academics and researchers (May 2020)

In this webinar, we updated academics and researchers on our progress in developing the TCAP.

Speakers:

- Adam Hadley, Director of Tech Against Terrorism.
- Alexander Corbeil, Research Advisor at Public Safety Canada.
- Dr. Shiraz Maher, Director of the ICSR.
- Peter King, Consultant on extremist media and Director at IbexMind Ltd, Consultant on the Terrorist Content Analytics Platform (TCAP) at Tech Against Terrorism.
- Tom Lancaster, Product Manager at Tech Against Terrorism.

### Online Regulation Series – Concluding Webinar: The State of Global Regulation (November 2020)

During this webinar, we welcomed a panel of regional experts to discuss the global regulatory approaches we had covered throughout the Online Regulation Series. We focused on the emerging trends for online regulations globally, and the potential concerns for smaller platforms and freedom of speech online.

Speakers:

- Maygane Janin, Research Analyst, Tech Against Terrorism
- Jason Pielemeier, Policy Director, Global Network Initiative.
- Smitha Krishna Prasad, Director, Center for Communication Governance at the National Law University Delhi.
- Professor Paul M. Barrett, Deputy Director, NYU Stern Center for Business and Human Rights.
- Christoph Schmon, International Policy Director, Electronic Frontier Foundation.
- Bruna Santos, Advocacy Coordinator, Data Privacy Brazil Research Association.
- Fabienne Tarrant, Research Assistant, Tech Against Terrorism (Moderator).

### Cooperation between the UN and smaller tech platforms in countering use of the Internet for terrorist purposes (December 2020)

This webinar, organised in partnership with the United Nations Counter Terrorism Executive Directorate (UNCTED), focused on how intergovernmental organisations can support the tech sector in countering terrorist use of the internet whilst respecting human rights. This webinar focused on cooperation between the UN and smaller tech platforms in countering use of the internet for terrorist purposes, and saw flash introductions from UN CTED, United Nations Office on Drugs and Crime (UNODC), United Nations Office of Counter-Terrorism (UNOCT), Office of the United Nations High Commissioner for Human Rights (UNOHCHR), The United Nations Interregional Crime and Justice Research Institute (UNICRI), and United Nations Development Programme (UNDP).

Speakers:

- ASG Michèle Coninsx, Executive Director, UNCTED; USG Fabrizio Hochschild, Special Adviser to the UN Secretary-General.
- Adam Hadley, Director, Tech Against Terrorism.
- Dr Jehangir Khan, Director, UNCCT, OCT
- Peggy Hicks, Director of OHCHR's Thematic Engagement, Special Procedures and Right to Development Division, OHCHR.
- Masood Karimipour, Chief of Terrorism Prevention Branch, UNODC.
- Dr Samuel Rizk, Head of Conflict Prevention, Peacebuilding & Responsive Institutions, UNDP.
- Leif Villadsen, Deputy Director, UNICRI.
- Lina Cepeda, Legal Officer, UN CTED;
- Dina Hussein, Policy Manager, Counter Terrorism and Dangerous Organisations, Facebook.
- Dr. David Scharia, Chief of Counter Terrorism Branch, UNCTED.

If you would like to access a recording of any of the above-mentioned webinars, please reach out to us at contact@techagainstterrorism.org.

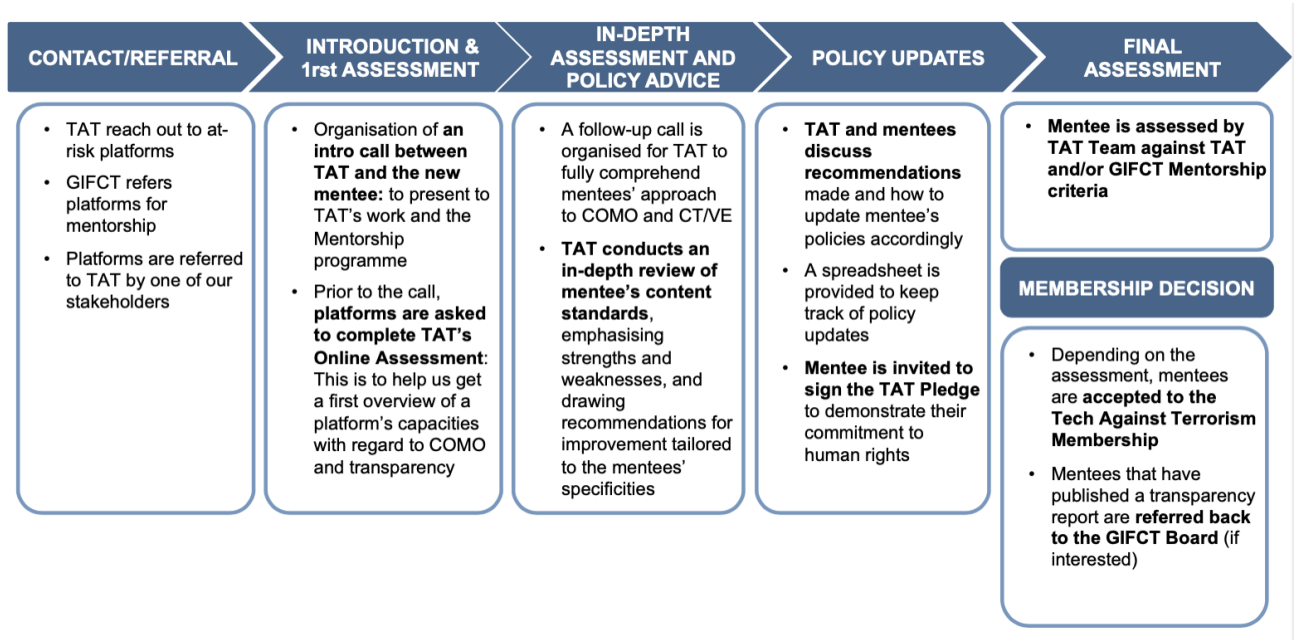
# TAT MENTORSHIP & MEMBERSHIP PROGRAMMES

## Mentorship Programme

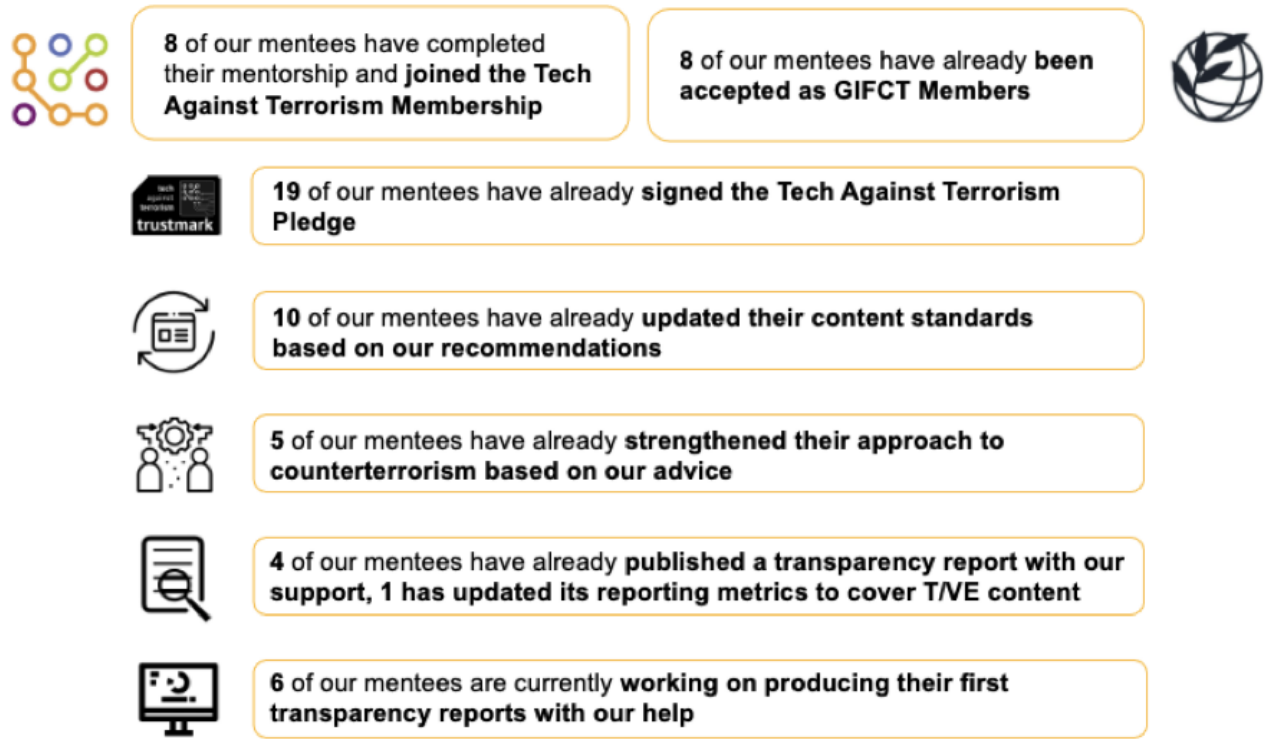
Since 2018, we have mentored 25 tech companies to help them tackle terrorist use of their platforms whilst respecting human rights. This practical support programme has significantly raised tech sector capacity to respond. The Mentorship Programme helps smaller platforms in improving and future-proofing their policies and enforcement mechanisms.

Our mentorship programme also supports tech platforms in strengthening transparency and accountability mechanisms around content moderation. In 2020, through our Mentorship programme, we engaged with 20 tech companies, totalling to 25 mentees in our programme since it was established in 2018.

The diagram below shows the steps involved in the Tech Against Terrorism mentorship process:



The below chart displays the key results of Tech Against Terrorism's Mentorship Programme for 2020.




## Membership Programme

Launched in 2017, the Tech Against Terrorism Membership is aimed at sharing best practice with tech platforms to help them build capacity in tackling terrorist exploitation. This provides ongoing support following the mentorship process to ensure that we can continue assisting platforms as the threat landscape evolves. Our Membership scheme is aimed at facilitating constructive working relationships built on trust with the global tech sector. The Tech Against Terrorism initiative is global and covers all technology that risks being exploited by terrorism and violent extremists. Our Membership is inclusive and we welcome tech companies of any size, region, technology, or service, offering to apply to become a member.

Throughout the mentorship process, we assist tech platforms in updating their policies and processes to meet the TAT and GIFCT membership requirements. A central pillar to our support for smaller tech platforms, our Membership programme is meant to provide continuous and long-term support to tech platforms. We work to build trusted relationships with platforms to help them counter terrorist and violent extremist exploitation of their services and stay ahead of the threat. Our mentorship programme partially supports the Global Internet Forum to Counter Terrorism (GIFCT), and is designed to assist tech companies in meeting the TAT and GIFCT Membership criteria.

Throughout the mentorship process, we assist tech platforms in updating their policies and processes to meet the TAT and GIFCT membership requirements.

| TECH AGAINST TERRORISM MEMBERSHIP CRITERIA |
| --- |
| 1. Explicit prohibition of terrorism in Content Standards |
| 2. Ability to receive reports on content violation CSs and act on it |
| 3. Commitment to transparency reporting |
| 4. A desire to explore new technical solutions |
| 5. A public commitment to respecting human rights, particularly freedom of expression and privacy |
| 6. Civil society support |
| 7. Ability to receive user appeals and act on it (not necessary for GIFCT membership) |
| **GIFCT MEMBERSHIP ADDITIONAL CRITERIA** |
| 8. Published transparency reports |

## Membership Plus Services

Tech Against Terrorism can also provide bespoke support in other areas as required by tech platforms to support their counterterrorism and transparency efforts. Companies will be provided with a dedicated Tech Against Terrorism point of contact that will oversee companies'needs throughout the entire process. To learn more about the topics covered within our bespoke company support, please see the section on TAT's catalogue of services and bespoke support.

## Mentorship Going Forward

In 2021, we are updating and expanding upon our Mentorship Programme. This applies to our policy and OSINT support. We will also ensure to further direct discussions and communications with our members through a dedicated Slack space, as well as through increased meetings, roundtables, and consultations.

## Policy Support

- We will conduct an updated Content Standards Review of our Members' policies every year. Members will additionally be able to submit policies that are being drafted for our review prior to their publication.

## OSINT Support

- We will be providing regular bespoke OSINT briefs for members, as well as terrorist use of the internet overview briefs.

## Slack Space

- This Slack space, reserved for tech companies regularly engaging with Tech Against Terrorism, is meant to create a direct and private means of communication between the Tech Against Terrorism team and our tech company stakeholders, whilst fostering a trusted and inclusive network. Through this medium, we will also share various information and resources of interest regarding, amongst others, the evolving terrorist and violent extremist online space, counterterrorism and content moderation policies, as well as how to promote transparency and accountability within the tech sector.

## Regular TAT members meetings, roundtable, and consultations

- TAT Member Meetings will provide an opportunity for us to update our member companies on our most recent work and projects, and how these relate to the policy and practical support we provide to our member companies. It will additionally allow us to present on our most recent open-source intelligence findings to update our members on the evolving terrorist and violent extremist online threat. Finally, members will be asked to provide their feedback on our work and to let us know where we should provide additional support.
- We will also organise roundtables and consultations on important workstreams such as transparency reporting processes, designation of terrorist groups, and information on terrorist operated websites.

## Membership Going Forward

In 2020, we also introduced changes to our criteria for Membership and compliance process

- In line with our commitment to support meaningful accountability from the tech sector, we added a seventh criterion for acceptance to our Membership: user appeal process.

As of January 2021, all tech companies interested in joining the Tech Against Terrorism membership will be required to have an appeal system in place for users to submit user appeal requests for contents and accounts removed or otherwise actioned.

User appeals are a key component of a platform's accountability towards its users as they ensure the possibility to contest a decision and be more informed about the thought process behind takedowns. This is an important safeguard for freedom of speech online, and it increases accountability towards users.

For mentees and members that joined before January 2021, we will support them to develop the necessary user appeal policy and process to ensure that all meet the requirements of membership.[11]

- To ensure compliance with the membership requirements, and continuous policy support Tech Against Terrorism is introducing yearly compliance review for all members.

The compliance review is based on the in-depth policy review we conduct and share with each prospective member at the beginning of their Mentorship process. This policy review serves as the basis of our yearly compliance review, alongside policy updates and new resources made available by the platform to its users. As for all Tech Against Terrorism's policy reviews, we also assess transparency efforts, in particular improvements in transparency reporting.

11. This criterion does not apply for members and mentees who joined prior to 2021. This means that mentees who joined in 2020 but are completing their mentorship in 2021 will not be assessed based on that, and existing members will not have their membership suspended.

Yearly compliance reviews of platforms' policies will also allow us to provide updated recommendations, informed by the evolution of the online terrorist and violent extremist threat, and by the changing regulatory landscape. This will help platforms continuously strengthen and adapt their counterterrorism and transparency efforts.

# OPPERATIONAL SUPPORT

## Terrorist Content Analytics Platform (TCAP)

### Background

The Terrorist Content Analytics Platform (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:

- To support tech companies in detecting terrorist content on their platforms, such as by alerting them with terrorist content, helping inform and manage company moderation procedures as companies will also be able to securely examine verified terrorist content on the TCAP.
- 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.
- 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.
- 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.

At the end of June 2019, the Government of Canada announced that they would provide funding towards the development of the TCAP. In 2019, we commenced pre-development preparation, including launching a public consultation process.

In 2019, Tech Against Terrorism conducted an online consultation process on the TCAP. This process was open to the public and sought input from three specific categories of stakeholders: tech companies, academic researchers, and civil society groups.

## 2020 Update

In May 2020, we organised a virtual meeting to update academics and expert researchers on progress in designing the platform, as well as on how the TCAP will support research on terrorist use of the internet.

In August 2020, we published a report on the public online consultation process on Terrorist Content Analytics Platform (TCAP). The release of this report is an important step as part of our commitment to ensure that the TCAP is developed in a transparent manner whilst respecting human rights and fundamental freedoms, including freedom of speech. Read the report here to learn more about key findings from this process.

In November 2020, we successfully launched automated terrorist content alerts powered by the Terrorist Content Analytics Platform (TCAP). The TCAP sends email alerts to tech companies when identifying terrorist content hosted or shared on their platform. In the first stage, we have included over 60 small, medium and large tech platforms representing various online services, including social media, file-hosting and content streaming. This number has expanded since November 2020.

In December 2020, we published our policy for inclusion of designated terrorist groups in the Terrorist Content Analytics Platform (TCAP). We also hosted our monthly office hours to update our stakeholders on the development of the platform.

In 2020, we also announced that the first version of the TCAP would also include online content produced by government designated far-right terrorist groups. This meant that we expanded the scope of the first version of the TCAP from Islamic State (IS) and al-Qaeda content.

## Office Hours

In October 2020, we held our first office hours for the Terrorist Content Analytics Platform (TCAP). These office hours are bimonthly hour-long sessions that provide an update on the development of the platform, as well as answer any questions interested stakeholders might have. We hosted our second session of the TCAP office hours in early November and the third in December. This is one of the steps we are taking to ensure that the platform is developed in a transparent manner.

If you were unable to attend our office hours, please contact us for a recording of the session. If you would like to take part in future sessions, please visit the TCAP website to stay up to date for any announcements of upcoming sessions throughout 2021.

## Alerts

In 2020, the TCAP alerted terrorist content to 38 tech companies. 105 tech companies were made ready to receive alerts for future discovery of terrorist content on the platform. A breakdown of the first month of the TCAP is included below. Please note that since these statistics, we have significantly expanded our efforts.

For more information on the TCAP, please visit the website here. For project news and updates, please register for our monthly newsletter here.

**First Month of TCAP:**

**Period:** November 20 – December 17

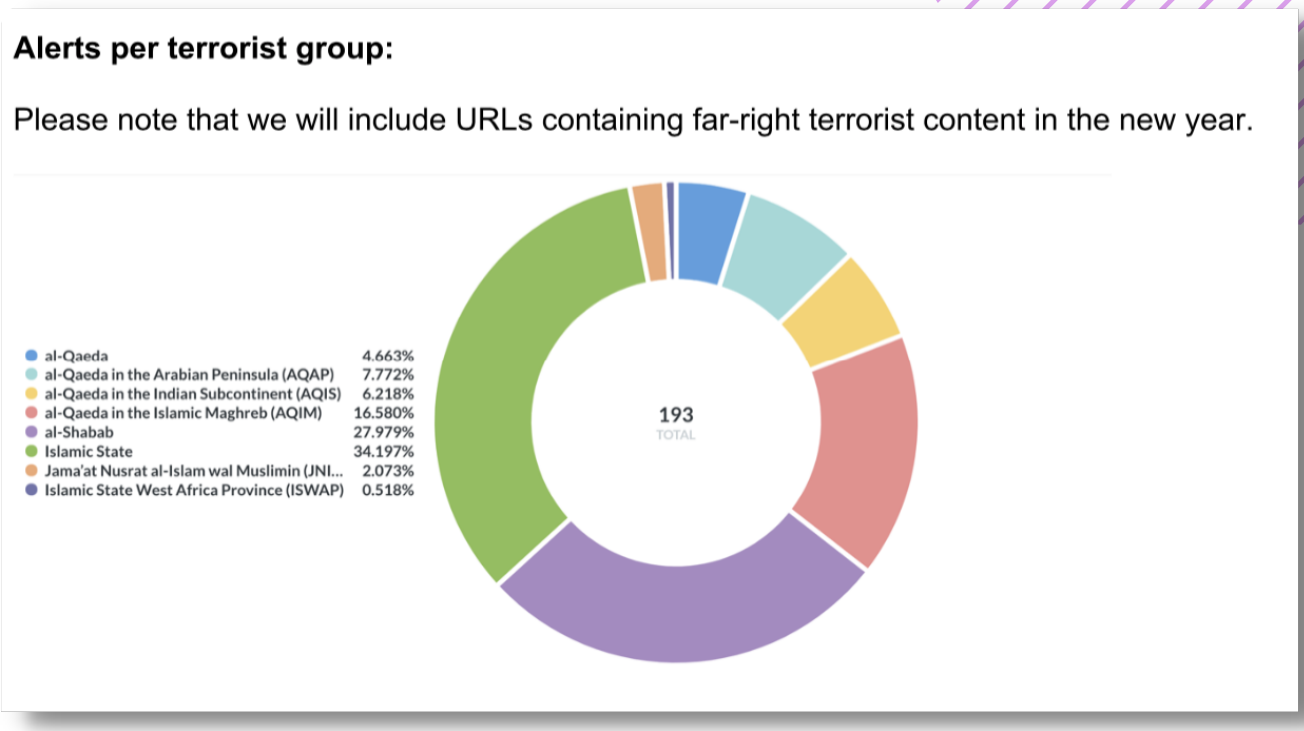
**Time of writing:** 18 December 2020

**Submissions:** 620

**Alerts:** 193

**Alerts per terrorist group:**

Please note that we will include URLs containing far-right terrorist content in the new year.




## TAT's Catalogue of services and bespoke support

We continue to deliver bespoke research and analysis as well as risk assessments for tech companies.

Our bespoke services include:

- Research and Analysis
- Threat Intelligence and risk assessments
- Policy guidance
- Crisis coordination response
- Data-driven solutions support

In 2020, we started delivering bespoke research and analysis as well as risk assessments for tech companies. To see the topics we explore within the research and analysis, please see the section on our extended knowledge.

Please get in touch with us at contact@techagainstterrorism.org if you would like to request more detail.

# PARTICIPATION IN STAKEHOLDER PROCESSES

## Events

Last year, Tech Against Terrorism continued its engagement with several ongoing processes and projects geared toward counterterrorism and countering violent extremism efforts. Below are some examples of where Tech Against Terrorism was invited to influence the direction of the program by providing evidence, or research insights. 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.

### UNCTED and the UN Counter Terrorism Committee

In January, our Director, Adam Hadley, presented at UN CTED's and the UN Counter Terrorism Committee's open meeting on countering terrorist narratives in New York.

### Foreign Terrorist Fighters – Addressing The Current Challenge

We started 2020 by participating in the "Foreign Terrorist Fighters – Addressing The Current Challenge" conference in Vienna. During this high-level event – jointly organised by UNOCT, the OSCE and Switzerland – our Research Manager Jacob Berntsson presented on the issue of online recruitment of foreign terrorist fighters, and the need for cross-sector collaboration to counter it.

## GIFCT Technical approaches working group

With the Global Internet Forum to Counter Terrorism (GIFCT) formalising its work as an independent organisation this year, we are delighted to announce that Tech Against Terrorism is the chair of the GIFCT's technical approaches working group. The working group works to identify opportunities for the innovative deployment of Artificial Intelligence (AI) and advanced analytics in identifying terrorist content and supporting platforms in effectively moderating terrorist content. Read our press release here.

## Global Network on Extremism and Technology Research Consortium

Tech Against Terrorism has joined the Global Network on Extremism and Technology's (GNET) research consortium in a "specialist support" capacity. We will leverage our work with the tech industry to support policy and practically oriented research at GNET, and support the development of ethical research standards on online terrorist content. To learn more about our partnership with GNET, read our press release here.

## Tech Against Terrorism Advisory Group and Experts Committee

Tech Against Terrorism held a virtual meeting for its Advisory Group and Experts Committee on 27 May 2020. This meeting followed up on the one held in 2019 at the UN CTED's headquarters in New York during the UN General Assembly week. In the 2020's meeting Tech Against Terrorism provided an update on its work around its core activities of outreach, knowledge-sharing, and practical support for the tech sector. The meeting saw opening remarks from ASG Michele Coninsx, Executive Director of UN CTED. Tech Against Terrorism would like to express its gratitude to our stakeholders who attended this meeting, including UN CTED, the governments of Canada, United States, United Kingdom, Switzerland, and Jordan, the European Commission, Europol, the Commonwealth, Facebook, Google, Access Now, VOX-Pol, and Swansea University.

## EU Internet Forum

On 5 May Tech Against Terrorism contributed to a virtual EU Internet Forum meeting on far-right violent extremist and terrorist use of the internet, sharing insights from our research on far-right terrorist use of online platforms. This meeting was the first EU Internet Forum meeting addressing far-right violent extremism and terrorism.

### GIFCT Summit

The 2020 GIFCT Multi-Stakeholder Summit took place on 23 July under the leadership of newly appointed executive director Nicholas Rasmussen. This is the fourth GIFCT summit, the first one having been organised by Tech Against Terrorism in 2017, and the first summit for the GIFCT as an independent organisation. The summit saw presentations from a range of stakeholders – including Tech Against Terrorism – recordings of which you can find here. During the course of the event, the different working groups were also introduced. Tech Against Terrorism is delighted to chair the working group on technical approaches, which you can read more about here.

### INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement

In late November, our Director, Adam Hadley, took part in the third INTERPOL-UNICRI Global Meeting on Artificial Intelligence for Law Enforcement, presenting during a panel dedicated to "Tapping into AI to Fight Crime – Terrorist Use of the Internet and Social Media".

### OCED Transparency Reporting

Finally, in 2020, we took part in the OECD's process on transparency reporting on TVEC.

## Consultations

Throughout 2020, Tech Against Terrorism took part in several consultations, including:

### EU Digital Services Act (DSA)

In September, we released our response to the consultation process for the EU Digital Services Act (DSA), which was organised to seek input on issues that will help shape the EU's rulebook on digital affairs. In our response, we highlighted three areas that we deem essential in guiding the EU in creating policies that tackle terrorist use of the Internet. Our full response can be found here.

## UK Ofcom

Until the United Kingdom Online Harms regime – aiming to counter harmful content online and announced in a White Paper in April 2019 – is implemented, there will be an interim regime with UK communications regulatory body Ofcom acting as regulator for online Video-Sharing Platforms (VSPs) in order to meet the UK's obligations under the EU's Audiovisual Media Services Directive (AVMSD) 2018.

Ofcom will be given new powers to regulate UK-established VSPs. This includes ensuring that VSPs have appropriate measures in place to protect users from illegal content as well as from incitement to hatred and violence.

Ofcom opened a call for evidence to inform its guidance for UK-established VSPs, which closed on 24 September.

Our arguments throughout our response can be summarised as follows:

- Accountability – Governments need to provide more leadership and strategic thinking in tackling terrorist use of the internet and not place the onus on private companies.
- Rule of Law – Counterterrorism and tackling online harms need to be based on the rule of law and pay due regard for human rights, in particular freedom of expression.
- Transparency – We encourage both governments and tech companies to be transparent in their efforts to counter terrorist use of the internet.

Our full response can be found here.

## UNOCT: Implementing the UN Global Counter-Terrorism Strategy: Call for Civil Society Feedback

We additionally submitted responses to the UNOCT's "Implementing the UN Global Counter-Terrorism Strategy: Call for Civil Society Feedback".

# EXTENDING OUR KNOWLEDGE

Over the course of 2020, we have extended our knowledge regionally as well as technically to stay ahead of the evolving threat landscape. In particular, we are extending our research in emerging technologies and online services, such as gaming platforms, end-to-end-encryption, and terrorist operated websites. The aim of this extensive research is to ultimately help the tech industry better understand terrorist use of the internet as well as the broader terrorist and violent extremist threat.
We have also furthered our research into new areas including online regulation. This is exemplified through our Online Regulation Series, which we are continuously expanding upon throughout 2021.

## Online Regulation

Following the Online Regulation Series in 2020, we are continuing our research and analysis of online regulation as well as tracking regulations globally. In 2021, we will continue our research and analysis on the global state of online regulation, both by tracking ongoing regulations as well as through drafting and launching our Online Regulation Series Handbook. In addition, we are expanding our research to cover new countries and regions in the 2021 edition of the Online Regulation Series.

## End-to-end-encryption

Tech Against Terrorism is currently expanding its expertise on the use of end-to-end encryption (E2EE), including how online users and the general public perceive encryption, and the wider "encryption debate". In doing so, we are analysing the threat posed to end-to-end-encrypted services, and exploring strategies which such services can employ to counter terrorist use of their platforms, whilst preserving privacy and security for users.

## Terrorist Operated Websites

Tech Against Terrorism is additionally dedicating research to terrorist operated websites. Terrorist operated websites (TOWs) play an important role in the online terrorist information eco-system and serve to ensure propaganda longevity online. There is currently a lack of a global legal framework and coordination between governments on how to mitigate the threat from TOWs, and there are significant rule of law and freedom of expressions concerns with regards to the potential wholesale removal of websites.

## Gamification

We are currently expanding our knowledge on the topic of gamification, specifically how terrorist and violent extremists exploit gamification and gaming culture for their own ends.

# 2021: Q1 & Q2

Below we outline the recent work and areas of research that Tech Against Terrorism has focused on since the start of 2021. Looking ahead for Q3 and Q4 of 2021, we will continue to work on and expand on all of the above workstreams as well as extending our knowledge.

## Events

Tech Against Terrorism has presented at a number of virtual events and conferences.

Tech Against Terrorism joined the EU Internet Forum Ministerial Meeting held on 25 January. Adam Hadley, our Director, presented on our work supporting smaller tech companies and the Terrorist Content Analytics Platforms, and called for improved government designation of far-right terrorist groups, as well as increased research into terrorist use of decentralised platforms and terrorist operated websites.

Our OSINT Analyst, Arthur Bradley, presented at a workshop organised by the United Nations Office on Drugs and Crime (UNODC) for Jordan on "The Online Terrorist Modus Operandi in the MENA region".

Our Head of Policy & Research, Jacob Berntsson, presented at the International Parliamentary Conference on "Global Challenges and Threats in the Context of the COVID-19 Pandemic: Terrorism and Violent Extremism" during the joint OSCE PA-PAM Working Session on "Assessing the Terrorist Threat and Efforts to Prevent Violent Extremism."

Our director, Adam Hadley, presented at the OSCE wide counter-terrorism conference organised by the Swedish chairpersonship, where he presented on Tech Against Terrorism's work, including the Terrorist Content Analytics Platform (TCAP) and the Knowledge Sharing Platform (KSP).

Tech Against Terrorism's Director, Adam Hadley, and Research Analyst, Anne Craanen, presented on the TCAP for the Digital and Social Media Action Group organised by the Global Coalition Against Daesh.

Our Research Analyst and Policy Lead of the TCAP, Anne Craanen, presented at the Researcher Ethics and Safety panel at GNET's first annual Conference. She spoke about the ethical and security principles that guide the development of the TCAP and the wider work of Tech Against Terrorism.

On 28 June our director Adam Hadley took part in a panel discussion on "Handling Terrorist Content Online: Toward Transparency" as part of the UN's Counter Terrorism Week. He developed on our Mentorship Programme and the key considerations that smaller platforms must have regarding transparency reporting.

Our Director, Adam Hadley, presented at Wales Tech Week in a panel on identifying and removing online terrorist propaganda: challenges and responses. He highlighted Tech Against Terrorism's work in this area, with a focus on the Terrorist Content Analytics Platform.

Our OSINT Analyst, Deeba Shadnia, presented at an event organised by the terrorism prevention branch of the United Nations Office on Drugs and Crime. The event was co-sponsored by the United Kingdom Foreign and Commonwealth Office and was directed toward practitioners in the Kingdom of Morocco. She discussed the role of tech platforms in countering terrorist exploitation of their services, and discussed current trends in terrorist use of the internet identified by our OSINT monitoring.

Our Senior Research Analyst, Maygane Janin, presented at the Terrorism & Social Media Conference 2021, organised by Swansea University, discussing transparency reporting and human rights considerations in platforms' counterterrorism and content moderation approaches. She highlighted how the Tech Against Terrorism's Mentorship and Membership support tech platforms in this regard.

Our Research Analyst, Anne Craanen, presented at a UN Counter Terrorism Week side event on "The opportunities and challenges presented by online and AI tools for the Prevention of Violent Extremism", co-hosted by the European Commission and UNDP. She highlighted the importance of including civil society in counterterrorism efforts, and stressed how we did so in building the Terrorist Content Analytics Platform.

On 7 July our Head of Policy & Research, Jacob Berntsson, presented at the ASEAN Regional Forum Workshop on "Preventing Terrorist Use of the Internet" where he spoke about our work on mentorship and knowledge sharing with smaller platforms.

Our Senior Research Analyst, Anne Craanen, was invited to the Taking Apart Terror podcast, by the Global Coalition to Defeat Daesh, to provide expert insight on the Islamic State's use of the internet and our work to counter it. You can access the recording here.

Anne Craanen participated in the BBC's Tech Tent podcast episode "Intel's Road Ahead", she discussed terrorist use of the internet and our work supporting smaller tech platforms. Listen to the episode here.

Our Director, Adam Hadley, spoke at the GIFCT Global Summit, discussing key trends in terrorist use of the internet, including terrorist operated websites and emerging tech platforms.

## Media

Adam Hadley spoke with Politico about violent far-right extremists' attempts to radicalise and recruit supporters of US President Trump in the wake of the storming of the Capitol. Read the article here.

We wrote an article for Counter Terror Business on terrorist use of the internet, and what we at Tech Against Terrorism are doing tackle the threat. Read it here.

Tech Against Terrorism was quoted in the Observer, analysing the efforts of far-right extremists to radicalise and recruit Trump supporters who have been pushed off Parler after its deplatforming in January 2021.

In an article for Axios, our Director, Adam Hadley, discussed far-right terrorist use of online platforms, and the importance of a holistic response that addresses root causes in addition to online countermeasures.

The United Nations released its 12th report on the threat posed by the Islamic State (IS) to international peace and security. In the report, Tech Against Terrorism's Terrorist Content Analytics Platform (TCAP)'s is highlighted as an effective tool to counter the dissemination of online IS content.

Adam Hadley wrote an op-ed for The Times, in which he argues that the UK's Online Harms framework is unlikely to help counter terrorist use of the internet and risks undermining key democratic principles like the rule of law and freedom of expression.

Our research was cited in a Guardian piece on how the violent far-right attempts to appeal to teenagers by exploiting youth culture. Adam Hadley was quoted in the article stating that "every day we are seeing far-right violent extremist and terrorist groups exploit youth culture, not only to evade content moderation, but also to radicalise young people themselves". Read the full article here.

Tech Against Terrorism's research on far-right videogame recreations of terrorist attacks was mentioned in an article by CityAM.

Our Head of Policy & Research, Jacob Berntsson, discussed the EU regulation on preventing the dissemination of terrorist content online, or TERREG, in a EURACTIV article. In particular, he noted that the "one-hour removal deadline will be nigh on impossible for most small platforms to implement effectively" and stressed the impact that this has on smaller platforms.

Our Senior Research Analyst, Maygane Janin, discussed content moderation, alternatives to content removal, and transparency reporting with Heidi News. She underlined tech sector efforts'at providing more contextual information to transparency reports, whilst emphasising that smaller platforms cannot be held to the same expectations due to a lack of resources. In doing so, she stressed the importance of increased tech sector transparency that accounts for proportionality and for the diversity of moderation policies. (Article in French).

Our Director, Adam Hadley, discussed the UK's Online Safety Bill and reiterating its relative blind-spot for smaller tech platforms on BBC News on the 12 May.

Our Director, Adam Hadley, also wrote an article for Wired providing a threat assessment of terrorist use of smaller platforms and the decentralised web. He also suggested changes in the designation processes for terrorist groups and a need to apply existing laws more effectively to combat online terrorist content.

Our parent organisation, The Online Harms Foundation, was quoted in a recent Times article on the UK's Online Safety Bill and the minimum age requirements enforced upon social media companies.

The TCAP was mentioned in the Digital Lockers Human Rights Report which discusses 'Voluntary Partnership Models' in archiving media evidence of 'Atrocity Crimes'. The report was published by UC Berkeley, you can access it here.

In June, Tech Against Terrorism were quoted in The Observer, The Guardian and Business Insider on our research concerning different aspects of the anti-vax movement and the intricacies with the far-right violent extremism online sphere.

On 30 June, Tech Against Terrorism was mentioned in a UN Interregional Crime and Justice Research Institute paper on "Countering Terrorism Online with Artificial Intelligence: An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia". We were quoted on our call for policymakers to provide clear regulations on what is illegal online content and how tech companies should respond to it.

Adam Hadley was quoted in a Politico article, in which he discussed Covid-19 misinformation, and the need to clearly differentiate between "racist content" and "terrorist content".

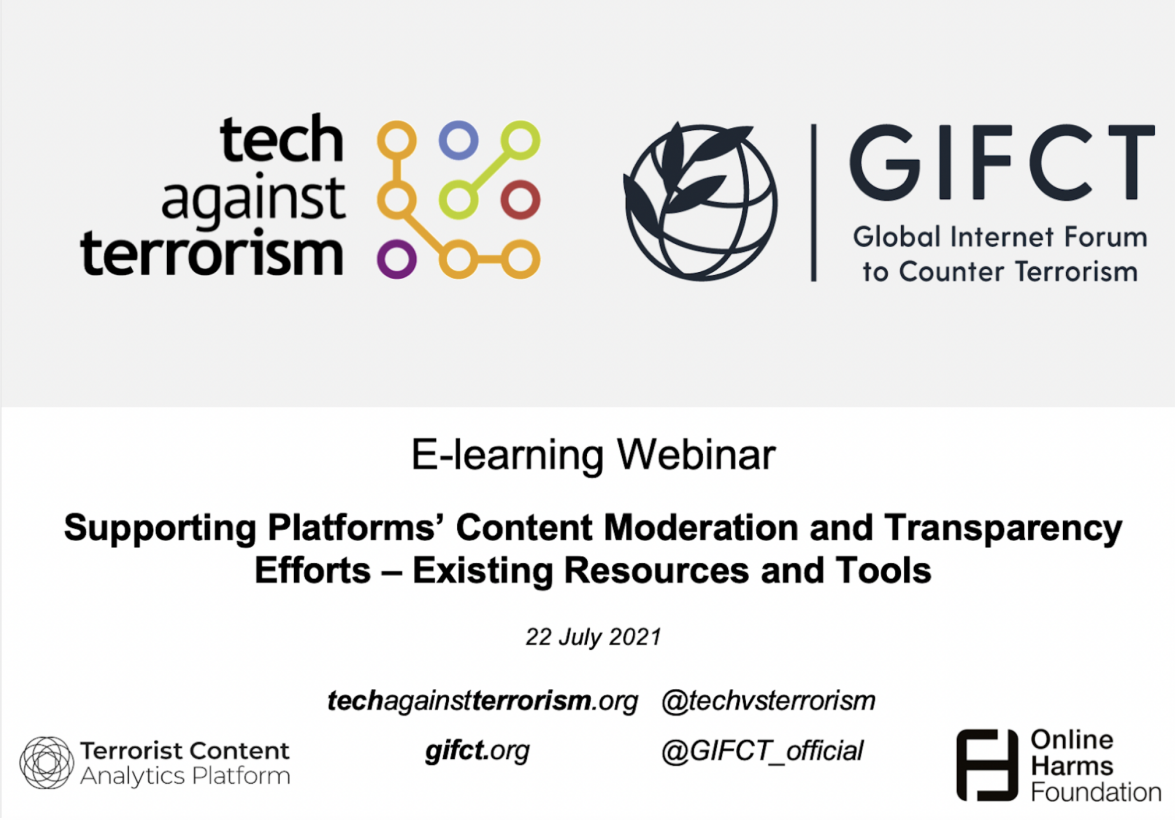
POLITICO Europe published an opinion piece by Adam Hadley, responding to law enforcement calls for backdoors to encrypted communications. He underlined that "A backdoor to encrypted communications would have a negligible effect on deterring terrorist activity", and suggested the forensic use of metadata by law enforcement collect evidence whilst maintaining privacy of communications for users.

## E-learning webinar series

We are continuing to organise webinars as part of our knowledge-sharing efforts. Tech Against Terrorism and the Global Internet Forum to Counter Terrorism's series of e-learning webinars are free webinar sessions particularly suited for tech professionals, content moderators, counterterrorism researchers, and others interested in learning more about terrorist use of the internet and how to counter it.

Since the beginning of 2021, we have organised the following webinars:

- "Countering Terrorist Use of Emerging Technologies: Assessing Risks of Terrorist Use of End-to-End-Encryption and Related Mitigation Strategies"
- "The Nexus Between Violent Extremism and Conspiracy Theory Networks Online"
- "Technical approaches to countering terrorist use of the internet: URL sharing and collaborative tech sector efforts"
- "The Nuts and Bolts of Counter Narratives: What works and why?"
- "APAC in Focus: Regional Responses to Terrorist and Violent Extremist Activity Online"
- "Supporting Platforms' Content Moderation and Transparency Efforts: Existing Resources and Tools"



If you were unable to attend either of the webinars and would like to access a recording, please get in touch with us at contact@techagainstterrorism.org.

## Responses to Regulations and Consultation Processes

- Tech Against Terrorism published a response to the open consultation regarding the Government of Australia's Online Safety Bill. Read our full response here.
- We submitted a response to the United Kingdom's House of Lords Communications and Digital Committee inquiry into Freedom of Expression Online consultation. You can read the response here.
- We submitted a response to the DSA consultation process, a summary of which can be found here. We also published a response to the EU's Digital Services Act. Read our full response here.
- On 2 June we published our submission to the consultation process of Ofcom's Consultation on Guidance for Video Sharing Platforms. Here we voiced our concerns on the rule of law, accountability and the consideration for smaller platforms. To read the full submission please see here.
- On 16 June we published a response paper to the EU's Regulation on Preventing the Dissemination of Terrorist Content Online. We express our concerns with the lack of recognition given to the threat of terrorist exploitation of smaller platforms, and with the little clarity provided on how smaller platforms will be supported in tackling this threat and in complying with the regulation.

## Publications

We published a position paper on content personalisation and terrorist use of the internet, in which we argue that whilst algorithmic recommendation systems warrant scrutiny policy-makers should prioritise other actions – including improving designation and supporting smaller platforms – in order to tackle terrorism online. Read our paper here.

In late July 2021, we released our report on "Gap Analysis on Technical Approaches", in partnership with the GIFCT. Our report outlines several policy and practical recommendations, including the need to formulate a strategy that encourages stakeholders to work towards a common goal and to ensure that technical solutions are considered alongside policy responses. You can access the full report here.

## Terrorist Content Analytics Platform (TCAP)

We have launched the beta version of the TCAP in 2021, and opened registration to the TCAP beta version for tech companies. On the TCAP, companies can view the content that the TCAP alerted to them. In addition, they can view whether this material is still online and filter this content to the date we alerted the material to them, which terrorist group produced the content, and other important criteria.

We are sharing TCAP Statistics on a monthly basis in the TCAP newsletter and on a weekly basis on our Twitter account, @TCAPAlerts. You can sign up to the TCAP newsletter here, and follow us on Twitter account at @TCAPAlerts for more information on the platform, as well as regular statistics on the TCAP alerts.

In 2020, the TCAP group inclusion policy was made public, outlining the inclusion of designated terrorist groups in the TCAP. In 2021, we uploaded our Content Classification and Verification Policy as well as TCAP's Legal review.

We have updated the TCAP FAQs page, in which you can find more information on our content verification policy and TCAP access.

Since 2020, we have held office hours for the TCAP, which we are continuing throughout 2021. These office hours are bimonthly hour-long sessions that provide an update on the development of the platform, as well as answer any questions interested stakeholders might have. This is one of the steps we are taking to ensure that the platform is developed in a transparent manner.

### Impact

Since the launch, the TCAP has identified and verified 11,640 URLs containing terrorist content, sent 6,477 alerts to 58 tech platforms across the globe. Over a 100 tech companies are signed up to the TCAP and ready to receive alerts when terrorist content is identified on their platforms. 96% of alerted content has now been removed, 80% of which in the days following our alert.

We are pleased that the TCAP was praised by Prime Minister of Canada Justin Trudeau at the Christchurch Call to Action 2021.

The TCAP was mentioned in a report by Human Rights Watch, as they state that the considerations taken by Tech Against Terrorism in building the TCAP will be informative for Human Rights Watch' mechanism to archive removed material for evidence of war crimes.

The TCAP's contribution to countering Islamic State's propaganda was highlighted by the United Nations Counter-Terrorism Directorate (UNCTED) in their Twelfth report on the Threat posed by ISIL, Daesh to international peace and security.

The TCAP was mentioned in the Digital Lockers Human Rights Report which discusses 'Voluntary Partnership Models' in archiving media evidence of 'Atrocity Crimes'. The report was published by UC Berkeley, you can access it here.

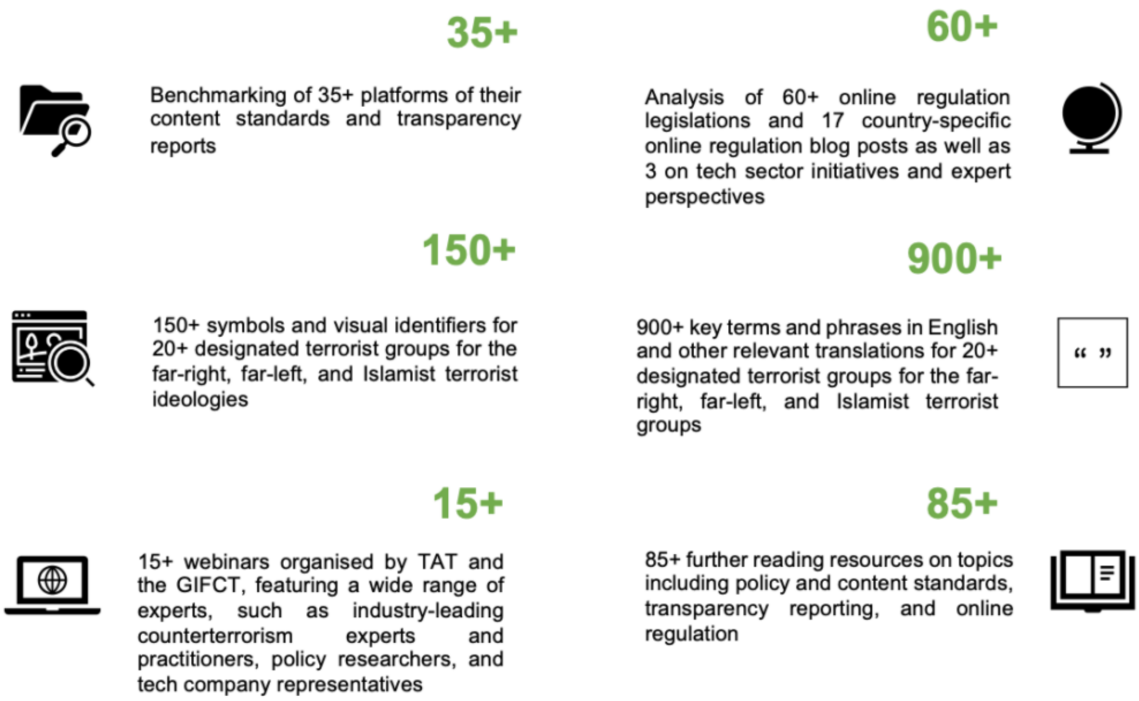
## Knowledge Sharing Platform (KSP)

An updated version of the Knowledge Sharing Platform (KSP) was re-launched to tech platforms in July 2021 in partnership with the UK Home Office. The KSP is a collection of interactive tools and resources designed to support the operational needs of smaller tech platforms. It is a "one stop shop" for companies to access practical resources to support their counterterrorism and transparency efforts.

Our resources include research and analysis on terrorist use of the internet, such as the threat landscape and proscribed organisations, on global online regulation, as well as guidelines and recommendations on content standards and on transparency reporting. All of our key recommendations and policy resources will be accessible via this platform.

The re-launch of the KSP was accompanied by a launch event, which featured opening remarks from Tech Against Terrorism Director Adam Hadley, a keynote speech from Richard Thompson OBE, Head of Online Policy Unit at the UK Home Office, as well as well as a demo of the KSP. If you were unable to attend the launch event and wish to access a recording, please reach out to us at contact@techagainstterrorism.org.

To read more about the Knowledge Sharing Platform, please visit our blog post on it here.



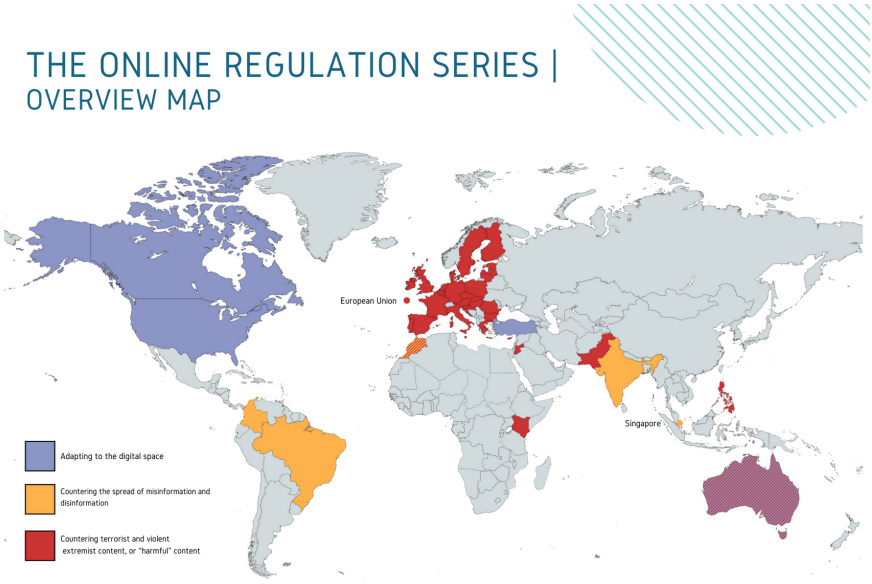

## Open-Source Intelligence (OSINT)

We are scaling up our open-source intelligence work, such as by focusing on bespoke OSINT and intelligence reporting, as well as investigative briefings for new TAT mentees and members. Increasing members and mentees'understanding of far-right violent extremism and the nuance of ideologies and groups involved. Ongoing outreach and communication with platforms around key trends of concern and intelligence sharing. As a part of the updated TAT Membership, in 2021 are continuing our regular bespoke OSINT briefs for members, as well as terrorist use of the internet OSINT briefs.

On 30 July we released our Trends in Terrorist and Violent Extremist Use of the Internet report, covering the key trends observed by our Open Source Intelligence (OSINT) team over the past six months. You can access the full report here.

## Online Regulation

Tech Against Terrorism is pleased to have launched the Online Regulation Series Handbook, providing insight and analysis of over 60 regulations and legislative proposals in 17 countries, including our recommendations for policymakers. You can access the handbook here.


The Handbook is based on analysis published throughout October and November 2020 for the first edition of our Online Regulation Series, and all country analyses have been updated to reflect recent regulatory changes. For each country, we provide a summary of the regulatory framework, key takeaways for tech platforms, and Tech Against Terrorism's commentary.

The Handbook also includes Tech Against Terrorism's key recommendations for governments, and an analysis of International Human Rights Law as a possible framework for content regulation and governance.

With this Handbook we aim to provide a comprehensive and accessible resource for tech platforms to improve their understanding of legislative developments and key trends in online regulation. All resources included in the Handbook can be accessed via our relaunched Knowledge Sharing Platform.

## Designation – Proscribed Organisations

In 2021, we are expanding our knowledge on designation processes. We currently have an ongoing project on the designation processes which we aim to complete this summer.

## Transparency Reporting Guidelines for Governments and Platforms

On 26 July we released the Tech Against Terrorism Guidelines on Transparency Reporting on Online Counterterrorism Efforts, for tech platforms and governments. Our Guidelines seek to encourage improved meaningful transparency and accountability, from both governments and tech companies, around online counterterrorism activities. You can access the guidelines here.

## TAT Mentorship and Membership Programmes

We are currently working on updating and expanding upon our Membership Programme. This will apply to our policy support, OSINT support, as well as furthering direct discussions and communications with our members through a dedicated Slack space, as well as through increased meetings, roundtables, and consultations. To read more about our next steps for the Mentorship and Mentorship Programmes, please see our blog post here.

You can read our 2018 – 2020 Overview of the Mentorship Programme, highlighting the great results of the programme so far here.

In 2021, we will continue to develop and strengthen our policy and practical support to ensure that we provide our members with the adequate support.

Tech Against Terrorism connects industry, government, and civil society to prevent the terrorist use of the internet whilst respecting human rights.

A project supported by UN CTED under mandate of the United Nations Security Council Counter-Terrorism Committee

Find out more at:

techagainstterrorism.org
@techvsterrorism
contact@techagainstterrorism.org

tech against terrorism