REPORT:
Conclusions from the Online Consultation Process for the Terrorist Content Analytics Platform (TCAP) – August 2020

tech
against
terrorism

Supporting the global tech industry in tackling terrorist use of the internet whilst respecting human rights

Table of Contents

A) Executive summary

In 2019, Tech Against Terrorism conducted an online consultation process on the Terrorist Content Analytics Platform (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. This report summarises feedback submitted during the consultation process, and outlines some of the key ideas that we will incorporate in the development of the TCAP. Below we share key insights from the process:

- The TCAP is seen as a useful tool for tech companies and as an important initiative supporting academic research on the terrorist use of the internet

- Researchers and tech companies stressed that the TCAP should be a comprehensive analytical tool, allowing for in-depth analysis of terrorist use of the internet

- Academics and researchers emphasised that the range of content hosted on the TCAP should be as broad as possible, and not limited to Islamist terrorism. Having initially stated that the initial version of the TCAP would only contain official IS and al-Qaeda content – with a view to include other groups after a proof of concept stage – we decided to include designated far-right terrorist organisations as part of the initial remit

- Civil society responses emphasised that the TCAP should be as transparent as possible and highlighted the importance of the platform remaining independent. Respondents also underlined the importance of respecting tech platforms' autonomy with regard to moderation policy and enforcement decisions

- Across all sectors, respondents stressed the importance of safeguarding mental health and welfare of researchers and content moderators

B) Background: Terrorist Content Analytics Platform

In June 2019, Tech Against Terrorism was awarded a grant by Public Safety Canada to develop the TCAP, the world's first free centralised platform of verified terrorist content. The platform will support smaller tech companies in swiftly and accurately identifying terrorist content discovered on their platforms, allowing them to consider this content against their own content standards. The TCAP will also drive improved analysis of terrorist use of the internet. To that end, the TCAP will be accessible for tech companies, academic researchers, and civil society.[1]

[1] For a comprehensive explainer on the TCAP, please see the FAQ section on the TCAP website: https://www.terrorismanalytics.org/faq

In the initial phases, Tech Against Terrorism identified four key concerns to be taken into consideration:

1. Rule of law: our approach should be based on internationally recognised designation lists and normative approaches; in the first phase of development the TCAP will initially focus on IS, al-Qaeda (and affiliated organisations), and designated far-right terrorist organisations[2]

2. Accuracy and transparency: an independent academic advisory board will be recruited to allow for content verification, and we will allow for a civil society oversight of the content included on the platform

3. Privacy and security: users will pledge to not disseminate any content hosted on the TCAP; and personal identifiable information will not be accessible through the platform[3]

4. Tech platform autonomy: alerts will be on an advisory basis only[4] and human verification and moderation will be required

These considerations were presented to participants of the consultation process.

C) Consultation Process

To fully understand these and other potential areas of concern, Tech Against Terrorism commenced a public consultation process in the latter half of 2019. This consultation process is part of our risk mitigation strategy and was conducted publicly to allow for transparency and accountability. The risk mitigation strategy aims to gain relevant insights from the potential users of the TCAP, to ensure that the platform is useful and does not constitute any risk with regards to privacy, security, or contributes to the restriction of human rights and fundamental freedoms, including freedom of speech.

One consultation meeting was co-organised with UN CTED during the UN General Assembly week on 24 September 2019. The meeting was attended by members of civil society, academia, the tech sector, as well as government and intergovernmental organisations. The main recommendations that emerged from this meeting emphasised the importance of:

[2] The decision to include designated far-right terrorist organisations was announced in July 2020. For more information, see here: https://www.techagainstterrorism.org/2020/07/02/update-initial-version-of-the-terrorist-content-analytics-platform-to-include-far-right-terrorist-content/

[3] Tech Against Terrorism will ensure that all information available through the TCAP will be anonymised

[4] The TCAP will include an “alert” function that will inform companies when a piece of terrorist content verified by the TCAP is uploaded on their platform, based on this alert they can decide to remove the content according to their own content removal policy

- Including mental health safeguards
- Building mechanisms to allow users to track their usage patterns
- Hiring a diverse academic advisory board
- Developing mechanisms to ensure that potential biases are not reflected in the database

In addition to this meeting, an online consultation process was launched in October 2019 to solicit feedback from smaller tech companies, academia and expert researchers, and civil society. This process was closed in December 2019.

The online consultation process sought input from three specific groups of stakeholders: tech companies, academic researchers, and civil society groups. These groups were chosen to reflect the core user base of the TCAP and to ensure that the platform is developed in line with Tech Against Terrorism's commitment to tackling terrorist use of the internet whilst respecting human rights and fundamental freedoms. To that end, the consultation was divided into three different surveys, where each sector replied to a different set of specifically adapted questions.

The survey for smaller tech companies aimed at receiving inputs on the requirements that the TCAP would need to meet to support companies in effectively tackling terrorist content and managing takedown requests and removal orders, as well as other features.

For academics and researchers, we asked how the platform could improve their research efforts, in particular regarding quantitative analysis and the innovative use of data science. Researchers were also asked to provide advice on issues relating to research ethics and mental health safeguarding.

At Tech Against Terrorism, protecting human rights and fundamental freedoms, including freedom of speech when tackling terrorist use of the internet is our key aim. Input from civil society was thus meant to ensure that concerns regarding online freedom of expression, privacy and other relevant human rights issues are taken into consideration when developing the TCAP.

A full list of all questions asked in the survey is available in Annex section of this report.

This report provides an overview of the main contributions by the respondents to the TCAP online consultation process.[5] Replies notably underline the potential challenges that the TCAP might meet (e.g. issues of privacy and security, potential biases), and potential areas of further development for the platform (e.g. ideologies other than Islamist terrorism).

[5] Legal concerns raised by the responses to the online consultation process, and during the wider risk mitigation strategy, will be addressed in a separate Legal Review document

D) Acting on key concerns and suggestions

Results from the online consultation process allowed us to identify the main concerns raised by tech companies, academia and researchers, and civil society. Whilst we were aware of a majority of these concerns and had considered them in our initial planning phase, we will pay significant attention to the following when developing the platform:

- Developing the TCAP within an explicit human rights framework
- Expanding the initial scope of terrorist content on the TCAP beyond IS and al-Qaeda (and affiliates) to designated far-right terrorist groups
- Ensuring the security and privacy of the platform, including in preventing the misuse of material
- Safeguarding the mental health and welfare of those accessing the platform
- Ensuring that researchers accessing the platform are vetted correctly and have access to adequate institutional support
- Ensuring a diverse academic board, notably through diverse regional and linguistic representation
- The range of content hosted on the platform and feedback on Tech Against Terrorism's decision to initially focus on internationally designated groups
- Ensuring that tech platform autonomy is respected

Several comments were made by respondents regarding the importance of considering human rights when developing the TCAP. Protecting human rights and fundamental freedoms, including freedom of speech, when tackling terrorist use of the internet is a key aim for Tech Against Terrorism, and it will be reflected in the development of the TCAP. The platform will be developed within an explicit human rights framework, taking into consideration international human right law considerations.[6] We will ensure and test all features introduced against a human rights framework to assess risks.

Respondents also raised the issue of content documenting human rights abuses and content used for journalistic purposes, raising concerns around such content being taken down by

[6] The human rights framework of the TCAP will be guided by the Tech Against Terrorism Pledge, a set of six guiding principles that provides simple and accessible guidelines to help smaller tech platforms tackling terrorist exploitation of the internet in a manner that respect human rights and freedom of speech. The Pledge itself is based on internationally recognised norms that provides crucial normative precepts for tech companies to tackle exploitation of their services whilst promoting and protecting human rights as articulated in: the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on Economic Social and Cultural Rights, the UN Guiding principles on Business and Human Rights, and UN Security Council resolutions and documents S/RES/1624 (2005), S/RES/2129 (2013), S/RES/2322 (2016), S/RES/2354 (2017) and S/2017/375.

tech platforms due to lack of contextual understanding and/or under algorithmic moderation procedures. To address this concern, Tech Against Terrorism will share resources on content moderation guidance with tech companies, providing them with guidelines and best practice to ensure that content moderation does not have a negative impact on material shared for the above purposes. We also believe that the TCAP could support the archiving of content that may be removed due to violation of company policies but could prove crucial in terms of documenting human rights abuses, war crimes, or for other journalistic or research purposes.

Concerns over the possible misuse of material were also been raised by respondents. Security and privacy are key priorities for Tech Against Terrorism in developing the TCAP, and we will ensure that the TCAP meets the necessary security requirements considering the sensitive nature of the content on the platform. To this end, we will work with data security and privacy experts to ensure that content is stored in accordance with data regulations and in respect of fundamental privacy concerns. Vetting for the TCAP will be informed by best practices learned by Tech Against Terrorism in our work with the academic blog Jihadology.net.[7] Furthermore, content uploaded on the TCAP will bear a watermark to deter against potential misuse.

Mental health and welfare have been a primary concern in the development of the TCAP. To this end, we will incorporate tech features to attempt to safeguard the mental health of those accessing the platform and limit potential negative impact of graphic and/or disturbing content. We will also aim to introduce surveys to be sent to users on a regular basis to draw attention to and assess potential negative mental health impact. In addition, Tech Against Terrorism will share resources and best practices on safeguarding mental health via the platform. The issue of mental health will be further discussed in the following phase of the consultation process.

Suggestions were also made with regard to who will be able to access the platform. With regards to researcher access, one respondent suggested limiting access to researchers with adequate institutional support.

Respondents further stressed the importance of ensuring the diversity of the academic advisory board. Tech Against Terrorism will engage with, and further develop, its network of academia and research experts to ensure that geographic and linguistic diversity is well represented on the board. Tech Against Terrorism will also work in collaboration with the Canadian Network for Research on Terrorism, Security and Society (TSAS) in this endeavour.

The results of the online consultation process show a strong interest for the TCAP to be a portal for knowledge sharing, where tech companies can find best practices and policy guidelines. It should be noted that Tech Against Terrorism's Knowledge Sharing Platform (KSP) could already fulfil this need, as it allows registered tech companies to access a variety of tools and resources to protect themselves from terrorist use. The KSP contains a variety of educational materials and tools, such as compendiums of characteristic elements of terrorist

[7] https://www.techagainstterrorism.org/2019/04/10/press-release-10th-april-2019-launching-an-updated-version-of-jihadology-to-limit-terrorist-exploitation-of-the-site/

groups (including logos and terminology), as well as practical advice around Terms of Service and transparency reporting, to improve companies' understanding of the threat landscape and inform their efforts in identifying and tackling terrorist exploitation of their platforms.

Respondents from academia and civil society expressed concerns over Tech Against Terrorism's decision to initially only include IS and al-Qaeda content. Whilst we had taken such concerns into consideration, our decision to focus on IS and al-Qaeda was taken to a) delimit the scope for our proof of concept b) to avoid adding content produced by groups around which there is no clear definitional consensus. We did not see it as our role to, by extension, designate groups or actors as terrorists that have not yet been designated as such by the international community, with the risk of including lawful content on the platform.[8] However, we have listened to concerns raised by participants in this consultation process. Furthermore, fortunately there is a growing (albeit limited) trend of increasingly designating far-right terrorist groups. As a result, we will include designated far-right terrorist entities in the initial scope of the TCAP.[9]

In relation to the broader discussion on moderation of online terrorist content, suggestions were made for transparency reports on the use of the TCAP to be compulsory for tech platforms using the TCAP. Whilst we encourage this drive for tech sector transparency, on the basis of our commitment to tech companies, they will not be required to publish reports on their use of the platform in order to access the TCAP. However, Tech Against Terrorism does encourage tech companies to produce transparency reports on their use of the TCAP and will continue to work to develop tools to assist smaller companies in improving their transparency reporting efforts generally.[10] We will also introduce regular transparency reports detailing content hosted on the TCAP.

[8] Such considerations will continue to be important in our development of the TCAP. Specifically, we are aware of the risks of the TCAP contributing to so called "content cartel creep" (see more here: https://knightcolumbia.org/content/the-rise-of-content-cartels)

[9] At the time of writing, this includes groups designated by the United Kingdom, Canada, and the United States. We encourage more states to accurately and responsibly designate far-right terrorist groups.

[10] Commitment to "improve transparency reporting" is notably included in the requirements for the Tech Against Terrorism Membership. Whilst we encourage all companies to make efforts to meet the Tech Against Terrorism membership criteria, we do not (at the time of writing) envisage membership of Tech Against Terrorism as a requirement for accessing the TCAP. However, and following our commitment to transparency reporting practices, we will offer guidance on the matter for tech companies willing to produce a transparency report on their use of the TCAP, or to include it within their broader transparency reports.

E) Summary of Responses

For a comprehensive understanding of the feedback received during the online consultation process, below we summarise the main points made in response to each survey. For a full list of questions asked to tech companies, see Annex 1.

1) Tech platforms

Summary of key points made by tech sector respondents:

> **TP1.** The TCAP should be an all-encompassing tool, assisting tech platforms in identifying covert signs of association with terrorist and violent extremist groups[11] (e.g. cryptolect and/or images whose meaning is only or predominantly understood by in-groups)
>
> **TP2.** Responses show that mental health of content moderators is a primary concern for tech platforms
>
> **TP3.** Tech respondents were interested in how the platform would work with existing technologies for content takedown and workflow management
>
> **TP4.** When asked about transparency reporting and the possibility of creating an aggregated global transparency report, respondents showed interest but underlined that it would be dependent on the resources needed. Respondents also stressed that not all transparency reports can include similar metrics due to differences in technology and platform policies

Most companies taking part in the survey were small tech platforms with less than 250 employees, based in Europe and North America. In terms of user base, a majority of the respondents had a relatively small base of less than 100,000 users, but a significant proportion had a base of over 1,000,000 users. Overall, respondents to the survey cover a wide range of the tech ecosystem, and include companies across social media, audio-sharing, fintech, as well as messaging and pasting sites.[12]

[11] Whilst the TCAP will, in the first instance, be limited to certain terrorist groups, the mention of violent extremist groups in this report reflects respondents' interest in the TCAP expanding its scope to such groups. Moreover, Tech Against Terrorism continues investigating violent extremism more broadly, as the TCAP could potentially cater to those groups going forward.

[12] More detailed information on the profile of companies who responded to the survey can be found at the end of the report, alongside a more complete overview of the answers given by respondents to the tech company survey

Figure 1: "Where is your company based?"

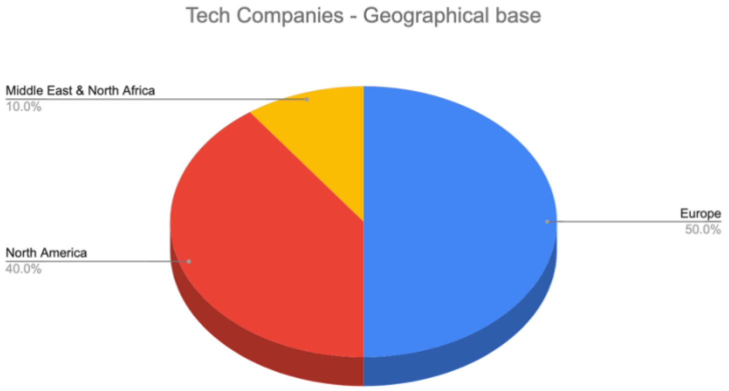


Figure 2: "How many employees does your company have?"

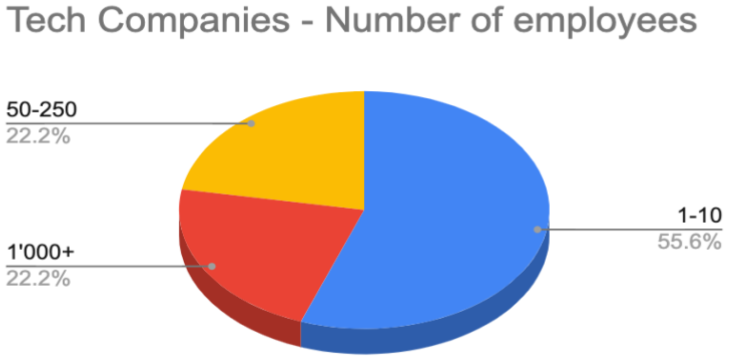


Figure 3: "How many users does your company have?"

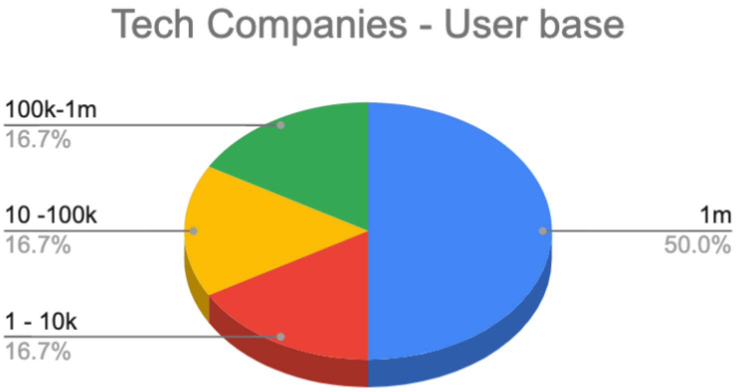
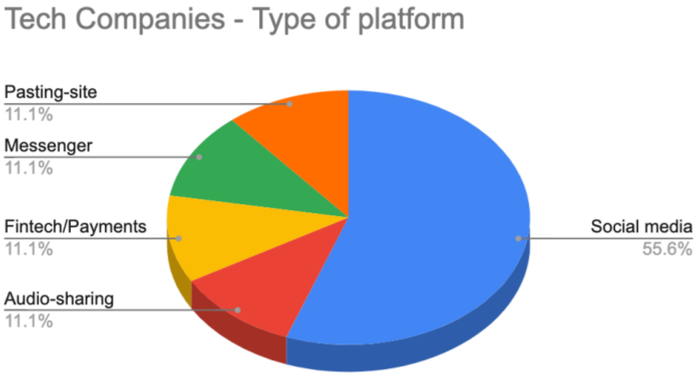


Figure 4: "Which of the following categories best describe your company / the company you work for?"



For tech companies, the most common suggestion is for the TCAP to be an all-encompassing tool, not only supporting them in flagging individual pieces of content but also providing them with links to related content on their platforms, as well as on other platforms.[13] Assistance in identifying covert symbols of association with terrorist groups was also mentioned. Further, suggestions were made for the TCAP to be a platform where companies can share best practices and have access to policy guidelines.

The need to safeguard the mental health and welfare of employees dealing with terrorist content on a daily basis also came up as an important issue for tech companies. In addition to sharing best practices and policy guidelines, respondents suggested that advice on mental health should be shared on the TCAP for it to be a comprehensive tool for tech companies.

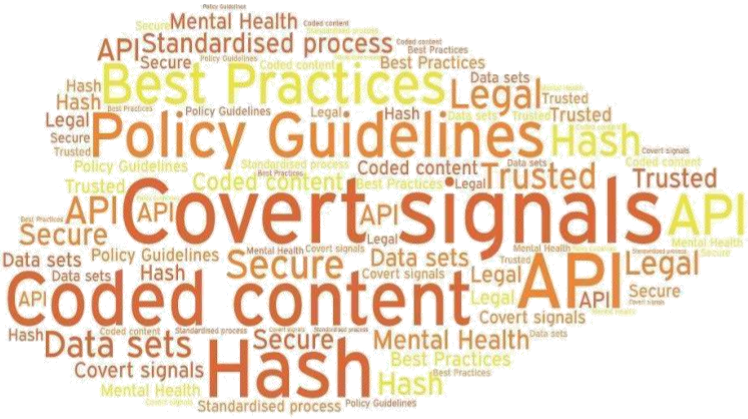
Tech platforms expressed interest in the more practical functions of the TCAP. In particular, they were interested in how the TCAP would work with their existing tools for content takedown and workflow management, as well as in further integration with their APIs.

Furthermore, tech companies said that transparency reporting is arduous, but expressed interest in receiving support to produce transparency reports. Responses also underline a desire to avoid the standardisation of transparency report formats across all platforms. As an initiative, Tech Against Terrorism encourages tech platforms to introduce transparency reporting in a way that is proportionate and provides users with clarity with regards to the platform's content moderation enforcement and government requests made to the platform.[14]

[13] The TCAP will predominantly look to collect content from 'beacon' platforms. We are in the process of carrying out a full legal review of our content collection practices.

[14] See more here: https://www.techagainstterrorism.org/2020/03/02/transparency-reporting-for-smaller-platforms/

Figure 5: Word cloud of responses to the tech platforms survey



2) <u>Academia and expert researchers</u>

Below is a summary of key points made by academia and expert researchers. For a full list of questions asked to academics and expert researchers, see Annex 3.

A1. The TCAP was commended as a good resource to research content in a secure and ethical manner

A2. Respondents said that the TCAP should aim to be a comprehensive and user-friendly analytical platform, supporting researchers in their analysis of terrorist use of the internet

A3. When asked about the type of material that the TCAP should host, respondents emphasised the difficulty in delimiting a scope for the TCAP. Respondents also argued for non-Islamist terrorist groups and self-radicalised individuals to be included, based on our initial announcement that only IS and al-Qaeda would be included in the first version of the platform

A4. Learning from other databases of terrorist content, respondents stressed the challenges of verifying content authenticity, suggesting that any decision to include content made by the TCAP should be reversible if required

A5. Respondents underlined the importance of considering mental health and incorporating features supporting researcher welfare

A6. Respondents also stressed that strong institutional support should be required in order to gain access to the TCAP, especially in the case of students[15]

[15] Access to the TCAP for university students will be conditional to a professor/university's approval and should be strictly supervised by said professor/university to ensure students' mental health and prevent misuse of material.

Whilst most of the respondents to the academia and researchers survey were from academic institutions, private sector research and think tanks were also well represented. The majority of the institutions who responded were based in Europe and North America. There was also some representation from Oceania and Asia.

Figure 6: "Where is your organisation based?"

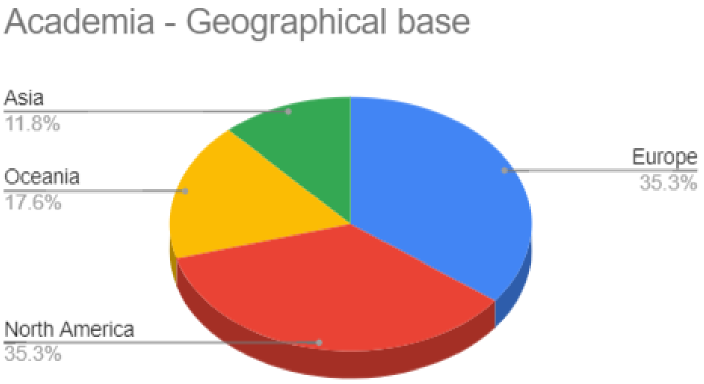
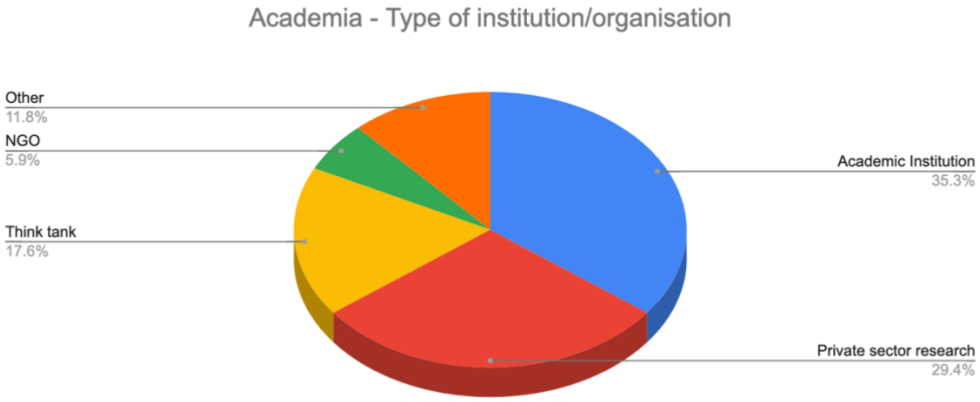


Figure 7: "What type of institutions do you represent?"



One key insight is that the TCAP should not limit itself to a repository of terrorist content. Respondents suggested that tools allowing for analysis of evolving trends within terrorist use of the internet and features to support research methodologies, including visualisation tools, compatibility with corpus linguistics, and coding software should be included. This would allow researchers to analyse emerging groups and trends in terrorist use of the internet and situate the content within its broader context (e.g. type of extremism, geography and language).

Furthermore, respondents underlined the difficulty of deciding on the kinds of terrorist and violent extremist ideologies that should be covered by the TCAP. One of the most prevalent comments was thus regarding the TCAP's initial focus on Islamist terrorist groups (IS, and al-Qaeda), and several respondents recommended including groups from other ideological strands as well. As previously mentioned, this has now been updated to include designated far-right groups. In addition, respondents said that the TCAP should also cover content from non-affiliated groups and self-radicalised individuals. Researchers also expressed an interest in accessing meta-data, the location of the original upload, how many files contained the same content, English translation, and mapping of reaction to the content, amongst others. Interest was also expressed for a compendium of images, including symbols and logos of terrorist groups but also social media profiles and memes (particularly used by right-wing terrorists).[16]

Respondents said that the TCAP interface should be as user-friendly as possible, with indexes, visualisation tools, and the possibility for researchers to use the TCAP in combination with other tools (e.g. linguistics and coding software). Some respondents also expressed an interest in the possibility to interact and communicate with other researchers within the platform, for example via an in-platform feature. Respondents also suggested hiring dedicated support staff.

Lessons learned from existing databases indicate that some of the main challenges for the TCAP will probably be linked to the large volume of data and to the authenticity of the content. The question of who is to adjudicate on content authenticity was particularly recurrent amongst the answers given, alongside recommendations to include the possibility to contest specific decisions.

The issue of ensuring researchers' mental health and welfare also drew some interesting suggestions – from integrated tools to mental health webinars – reaffirming that Tech Against Terrorism's commitment to developing the TCAP with mental health safeguards in mind was well-received. Alongside integrated tools to warn of violent and graphic content and to mitigate the effects of reality (e.g. reduced resolution, black and white option, smaller screens), respondents also underlined that an introduction to mental health safeguarding (either in-person or online) would be useful.[17] The organisation of regular meetings and workshops was also strongly advised to check on researchers' mental health and provide additional advice. Further, some respondents to the survey recommended that only researchers with adequate institutional support should be allowed access to the platform.

Whilst access to the TCAP for students overall was seen as a good opportunity for student research on verified primary source material, concerns about welfare were raised. It was strongly recommended for students to only be able to access the platform in a controlled environment and with strong support from their institutions. Student welfare and mental health was already amongst Tech Against Terrorism's initial concerns in developing the TCAP. Therefore, student access to the TCAP will be conditional to a professor's or university's

[16] Such compendiums of key terrorism identifiers are already available to registered tech platforms through the Knowledge Sharing Platform.

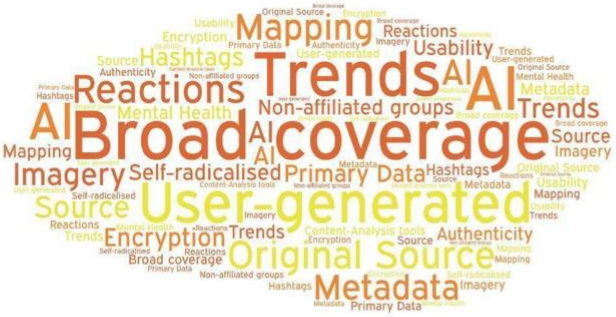
[17] Additionally, such mental health induction prior to accessing the TCAP could also link users with mental health organisations that could offer them support if needed.

approval, and should be strictly supervised by said professor or university to ensure students' mental health and prevent misuse of material. In this regard, respondents also mentioned the possibility for leading universities in the field to develop specific supervising programs to ensure proper ethical access and protect the mental health and welfare of students.

The TCAP was commended by researchers as a good tool for viewing, researching, and storing content in a secure and ethical manner. Concerns regarding the privacy and security of the TCAP were raised by the respondents, however, notably with regard to the potential misuse of material, and the balance between the privacy of individuals (especially children) depicted in the content with the traceability of the data.

Overall, researchers saw the development of the TCAP as an important initiative that would greatly benefit research and methodology on terrorist content analysis, but also provide insightful historical snapshots of the evolution of the terrorist use of the internet. Responses to the academia survey also emphasised that it is essential for the TCAP to remain a free and transparent platform.

Figure 8: Word cloud of responses to the academia survey



3) Civil society

Below is a summary of key points made by civil society. For a full list of questions asked to civil society stakeholders, see Annex 4.

CS1. Respondents expressed concerns regarding the use of internationally recognised designation lists as a baseline for selection of content included on the TCAP due to the limitations of such lists

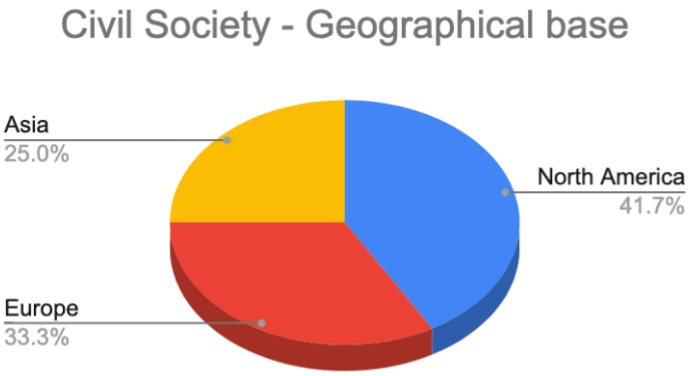
CS2. Results stressed the importance of a diverse and impartial oversight body to ensure that such a body reflects the diversity of expertise and of communities affected, as well as to prevent potential biases

CS3. Respondents emphasised the importance of the TCAP being developed in a transparent and autonomous manner to ensure integrity and accountability

CS4. Respondents raised concerns regarding the security of the platform and the sufficiency of a pledge to prevent dissemination of content

Most of the civil society respondents were based in North America and in Europe.

Figure 9: "Where is your organisation based?"



Responses to the civil society consultation survey emphasised concerns regarding the decision to, in the first instance, only include internationally designated groups like IS and al-Qaeda. Respondents underlined the shortcomings of this approach, especially concerning the non-inclusion of certain terrorist and violent extremist organisations (especially far-right groups) and lone actors. As has been mentioned, we have now changed our policy to include designated far-right terrorist groups. As some of their academia counterparts, many civil society respondents advocated for content to be identified by the "value of its message" rather than by its source.

Respondents stressed that the TCAP should be explicit in its recognition of human rights and human rights mechanisms, whilst also taking into account regulation mechanisms in place in the private sector and the potential impacts the TCAP could have on them. Despite Tech Against Terrorism's explicit commitment to, and existing work under, an internationally recognised human rights framework, respondents were particularly cautious about the human rights challenges that may occur. This includes concerns around criteria for inclusion being fully in line with freedom of expression and ensuring that content can still be used for journalistic and human rights purposes. Overall, they called for the recognition of human rights standards and the importance of inscribing the TCAP within an international human rights law framework to be more explicit.

Transparency was also strongly emphasised in the responses. Specifically, respondents encouraged regular publication of TCAP transparency reports, with information detailing how content included on the platform was discovered and which institutions have access. It was also suggested that companies should publish transparency reports on their use of the platform, in addition to their existing transparency reporting.

Respondents commended the fact that a civil society oversight board will be created, and emphasised the necessity for such a mechanism to be impartial and diverse, both with regard to the experts' backgrounds and areas of expertise, and to the representation of different regions, cultures, and communities. Suggestions made by civil society regarding the composition of the board were broad and could provide indication as to who the board should include in order to ensure diversity and expertise. For instance, it was suggested that experts with more practical knowledge should be part of the oversight board (e.g. field experts, journalists), as well as experts on content moderation and on the related human rights challenges. One respondent suggested that de-radicalised individuals should be part of the oversight board.

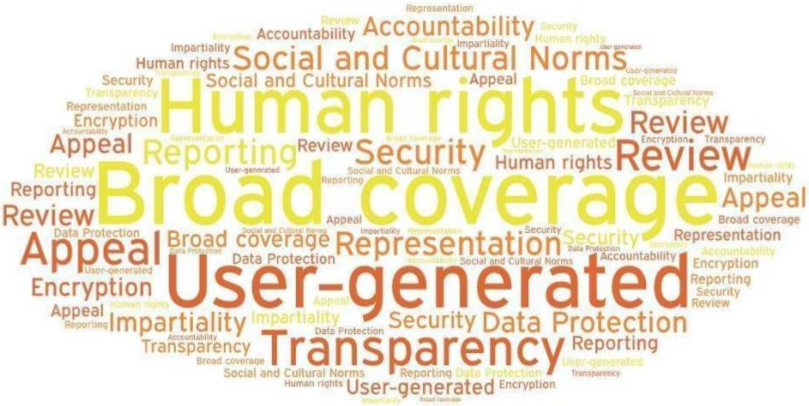
Respondents also stated that the oversight board should also be fully involved in the TCAP's internal functioning, with a say in the content inclusion mechanism and the possibility to review and challenge the inclusion of content. This might also imply that the different decisions made by the TCAP should be reversible if content is found to have been included incorrectly. Some criticism was voiced regarding the academic focus of the advisory board, pointing to the risks of missing insightful expertise and perspectives from civil society and field experts.

Concerns were also expressed regarding the sufficiency of a pledge to avoid the dissemination of content stored on the platform. Instead, respondents recommended restricting downloads and screenshots, in addition to introducing minimum security requirements. For example, Tech Against Terrorism could introduce the capacity to trace back content if disseminated by users, by making users consent to such measures in the user agreement. Some respondents also suggested the establishment of independent privacy and security audits.

The autonomy of tech platforms' internal moderation policies was seen as essential for most of the civil society respondents and should in no case be compromised by the TCAP.

Therefore, the advisory nature of the platform should always be stressed, especially to avoid the risk of governments attempting to influence and pressure tech companies' content moderation policies, for instance by forcing them to remove content flagged by the TCAP regardless of the platform's content standards. To preserve this independence, the need to ensure the representation of the tech industry in the oversight board was also stressed, notably to guarantee that companies can have a say in how data is shared.

Figure 10: Word cloud of responses to the civil society survey



E) Annex 1: Tech companies: responses to the survey

Figure 11: "Has your company had to remove terrorist and/or violent extremist content from your platform, or deal with terrorist use of your services?"

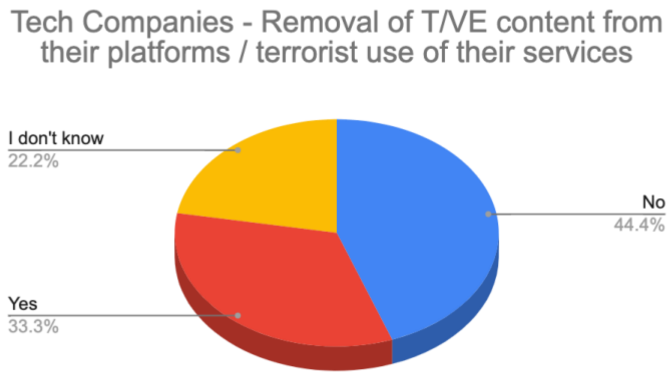


Figure 12: "If yes, how many times would you estimate that your platform has removed terrorist content in the past year?"

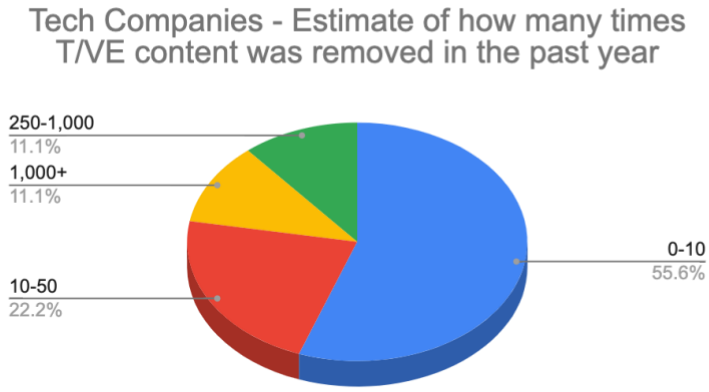


Figure 13: "How would you rate your platform's current response to terrorist and violent extremist content discovered on your platform?"

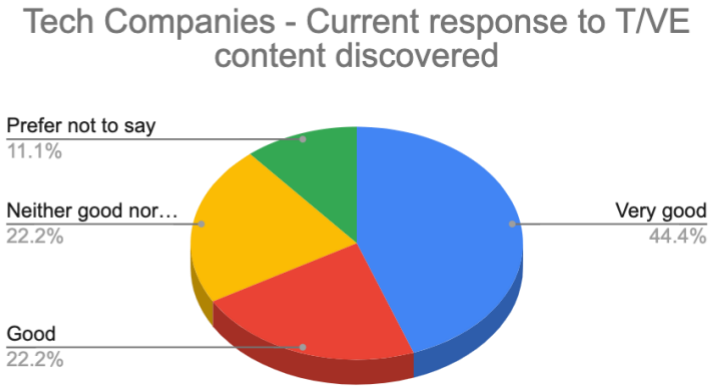


Figure 14: "How would you rate your platform's current financial resources available for tackling terrorist exploitation?"

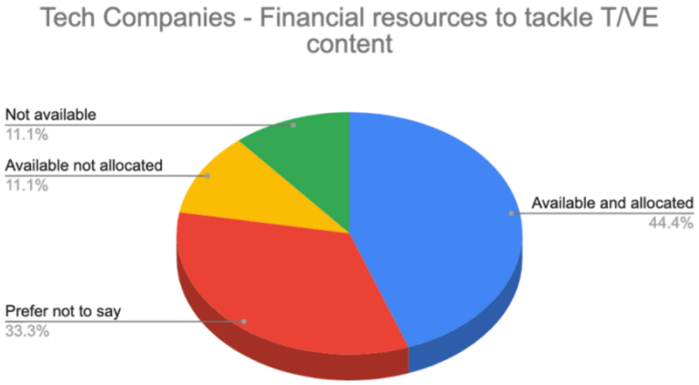


Figure 15: "How would you rate your platform's current technical resources available for tackling terrorist exploitation?"

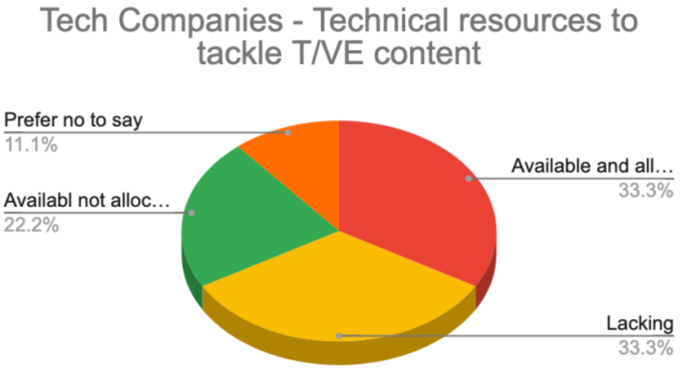


Figure 16: "How would you describe your interest in learning more about transparency reporting?"

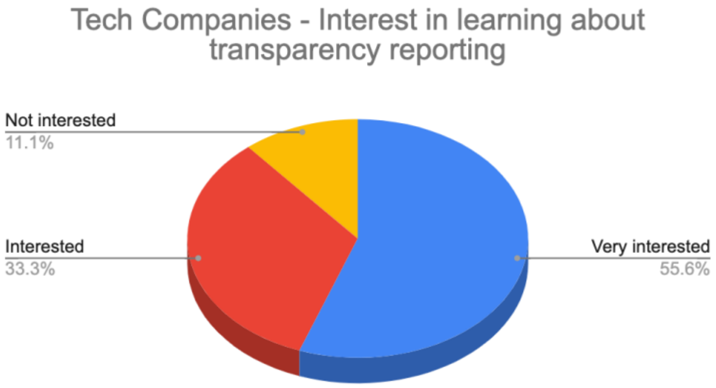


Figure 17: "As a tech company representative, what argument FOR your platform producing transparency reports do you see?"

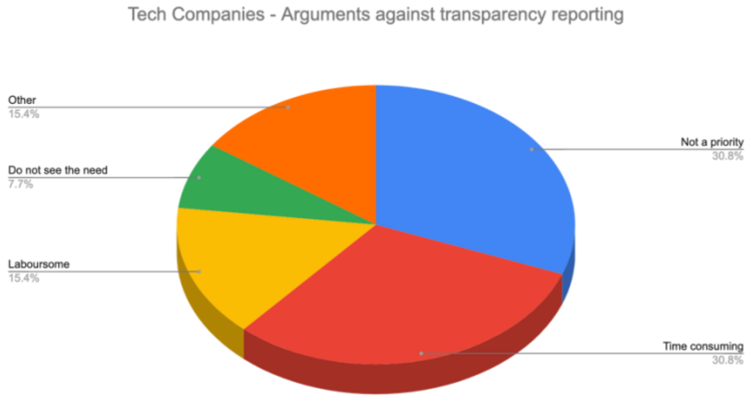


Figure 18: "What arguments AGAINST your company producing transparency reports do you see?"

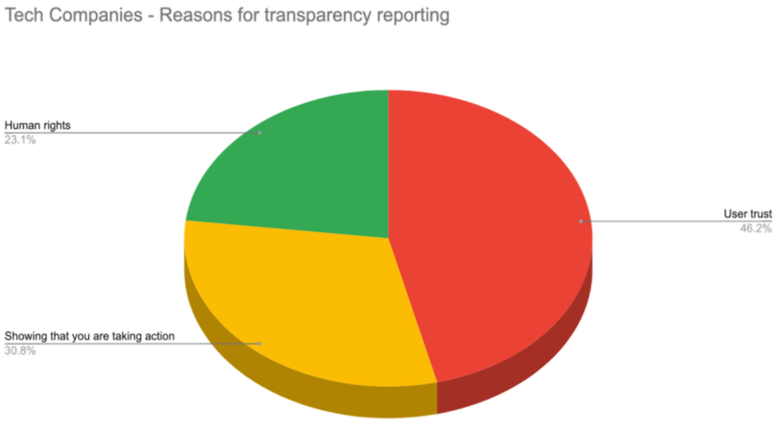


Figure 19: "Would you be interested in support from TaT in generating transparency reports and potentially aggregating these on an online platform hosted by TaT?"

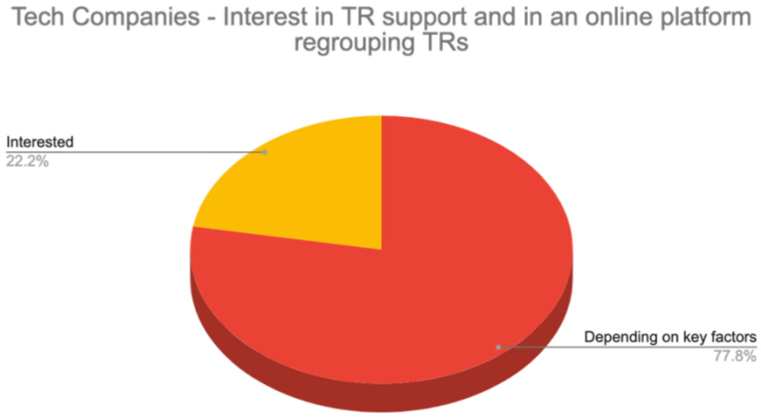


Figure 20: "Would you be interested in having your transparency report be part of a global aggregated report?"

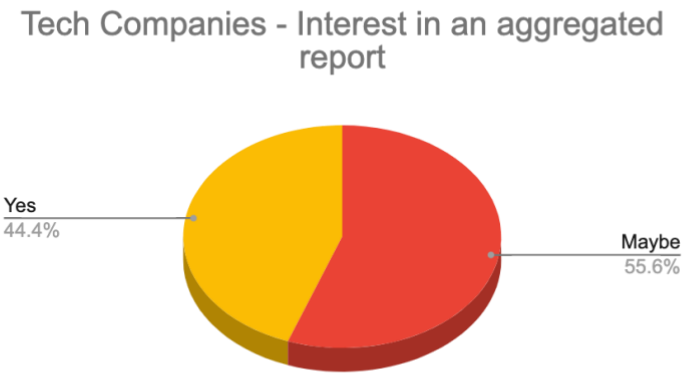
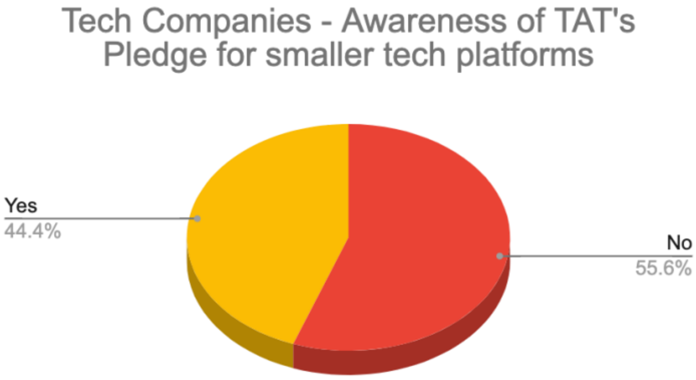


Figure 21: "Are you aware that Tech Against Terrorism has designed a Pledge for smaller tech platforms that is built on internationally recognised principles on freedom of expression and responsible business practices?"



F) Annex 2: Tech platforms survey: questions

Question 1: How many employees does your company have? Multiple choice, one choice

- 1-10
- 10-50
- 50-250
- 250-1,000
- 1,000+

Question 2: How many users does your company have?

- 0-1,000
- 1000-10,000
- 10,000-100,000
- 100,000-1,000,000
- 1,000,000+

Question 3: Which of the following categories best describe your company / the company you work for?

- File-sharing
- Social media
- Pasting site
- Web hosting / infrastructure
- Fintech / payments
- Video-sharing
- Audio-sharing
- Messaging
- Other, please specify

Question 4: Has your company had to remove terrorist and/or violent extremist content from your platform, or deal with terrorist use of your services? Multiple choice, one choice only

- Yes
- No
- I don’t know

Question 5: If yes, how many times would you appreciate that your platform has removed terrorist content in the past year?

- 0-10
- 10-50
- 50-250
- 250-1,000
- 1,000+

Question 6: How would you rate your platform's current response to terrorist and violent extremist content discovered on your platform? Multiple choice, one choice only

- Very good
- Good
- Neither good nor bad
- Not good
- Prefer not to say

Question 7: How would you rate your platform's current financial resources available for tackling terrorist exploitation? Multiple choice, one choice only

- Financial resources are available and we CAN afford to allocate them to tackle terrorist exploitation
- Financial resources are available but we CANNOT afford to allocate them to tackle terrorist exploitation
- There are no financial resources available
- Prefer not to say

Question 8: How would you rate your platform's current technical resources available for tackling terrorist exploitation? Multiple choice, one choice only

- Technical resources and know-how are available and CAN be allocated to tackle terrorist exploitation
- Technical resources and know-how are available but CANNOT be allocated
- We lack technical resources and relevant know-how to tackle terrorist exploitation

Question 9: Are you aware that Tech Against Terrorism has developed a self-assessment form for tech companies to allow platforms to assess their capacity to tackle terrorist use of their services?

- Yes
- No

Question 9: Content identification and moderation via the TCAP

In addition to facilitating tech company examination of content and alerting tech companies to when terrorist content is discovered on their platforms, which specific content moderation features and tools and/or considerations should the TCAP include to support tech companies in identifying and tackling terrorist content on their platforms? What challenges do you encounter?

Question 10: Law enforcement engagement

In our experience working with the tech sector, many smaller tech companies are overwhelmed by the amount and manner in which they receive takedown requests from governments and law enforcement agencies. Which specific tools would be beneficial for smaller platforms in managing such requests? Which specific considerations would we need to make? Please answer as specifically as possible.

Question 11: Content management and takedown workflow

Managing large amounts of content, including terrorist content, discovered on a platform in a structured manner can be difficult for a smaller tech company with limited resources. Would a content management system and a workflow supporting reporting on takedowns be useful for your platform? Which specific features should such a system contain? Which considerations would it need to make? Please answer as specifically and detailed as possible.

Question 12: Transparency (small tech companies only)

As a tech company representative, how would you describe your interest in learning more about transparency reporting? Multiple choice, one choice only

- Very interested
- interested
- not interested

Question 13: Transparency (small tech companies only)

As a tech company representative, what argument FOR your platform producing transparency reports do you see? Multiple choice, several choices allowed

- User trust
- Beneficial for human rights & freedom of expression
- Showing governments that you are taking action
- Other, please specify

Question 14: Transparency (small tech companies only)

As a tech company, what arguments AGAINST your company producing transparency reports do you see? Multiple choice, several choices allowed

- Time consuming, please specify how long you appreciate this takes you
- Laboursome
- Not a priority
- Do not see the need
- Other, please specify

Question 15: Transparency (small tech companies only)

Would you be interested in support from Tech Against Terrorism in generating transparency reports and potentially aggregating these on an online platform hosted by Tech Against Terrorism? Multiple choice, several choices allowed

- Definitely interested
- Interested, depending on a few key factors, please specify which
- Not interested, but could be convinced, please explain what would make you change your mind

Question 16: Transparency (small tech companies only)

Would you be interested in having your transparency report be part of a global aggregated report? Multiple choice, one choice only

- Yes / No
- Maybe, please explain on what this is contingent

Question 17: Transparency (small tech companies only)
Are you aware that Tech Against Terrorism has designed a Pledge for smaller tech platforms that is built on internationally recognised principles on freedom of expression and responsible business practices?

- Yes
- No

G) Annex 3: Academia and research survey questions

Question 22: Content and materials useful for research part 1

In order to make the TCAP as useful for researchers as possible, we invite you to share your thoughts on what type of material the platform should host. As a researcher, what content and materials do you think would help you improve your quantitative research on terrorist use of the internet? Please provide detailed answers.

Question 23: Content and materials useful for research part 2

It is envisaged that the TCAP will initially provide access to a repository of official media output from the two main Sunni jihadist terrorist groups - Islamic State/Daesh and al-Qaeda. What other groups would you expect/like to be covered in the longer term? What other forms of content (e.g. unofficial media output, memes, open discussions among support networks) would you expect/like to be covered? Do you have a corpus of material that you would like to offer for inclusion in the TCAP?

Question 24: Tools and features useful for research

In order to make the TCAP as useful for researchers as possible, we invite you to share your thoughts on what specific platforms features we should consider implementing. As a researchers, what tools and features do you think would help improve your quantitative research on terrorist use of the internet improve your user experience?

Question 25: Taxonomy

To make the platform user friendly for researchers, we will implement a taxonomy of content across the platform. This taxonomy will cover things such as group, sub-group, date of publication, name of publication, and type of content (PDF, audio, video etc). As a researcher, what other categories should this taxonomy include? What specific considerations do we need to make? Please provide detailed answers.

Question 26: Lessons learned from existing databases

It is recognised that many researchers will have built up their own databases of open source content over the years. If this applies to you, what issues or problems have you encountered that we might learn from? Even if it doesn't apply to you, what other issues, not already mentioned, could you anticipate that we might encounter?

Question 27: Researcher welfare and mental health

Safeguarding the mental health and well-being of those using the TCAP for research purposes is one of our key concerns. As a researcher, what specific measures do you think we should take to achieve this? Please provide detailed answers.

Question 28: Ethics

In terms of establishing the TCAP as a research platform, what ethical considerations besides mental health and researcher welfare do we need to make? Please provide detailed answers.

Question 29: Teaching and student research on primary source material

In what way do you see the TCAP being able to support university student research on primary source terrorist material? What considerations do we need to make?

H) Annex 4: Civil society survey questions

Question 17: Rule of Law

The TCAP will be based on internationally recognised designation lists and normative approaches. With respect to ensuring the rule of law, what other considerations should we make in developing the TCAP?

Question 18: Transparency

We aim to provide civil society oversight of the TCAP. What do you think this oversight function should look like? What consideration do we need to make when designing this function?

Question 19: Accuracy

We will recruit an academic advisory board who will be tasked with verifying content to ensure that content collated on the TCAP is accurately identified as terrorist content and does not lead to undue takedown of legal content. In the first instance, we will look to only host branded ISIS and al-Qaeda (and affiliates) content and will therefore seek to recruit a board whose expertise reflects that target area. What considerations do we need to make in designing the composition of our advisory board? What are the potential pitfalls that we should be aware of?

Question 20: Privacy and Security

Before giving access to users, we will verify all users who will pledge to not disseminate any content located on the TCAP. Only tech companies, researchers, and civil society will be allowed access to the platform. We will also ensure that personal identifiable information (PII) of users is not traceable on the platform. What other considerations do we need to make?

Question 21: Tech platform autonomy

Tech Against Terrorism wants to safeguard tech platform autonomy and does in no way seek to force platforms to make certain moderation decisions. To that end, any alerts to platforms triggered by the TCAP are on an entirely advisory basis. What other considerations do we need to make to ensure that tech platform autonomy is not compromised?