tech against terrorism

Supporting the tech industry in tackling the use of internet technologies for terrorist purposes whilst respecting human rights

2017 Annual Report

An initiative launched and supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED) pursuant to United Nations Security Council Resolutions S/RES/2129 (2013), S/RES/2354 (2017), S/RES/2395 (2017) and S/RES/2396 (2017)

QuantSpark Foundation

tech against terrorism

CTED Counter-Terrorism Committee Executive Directorate

1. Executive Summary

Tech Against Terrorism was launched by the United Nations Counter-Terrorism Executive Directorate (UN CTED) in April 2017 at AccessNow's RightsCon[1], following the 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'.

Tech Against Terrorism is a public-private partnership whose mission is to support the tech industry in developing more effective and responsible approaches to tackling the use of the internet for terrorist purposes whilst respecting human rights. It does this through a programme of practical engagement with internet platforms such as social media, pasting, file-storage, messaging, and fintech, helping them to identify and mitigate risk, sharing knowledge of best practice, developing resources to assist platforms, and building a network to facilitate and sustain these activities.

In 2017 the initiative was launched by UN CTED pursuant to four UN Security Council Resolutions[2,3,4,5] as well as the Comprehensive International Framework to Counter Terrorist Narratives[6] that calls for improved public-private co-operation regarding tackling the use of the internet for terrorist purposes whilst respecting human rights. Building on the original scoping exercise in 2016, Tech Against Terrorism focused its first year's work in 2017 on outreach and knowledge-sharing with three objectives:

1. Provide practical resources and insight for smaller tech platforms for example to help them improve Terms of Service while reinforcing the importance of upholding human rights and freedom of expression
2. Foster an encouraging environment for peer learning and support between the larger and smaller companies
3. Develop sustainable links between small and large platforms, government civil society, and academia, through the public-private partnership model

Tech Against Terrorism considers all significant "use-cases" of internet technologies for terrorist purposes. This includes strategic applications such as the hosting and dissemination of propaganda content designed to influence general populations and to radicalise and recruit vulnerable individuals. Terrorists and violent extremists also use internet technologies for operational purposes such as gathering intelligence, "off-ramping" vulnerable individuals onto to encrypted messaging platforms, carrying out command and control communications, and distributing bomb-making manuals. Specific internet technologies commonly used for terrorist purposes include large-scale social media, file-sharing, link-shortening, content storage, video-sharing, content-sharing/pasting, archiving, and blogging platforms. Terrorists also exploit internet infrastructure services (domain registration, web hosting, DDOS-protection) as well as fintech, e-commerce, encrypted messaging,

[1] "Launch of 'Tech Against Terrorism' – a partnership between technology companies, governments, and UN CTED" retrieved from https://www.un.org/sc/ctc/news/2017/03/31/launch-tech-terrorism-partnership-technology-companies-governments-un-cted
DISCLAIMER: This report does not necessarily reflect the views of the United Nations and Counter-Terrorism Executive Directorate
[2] Resolution 2129 (2013) notes the evolving nexus between terrorism and the internet, and directs UN CTED to help address this
[3] Resolution 2354 (2017) mandates UN CTED to recommend ways for Member States regarding counter terrorist narratives
[4] Resolution 2395 (2017) recognises the development of Tech Against Terrorism and its efforts to foster collaboration between the tech industry, academia, and governments to disrupt terrorists' ability to use technology for terrorist purposes
[5] Resolution 2396 (2017) recognises the development of Tech Against Terrorism and its efforts to foster collaboration between industry, academia, and governments to disrupt terrorists' ability to use technology for terrorist purposes
[6] S/2017/375 Security Council proposal for a comprehensive international framework to counter terrorist narratives with focus on public-private partnership - describing the Tech Against Terrorism initiative as good practice

VPNs, gaming, and anonymous email services. Ongoing research as part of Tech Against Terrorism seeks to identify and quantify these emerging threats to support ongoing outreach efforts.

The guiding principle of Tech Against Terrorism's work is that smaller platforms represent the most important - and often overlooked - strategic threat with regards to the use of the internet for terrorist purposes. The displacement of terrorists from larger platforms means that terrorists often use smaller platforms with impunity, as smaller platforms often cannot tackle exploitation of their platforms on their own.[7] Taking advantage of the decentralised nature of the internet, many terrorist and violent extremist groups now rely on a growing number of smaller platforms to disseminate their propaganda as larger tech companies mitigate much of the threat on their own systems.

Currently the largest threat regarding the use of the internet for terrorist purposes concerns the dissemination of violent extremist content. However, it should not be assumed that the international community itself agrees on the definition and designation of such content. At the same time, there are already robust international frameworks in place regulating the right to freedom of expression and privacy. One of the major objectives of the Tech Against Terrorism initiative is to encourage public and private sector actors to uphold international law and human rights while looking for solutions in addressing counter-terrorism and violent extremist activities online. In all engagements with tech companies, Tech Against Terrorism reinforces and promotes international norms regarding the right to freedom of expression[8] and privacy[9]. To this end, tech companies must agree to the Tech Against Terrorism Pledge as a requirement of Membership.[10]

During 2017, Tech Against Terrorism worked closely with larger tech companies such as Facebook, Google, Microsoft, and Twitter and in August 2017 supported their launch of the Global Internet Forum to Counter Terrorism (GIFCT).[11,12] In five months and across nine cities, Tech Against Terrorism, in partnership with the GIFCT, organised nine high-level workshops to bring together representatives from academia, civil society, government, and more than 65 platforms of all sizes. 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.

Tech Against Terrorism received support from a range of states and companies during 2017 and extends its thanks to the Governments of Switzerland, the Republic of Korea, and Spain, as well as Telefonica, Facebook, Microsoft, and Google for their support.

In summary, during 2017 Tech Against Terrorism:

- Organised nine workshops and engaged with more than 65 at-risk platforms
- Launched the Knowledge Sharing Platform (KSP) to host guidance for smaller platforms

[7] See our 2016 report "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust" retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf
[8] The Universal Declaration of Human Rights: Article 19
[9] The Universal Declaration of Human Rights: Article 12
[10] More details of the Tech Against Terrorism Pledge please refer to: https://www.techagainstterrorism.org/membership/pledge
[11] Global Internet Forum to Counter Terrorism to Hold First Meeting in San Francisco, Facebook, 13 July 2017 retrieved from https://newsroom.fb.com/news/2017/07/global-internet-forum-to-counter-terrorism-to-hold-first-meeting-in-san-francisco
[12] "Update on the Global Internet Forum to Counter Terrorism", Global Internet Forum to Counter Terrorism, 4 Dec 2017 retrieved from Facebook, YouTube, Microsoft, and Twitter: https://blog.twitter.com/official/en_us/topics/events/2017/GIFCTupdate.html, https://newsroom.fb.com/news/2017/12/update-on-the-global-internet-forum-to-counter-terrorism

- Developed an online risk assessment tool to help platforms identify areas to improve
- Supported the GIFCT in establishing an industry-led forum to tackle terrorist exploitation
- Engaged with stakeholders across civil society, academia, and government (parliamentarians, prosecutors, law enforcement) through participating in meetings organised by UN CTED, OSCE, the EU, and the US government

2. Detailed activities carried out in 2017

In 2016 Tech Against Terrorism carried out a scoping exercise by holding workshops with companies, civil society, academia, and governments in Silicon Valley, Zurich, and Kuala Lumpur. That research led to the establishment of the Tech Against Terrorism initiative in April 2017 and informed its initial priorities in engaging with the tech sector.

During 2017 the initiative focused on outreach and knowledge-sharing with the technologies that were assessed in 2016 to be (i) most at risk of terrorist exploitation: social media, communications, content storage, and fintech, and (ii) most in need of advice and support: smaller internet platforms.

Outreach and knowledge-sharing was largely carried out through one-on-one meetings, calls, small roundtables, and workshops – often in collaboration with the Global Internet Forum to Counter Terrorism (GIFCT) – with smaller tech platforms, larger tech companies, and critical stakeholders from civil society, academia, and government, in order to:

a) gain an understanding of the needs of tech platforms
b) learn about innovative private sector responses
c) share the Three Pillars of emerging best practice within the industry[13]
d) build trust and confidence to facilitate knowledge-sharing and collaboration on best practice
e) launch the Knowledge-sharing Platform (KSP) to support companies

2.1 Tech Against Terrorism workshops

Between August and December, Tech Against Terrorism, in partnership with the GIFCT, organised nine high-level workshops to bring together all stakeholders, including more than 65 platforms of all sizes in nine cities. The first workshop was in San Francisco, with subsequent workshops in London, Dublin, Paris, Beirut, Jakarta, New York, Washington, culminating with the final workshop of 2017 in Brussels on the margins of December's EU Internet Forum Ministerial meeting.

These workshops achieved three objectives:

1. Provide platforms with a deeper understanding of the threat of terrorist exploitation
2. Share knowledge about emerging responses and elicit feedback to improve our advice
3. Encourage and facilitate a network of cross-industry knowledge-sharing and self-regulation

Most of the full-day workshops were in two parts; the mornings convened counter-terrorism academics, civil society, prosecutors, government representatives, and members of the GIFCT to

[13] 1) Terms of Service / Community Guidelines; 2) Content Moderation; 3) Transparency and Redress

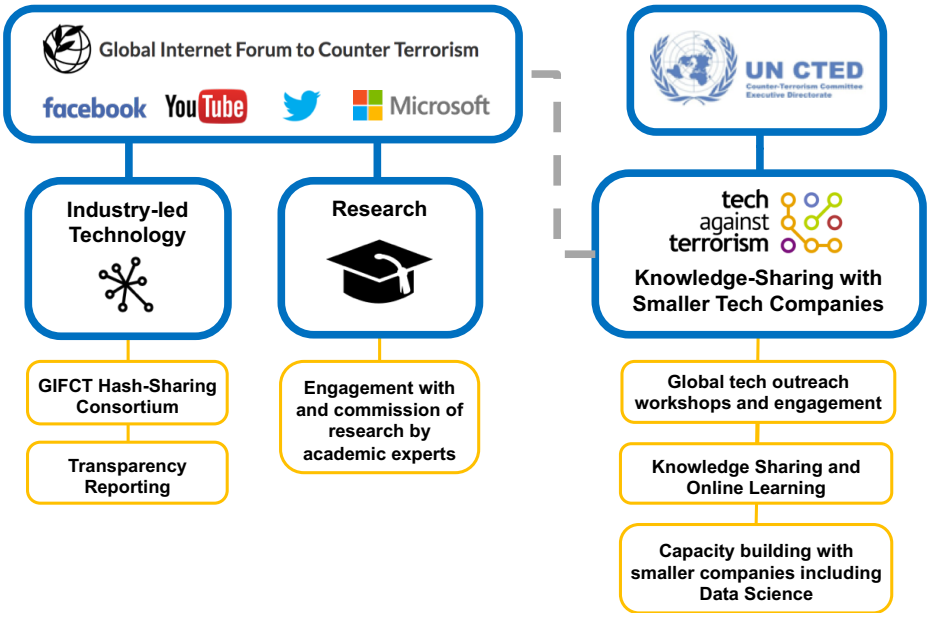
present analysis and share experiences. The closed afternoon sessions involved only platforms and companies to focus on the three pillars of Terms of Service, Moderation, and Transparency Reporting. The closed sessions encouraged more open conversation and highlighted the commitment of Tech Against Terrorism and the GIFCT to focus on assisting smaller tech platforms. Feedback from the closed sessions has been instrumental in shaping the direction of the initiative and the content hosted on the KSP.

2.2 The Knowledge Sharing Platform (ksp.techagainstterrorism.org)

Based on the needs identified in 2016, Tech Against Terrorism developed a Knowledge Sharing Platform (KSP) which was subsequently launched as a Proof of Concept product at a special meeting at UN headquarters in November 2017. The KSP is designed to be is a "one stop shop" for platforms to access resources to support the operational needs of smaller platforms. It hosts a collection of interactive tools and resources such as a database of terrorist groups and individuals listed on the UN sanctions list, recommendations for model Terms of Service, Transparency Reporting, standardised reporting formats, and other practical resources. Members of Tech Against Terrorism have access to the KSP once they complete the Tech Against Terrorism risk assessment, a tool to assist in identifying risk areas of platforms where improvements are recommended.

2.3 Collaboration with the tech industry and the Global Internet Forum to Counter Terrorism (GIFCT)

Following the success of Tech Against Terrorism's engagement with tech companies in 2016, the initiative was invited by Microsoft, Twitter, Google and Facebook to support the establishment of the Global Internet Forum to Counter Terrorism (GIFCT). Tech Against Terrorism now facilitates knowledge-sharing with smaller tech platforms in partnership with the GIFCT. Tech Against Terrorism convened the inaugural meeting of the GIFCT in San Francisco in August 2017, hosting the heads of United States' Department for Homeland Security and the United Kingdom's Home Office in addition to executives from the GIFCT.



3. Findings and Recommendations

Below provides a summary of the main findings and recommendations from the engagement with companies, academia, civil society and government stakeholders in 2017. These recommendations build upon the 2016 report entitled "Private Sector Engagement in Responding to the Use of the Internet and ICT For Terrorist Purposes: Strengthening Dialogue, Building Trust."[14]

3.1. Recommendations for policymakers

1. Encourage industry-led self-regulation driven by consensus and transparency
2. Strengthen international norms for defining terrorist exploitation for example through the UN Sanctions process and consider the importance of the rule of law and respect for human rights when drafting counter-terrorism policies
3. Establish a multilateral mechanism to coordinate government engagement with the tech sector
4. Improve transparency regarding requests to have content taken down based on violations of Terms of Service and other requests for content removal
5. Increase investment in open-source intelligence and data science regarding use of the internet for terrorist purposes
6. Work with the private sector to share government expertise on the nature of the terrorist threat
7. Recognise that terrorist exploitation of the internet occurs on technologies of all forms

3.2. Recommendations for the tech industry

1. Focus on the three pillars of emerging best practice: 1) Improving Terms of Service / Community Guidelines, 2) Developing proportionate operational responses to terrorist exploitation whilst respecting human rights, 3) Improving transparency reporting and redress
2. Advocate for an industry-led approach for self-regulation based on communicating what constructive efforts have already been made by the tech sector to tackle terrorist exploitation
3. Develop a more systematic approach to sharing emerging best practice, threat intelligence, and innovative approaches to detect and mitigate terrorist exploitation
4. Consider membership of Tech Against Terrorism by agreeing with the Pledge[15] and using the risk assessment tool to evaluate the risk of terrorist exploitation

[14] The Phase 1 report from 2016 entitled "Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes Strengthening Dialogue and Building Trust" can be downloaded here: https://www.un.org/sc/ctc/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf
[15] For more details see here: https://www.techagainstterrorism.org/membership/pledge/

4. Membership of Tech Against Terrorism

Tech Against Terrorism has created a Membership programme in order to support industry-led self-regulation and help recognise companies that are pro-actively considering measures to tackle terrorist exploitation.

4.1 Membership requirements

1. Develop Terms of Service / Community Guidelines that repudiate terrorist exploitation
2. Confirm ability to receive and action requests for content moderation
3. Commit to deploying new tech solutions including machine learning and co-locating counter-narrative materials on
4. Publish regular Transparency Reports
5. Agree to the Tech Against Terrorism Pledge
6. Complete the online Assessment Tools with a minimum threshold score

4.2 The Pledge

Tech Against Terrorism has developed six guiding principles (the Tech Against Terrorism Pledge) which underpin our framework for engaging with the very smallest technology companies.[16] These principles reinforce the importance we place on addressing challenging content in the context of commitment to upholding human rights. The Pledge complements the Global Network Initiative (GNI) [17] Principles as it is specifically designed for smaller tech platforms.

The Tech Against Terrorism Pledge provides simple and accessible guidelines to help the very smallest platforms understand the importance of tackling terrorist exploitation in a manner that respects human rights and freedom of expression. With our Pledge, we seek to ensure that small companies – who often do not have enough resources to familiarise themselves with the many legal regimes and social contexts which may apply to their services – can help sustain a free internet. The Pledge is a foundation upon which we encourage companies to build their own appropriate policies. Company commitments to the Pledge should be understood as aspirations to be achieved as quickly and thoroughly as possible, consistent with available resources and scale.

Our pledge is based on the GNI Principles and internationally recognised norms as articulated in the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR"), the International Covenant on Economic, Social and Cultural Rights ("ICESCR"), 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, and the UN Guiding Principles on Business and Human Rights ("UN Guiding Principles"). These constitute crucial normative

[16] The Tech Against Terrorism initiative's pledge for smaller tech companies can be accessed via https://www.techagainstterrorism.org/membership/pledge/
[17] https://globalnetworkinitiative.org/gni-principles and Global Network Initiative (GNI): Extremist Content and the ICT Sector: https://globalnetworkinitiative.org/wp-content/uploads/2016/12/Extremist-Content-and-ICT-Sector.pdf

precepts to help technology companies tackle exploitation of their services in a manner that promotes and protects human rights.[18]

1) Freedom of Expression

"We respect the right to freedom of expression that should be enjoyed by our users and will take actions consistent with applicable law to protect it from unlawful or unnecessary restrictions."

> Article 19 of the ICCPR provides that "*1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.*"

2) Non-Discrimination and Diversity

"We respect the right of our users to express diverse views and opinions, and commit to educating users regarding what content and expression is not permitted on our platforms through clear terms of service and their transparent and consistent application."

> Article 24 of the ICCPR states that *"All persons are equal before the law and are entitled without any discrimination to the equal protection of the law."* Article 15 of the ICESCR recognises the rights of everyone to take part in cultural life.

3) Privacy

"We respect the privacy of all our users and will take actions consistent with applicable law to protect it from arbitrary or unlawful interference."

> UNDHR Article 12 and ICCPR Article 17 states *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

4) Transparency and Accountability

"We appreciate the need to account for what content we deem impermissible on our platforms, how we address government requests related to content on our platforms, and how we make determinations about content. To this end, we value and strive for transparency regarding those policies and practices, especially with regard to how they may impact the above-mentioned human rights-principles."

---

18 As such these principles do not purport to represent a complete catalogue of all responsible business conduct-related principles that companies should consider. Neither does their articulation or explanation here constitute legal advice. For a more complete framework of responsibilities, companies are advised to read and carefully consider the full text of the UN Guiding Principles and their accompanying commentary.

Guiding Principle 21 articulates an expectation that companies will account for how they address human rights and the commentary further explains that this "*requires that business enterprises have in place policies and processes through which they can both know and show that they respect human rights in practice. Showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors.*"

5) Remedy

"While we strive to apply content policies fairly and consistently, we recognise that resource limitations, cultural contexts, and other factors may result in decisions that unintentionally cause negative impacts. To address this eventuality, we commit to devising appropriate mechanisms to allow individuals impacted by our policies and practices to bring information to our attention."

Guiding Principle 20 states: *"To make it possible for grievances to be addressed early and remediated directly, business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted."*

6) Collaboration

"We commit to work with partner organisations and enterprises to collaboratively develop strategies to keep our platforms and products safe from abuse by terrorist organisations and their supporters, and to promote tolerance, coexistence and diversity."

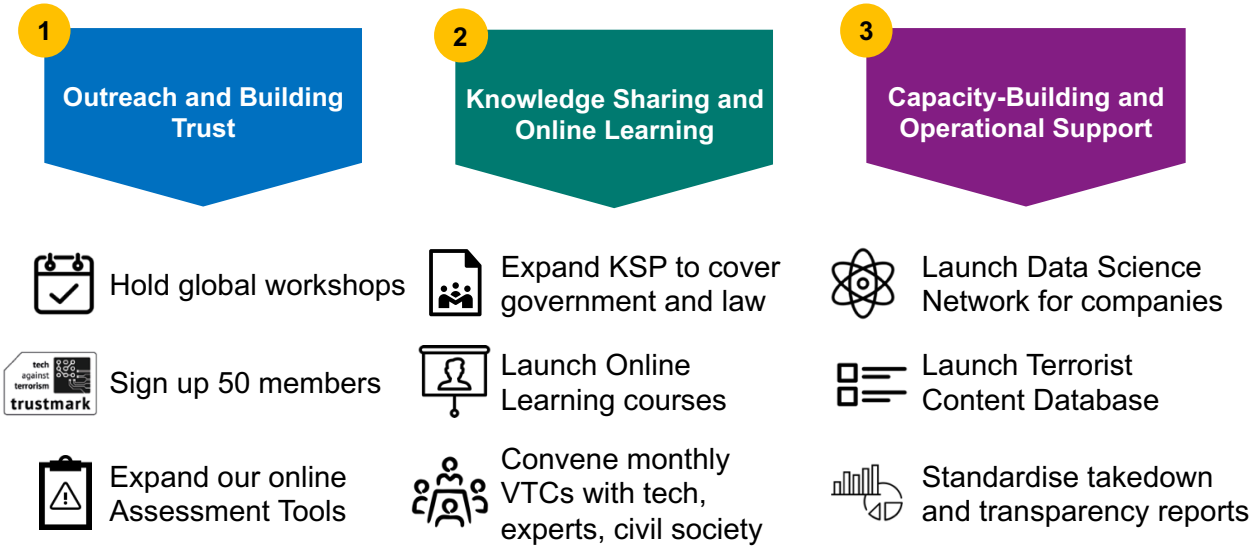
Article 19 of the ICCPR states that the exercise of freedom of expression carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order of public health or morals.

S/RES/1624 (2005) calls upon States to prohibit by law incitement to commit a terrorist act and S/RES/2354 (2017) condemns "*in the strongest terms the incitement of terrorist acts" and repudiates "attempts at the justification or glorification of terrorist acts that may incite further terrorist acts."*

S/RES/2354 (2017) further stresses the importance of the role of the business community *"in efforts to enhance dialogue and broaden understanding, and in promoting tolerance and coexistence, and in fostering an environment which is not conducive to incitement of terrorism, as well as in countering terrorist narratives."* It urges further development of initiatives to strengthen public-private partnerships in this area, and notes the benefits of engagement with a wide range of actors, including youth, families, women, community leaders, and other concerned groups of civil society.

5. Proposed Next Steps for 2018-2019

Over 2018-2019 Tech Against Terrorism intends to sustain and deepen our outreach and knowledge-sharing efforts with the global tech industry. As well as continuing in-person training and workshops with platforms, we will expand the scale of knowledge-sharing efforts through the innovative use of online learning tools and video conferencing. We will also explore ways to practically support platforms through the sharing of improved threat intelligence and data to support their efforts to tackle use of their platforms for terrorist purposes. If you have any suggestions of further work that you believe will be impactful, please do let us know by emailing contact@techagainstterrorism.org. We propose the following workstreams for 2018-2019:



5.1 Measurement and Evaluation

We will record metrics such as the number of companies engaged with (in person, through workshops), the number of companies that update their Terms of Service, complete our Assessment Tools, and become Members of Tech Against Terrorism.

6. The implementation team in 2017

Tech Against Terrorism (London): Adam Hadley (Director), Jacob Berntsson (Research Analyst), Leah Selig Chauhan (Research Analyst), Alexander Harris (Research Analyst), Claudia Wagner (Research Analyst), QuantSpark (KSP development)

United Nations Counter-Terrorism Executive Director (UN CTED): David Scharia (Director, Chief of Branch), Marc Porret (ICT Coordinator), Han Soal Park (Associate Legal Officer)

ICT4Peace Foundation: Daniel Stauffacher

Contact details: Email: contact@techagainstterrorism.org | Twitter: @techagainstterrorism.org

Appendix 1: Events in 2017

	Date	Description	Location	Format	Participation
Feb	22nd – 23rd	Expert Symposium: Countering Extremism Online	Bishkek, Kyrgyzstan	Roundtable	Presented
March	14th	Women, Technology & Partnerships - countering terrorist use of the Internet with SecDev Foundation	Ottawa, Canada	Conference	Co-organised
	29th	Phase 2 Launch at RightsCon	Brussels, Belgium	Session	Organised
April	24-26th	Eleventh International Forum "Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security" (IIS-2017)	Garmisch-Partenkirchen, Germany	Conference	Presented
May	22nd	Comparative approaches to understanding violent and non-violent extremism (Vox Pol)	London, UK	Workshop	Presented
	23rd – 24th	Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism (OSCE)	Vienna, Austria	Conference	Presented
	29th – 30th	1st Asia Dialogue on Information and Communication Technology (ICT) and Counter Terrorism	Republic of Korea	Conference	Presented
	31st May	Jeju Peace Conference	Republic of Korea	Conference	Presented
June	27th – 28th	2017 Terrorism and Social Media Conference	Swansea, UK	Conference	Presented
	27th	EU Internet Forum meeting for Senior Officials	Brussels, Belgium	Closed conference	Presented
	29th	"Harmful Speech Online: At the Intersection of Algorithms and Human Behavior" with Berkman Klein Center, Harvard Law School and the Institute of Strategic Dialogue (ISD)	Harvard Law School, Boston, USA	Conference	Presented
July	12th	London Launch of Tech Against Terrorism at Chatham House	London, UK	Initiative Launch	Organised
Aug	1st	**San Francisco Launch of Tech Against Terrorism**	**SwissNex, San Francisco, USA**	**Initiative Launch and GIFCT Workshop**	**Organised**
Sep	**6th**	**Tech Against Terrorism workshop**	**Beirut, Lebanon**	**GIFCT Workshop**	**Organised**

	7th	Tech Against Terrorism workshop partnered with VoxPol	Dublin, Ireland	Workshop	Organised
	11th	22nd IAP Annual Conference and General Meeting of the International Association of Prosecutors	Beijing, China	Conference	Presented
	18th	**Tech Against Terrorism workshop**	**Facebook office in New York, USA**	**GIFCT Workshop**	**Organised**
	18th – 22nd	Vox Pol Training Academy: Topics in Violent Political Extremism, Terrorism, and the Internet	The Hague, Holland	Training Academy	Attended
	29th	US DHS: Digital Forum on Terrorism Prevention	Washington D.C., USA	Forum	Co-organised
October	6th	"Addressing the Message and Protecting the Medium" – GNI Roundtable	London, UK	Roundtable	Attended
	24th	**Tech Against Terrorism workshop at Microsoft office**	**Microsoft office, Paris, France**	**GIFCT Workshop**	**Organised**
	30th	Tech Against Terrorism workshop	London, UK	Workshop	Organised
November	1st	"Building Resolve", National Counterterrorism Centre	Washington D.C., USA	Event	Presented
	7th	**Launch of Tech Against Terrorism and the GIFCT, APAC**	**Jakarta, Indonesia**	**GIFCT Workshop**	**Organised**
	8th	Web Summit 2017	Lisbon, Portugal	Tech Conference	Presented
	16th	ACAMS FinTech in the Nordics	Copenhagen, Denmark	Conference	Presented
	16th - 17th	GCTF Countering Violent Extremism (CVE) Working Group, Eight Plenary Meeting	Valletta, Malta	Conference	Attended
	23rd	The Westminster Counterterrorism Conference (RUSI)	London, UK	Conference	Attended
	29th	Launch of the Knowledge Sharing Platform at the United Nations	New York, USA	Initiative Launch	Organised
December	1st	Specialized Training on Global Threats to Justice, Peace and Security, UNICRI	Turin, Italy (joined via video conference)	Lecture via video conference	Presented
	5th	**Tech Against Terrorism workshop with GIFCT**	**Facebook office, Brussels, Belgium**	**GIFCT Workshop**	**Organised**
	6th	EU Internet Forum Ministerial Meeting	Brussels, Belgium	Event	Presented
	8th	The Legal Framework for Countering Terrorist and Violent Extremist Content Online, Swiss Institute of Comparative Law	Lausanne, Switzerland	Conference	Presented

Appendix 2: Workshops - Feedback from smaller platforms – *not the views of Tech Against Terrorism*

San Francisco on 1 August - Attendees: 107 - Companies: 25		
Terms of Service	**Content moderation**	**Transparency & Redress**
Encompass all terrorist and violent extremist groups when considering definitions used in Terms of Service and Community Guidelines Maintain the option for companies to opt-out of suggested ToS if they wish	Promote counter-narratives because content takedown should not be the only solution to tackling harmful content Create a way for small tech platforms to host counter-narrative content	Provide template transparency reports to guide how companies share data Encourage companies to include a disclaimer when content has been removed to enhance transparency
Beirut on 6 September - Attendees: 50 - Companies: 9		
Terms of Service	**Content moderation**	**Transparency & Redress**
Define terrorist content using the UN Sanctions List and other designations lists to ensure that there is great clarity Design Terms of Service and Community Guidelines that are tailored to the specific services of a smaller platform	Ensure that technology (AI and machine learning) is not solely responsible for moderation given concerns about bias and potential violation of freedom of expression Encourage user flagging of harmful content	Emphasise the need for greater transparency of data requests Provide more transparency about existing regulations with regard to the transfer of data between companies
Dublin on 7 September - Attendees: 34 - Companies: 9		
Terms of Service	**Content moderation**	**Transparency & Redress**
Encourage companies to include their own definitions of key terms in their Terms of Service Prioritise defining 'illegal activity' in Terms of Service as this encompasses everything harmful in a given jurisdiction	Consider the potential 'unintended consequences' of content takedown such as creating grievance and providing validation for terrorists and terrorist sympathisers Consider alternatives to takedown including warning notices, placing content behind login systems, removing from search / suggested content	Provide more transparency to ensure users are informed about which government agencies request information from tech companies Provide more detail in transparency reports in a way that facilities comparison of transparency reports across a range of platforms
New York on 18 September - Attendees: 75 - Company Representatives: 13		
Terms of Service	**Content moderation**	**Transparency & Redress**
Create Terms of Services templates that are specific to each type of technology Develop detailed ToS that helps users understand why content is flagged or considered harmful	Provide companies examples of "grey content" on an online portal Create a list of terminology to inform content moderation Provide tools such as translation	Develop a centralised database of national laws on regulation and content takedown Develop simple templates for companies to complete transparency reports – platforms already have limited time

Paris on 24 October - Attendees: 39 - Companies: 6		
Terms of Service	**Content moderation**	**Transparency & Redress**
Develop a company benchmark report that outlines how approaches vary in this area	Provide guidance to smaller companies based on the experiences of larger tech Collate extremist terminology to help understand nuances of harmful content	Provided clearer definitions regarding transparency reporting, i.e. breaking down government requests between federal and local – "if you want to be transparent, be fully transparent"
London on 30 October - Attendees: 42 - Companies: 9		
Terms of Service	**Content moderation**	**Transparency & Redress**
Provide companies with a list of typologies - patterns of behaviour - that companies could share with one another and use to inform Terms of Service development	Pair academics with tech companies to ensure that content moderators are well-informed	Expand transparency reports to include the fintech industry if possible since fintech have some similar challenges in terms of tackling criminal use
Jakarta on 6-7 November – Attendees: 30 - Companies: 6		
Terms of Service	**Content moderation**	**Transparency & Redress**
Ensure that Terms of Service and Community Guidelines are specific to the local and regional dynamics of the communities that are using the platform	Use smaller platforms to amplify of counter-narrative efforts Provide psychological support to content moderators Offer insight into how companies deal with harmful content	Provide user community with more information about the type of access governments request
Brussels on 5 December - Attendees: 60 - Companies: 12		
Terms of Service	**Content moderation**	**Transparency & Redress**
Collaborate with civil society to build inclusive Terms of Service that take into account human rights and freedom of expression concerns Encourage companies to work together in building consensus around effective terms of service and community guidelines	Understand the risk of automated content analysis/removal tools in relation to undermining important freedoms Encourage study of "mutual radicalisation" and its challenges namely how the rise of one form can trigger another	Encourage greater transparency around the rules of law that offer judicial oversight. For tech companies to continue assisting with law enforcement investigations and to work together while entering a "new legal era"