Adam Hadley

Executive Director, Tech Against Terrorism

Tech Against Terrorism is a public private partnership initiated by UNCTED in 2016. We are an independent not for profit and we work with all the major stakeholders in this area including a whole range of smaller and medium sized platforms as well as the industry-led Global Internet Forum for Counter Terrorism .

In addition to this, we work with governments, international organisations and civil society. Our purpose is to disrupt the terrorist use of the internet in order to save lives. We do this primarily by supporting smaller platforms, but recognising that it's critical to involve a broad network of stakeholders as genuine public private partnership. Whilst promoting improved tech responses to the terrorist use of the internet we also encourage stakeholders to uphold the rule of law and protect fundamental freedoms. What is the point of tackling the terrorist use of the internet if in doing so we erode our own hard won freedoms?

This session is focussed on public private partnerships. What I know about leading a public private partnership is that balancing perspectives and interests can be extremely challenging - we have to try to influence but not coerce. We believe that by providing meaningful support to platforms we are in a good position to ensure we continue to deliver positive impact. Accordingly, we support over 100 platforms, big and small with challenges as diverse as content moderation policy, threat intelligence, regulatory analysis, and technical approaches - all using inhouse open source intelligence and software engineering capabilities.

What do we do?

First, we seek to understand the threat and how terrorists use the internet. We have our own in-house team of open source intelligence analysts monitoring around 100 platforms at any one point for emerging terrorist content.

Secondly, we support platforms in a practical sense by providing operational support through online resources, regulatory analysis, workshops and webinars. We also support the Global Internet Forum for Counter Terrorism and many other organisations by providing a mentorship service to ensure that platforms meet minimum standards for tackling the terrorist use of the internet. Crucially this also includes requirements to uphold the rule of law and fundamental freedoms.

Thirdly, we build technology like the Terrorist Content Analytics Platform (TCAP) - more information at http://www.terrorismanalytics.org - that automates the process of identifying, verifying, alerting, and archiving terrorist content. As part of this we only include content that is officially created by terrorist organisations designated by the UN, EU, and other democratic jurisdictions. We also provide software engineering and data science support to platforms, as smaller ones often have limited capacity to implement technical approaches.

We know terrorists use a range of platforms, many dual-purpose, which presents challenges around content moderation while upholding rights. But terrorists are opportunistic and will exploit new technologies as they emerge, like generative AI.

While these innovations must be mitigated, we believe focus should not shift entirely from countering proven tactics. The current crisis in the Middle East reflects this - AI and decentralized tech are important but we must not forget to focus on the basics.

The tech sector is doing much better than before, but the threat remains. Terrorists can still use tried-and-tested methods to share content and propaganda.

One major concern is terrorist-operated websites (TOWs) - we're currently tracking over 300 created by designated groups, supported by more than 30 infrastructure providers. This shows the challenge in building partnerships. Terrorists should not have the right to operate their own websites, yet there is a significant presence online. As platforms improve responses, terrorists set up their own sites.

Also, we're seeing a return to normal tactics - in the Israel-Hamas conflict, much terrorist content on social media and messaging apps, mostly from one particular app. This content is graphic and grounded in images of victims and attacks.

The problems of 2016 when we were founded are still there today. While new tech matters, we can't lose focus on terrorists exploiting traditional approaches. One messaging app in particular is a major channel with over 700,000 subscribers associated with a designated terrorist organisation.

Public-private partnerships are difficult due to natural tensions, but the formidable work required makes them essential to ensure consistency, uphold rights and counter the terrorist threat.

(In response to intervention by the Russian Federation)

Thank you to the Russian Federation regarding their question about tech platforms consistently removing content.

At Tech Against Terrorism, we believe that upholding human rights and freedom of expression is essential in countering terrorists' use of internet. Self-evidently if we do not uphold the rule of law, we are letting terrorists win. With that in mind, at Tech Against Terrorism, we only focus on content that has been created by designated terrorist organisations and has been officially branded. We recognise that this excludes a large amount of content that might be considered sub threshold. But nevertheless, we think it's important to be clear about our scope of activity. More information about the scope of our work is available on our website at techagainstterrorism.org. We reference the UN, EU, and US lists of designated terrorist organisations. And then we recommend that tech companies reflect this in practice in terms of upholding their terms of service by removing content that is officially branded by a designated terrorist organisation. There is so much egregious content produced by designated terrorist organisations so we believe that that should be the focus: the perfect should not be the enemy of the good.

Nevertheless, we believe that tech companies ought to be encouraged voluntarily to uphold their terms of service and to be held to account when this doesn't happen.

We also work extensively with several countries and regulators to promulgate and promote best practice in terms of how online regulation is being adopted by the tech sector.

Foremost amongst this is an initiative that we are helping to implement on behalf of the European Union and funded by the European Commission called Tech Against Terrorism Europe (TATE), which works with tech companies offering services in the EU to help promote best practice regarding the EU's new Terrorist Content Online (TCO) regulation. TATE itself is a great example of a successful partnership since it is delivered jointly by a consortium of entities across the EU consisting of Tech Against Terrorism, Dublin City University (DCU), Ghent University, the JOS Project, LMU Munich, and Swansea University.

Much like the EU led the way with GDPR, we believe that the TCO and the Digital Services Act (DSA) also has the potential to improve the world for the better by setting a clear normative precedent for thoughtful regulation in this area. The TCO is clear in scope and brings to life the principle that platforms should uphold the rule of law with regards to the removal of terrorist content whilst also ensuring that protecting fundamental freedoms is embedded in tech sector responses.

Finally, we'd argue that transparency reporting is critical because there is a risk that platforms do not take their responsibility seriously enough. By contrast there is the opposite risk that platforms are pressured into removing content that isn't terrorist content. We believe that there's a significant risk that countering the terrorist use of the internet can become weaponized for political reasons. And so, transparency is an effective way of ensuring that tech platforms are removing what they should be. At the same we would encourage governments to be more transparent about what they are asking platforms to remove. With transparency, we believe this increase increases trust and confidence in the measures that the tech sector is developing to ensure that the most egregious content is removed from the internet in a timely and proportionate fashion.