Policinginsight

ANALYSIS:

Online harms: The threat from terrorist and extremist-operated websites

28th July 2022 | Andrew Staniforth | Policing Insight

Picture © MMD Made my dreams / Shutterstock

While the latest US drone strike highlighted the continuing physical global terrorist threat, extremist organisations are increasingly launching their own websites to spread their views and propaganda, and recruit new members; Policing Insight's Andrew Staniforth looks at the online threat posed by terrorists, and the work of Tech Against Terrorism to try and counter that threat.

Earlier this month a US-led military drone-strike operation killed Maher al-Agal, the Islamic State (IS) leader of the terrorist group's Syria branch and one of its top five leaders worldwide, providing evidence that IS remains a clear and present danger.

> "The scale of the threat from websites operated by terrorists and extremists reported by Tech Against Terrorism is shocking, and demonstrates the scale of the security challenge for all in authority engaged in counter-terrorism across the world."

The operation also indicates that active, covert intelligence activities against IS terrorist targets remain a high priority among western nations to preserve international security. The drone strike operation shows the level of investment and resource still being committed to confront the real physical threat from contemporary terrorism; but as more terrorists have taken their fight online in the virtual and ungoverned domain of cyber space, more needs to be done to address the continued rise of non-physical terrorist threat vectors.

As an example of online terrorist activity, earlier this year, Tech Against Terrorism published its report *The Threat of Terrorist and Violent Extremist-Operated Websites*, which found that terrorist and violent extremist actors were running at least 198 websites on the surface web.

Further in-depth analysis of 33 of the most prominent websites – run by actors such as IS, al-Qaeda, Atomwaffen Division, and the Taliban – confirmed that these sites had 1.54 million monthly visitors, with the majority coming from Algeria, Pakistan, the US and the UK. The scale of the threat from websites operated by terrorists and extremists reported by Tech Against Terrorism is shocking, and demonstrates the scale of the security challenge for all in authority engaged in counter-terrorism across the world.

Adam Hadley, Founder and Director of Tech Against Terrorism stated: "The fact that terrorists and violent extremists are able to operate hundreds of websites attracting millions of views with impunity is a failure on behalf of the global online counter-terrorism sector. "Terrorist-operated websites are the key strategic threat with regards to terrorist use of the internet. It is clear that policymakers need to devote more political capital towards identifying practical and policy-oriented solutions to this challenge."

Key findings

Since January 2021, Tech Against Terrorism has conducted open-source intelligence (OSINT) research into the threat of terrorist and violent extremist-operated websites. Their methodology comprised of keyword searches across several mainstream and niche social media and messaging apps, as well as search engines and bespoke apps, mostly conducting searches in English and Arabic, though also in Dari, Pashto and Russian.

They also identified terrorist and violent extremist-operated websites through daily monitoring of online terrorist spaces that were likely to promote sites, such as social media platforms and messaging platforms. The daily monitoring encompassed both mainstream and niche social media, video sharing platforms, and messaging platforms.

The 198 websites identified by Tech Against Terrorism included sites which promoted violent extremist ideologies such as Neo-Nazism, violent insurrectionary accelerationism, Salafi-Jihadism, and Incel ideology. Analysis of these sites found that 101 websites were operated by far-right violent extremist or terrorist groups, 79 by violent Sunni Islamist extremist or terrorist groups, and 18 by violent Shia Islamist extremist or terrorist groups.

> "The Tech Against Terrorism report indicates that terrorist-operated websites constitute a key propaganda organ for terrorist and violent extremist groups, allowing them to disseminate recruitment material without disruption."

The analysis of the 33 most prominent sites revealed that 91% displayed audio and visual propaganda, 73% contained an archive of historic terrorist content, and 57% included a contact address form. Of direct concern for UK Counter-Terrorism Policing is that 16 violent far-right websites saw most of their visitors from the US, the UK, and Czechia.

The Tech Against Terrorism report indicates that terrorist-operated websites constitute a key propaganda organ for terrorist and violent extremist groups, allowing them to disseminate recruitment material without disruption. The rise in prominence of such websites is likely the result of improved removal campaigns across other parts of the tech industry, including on larger social media platforms.

Key challenges

The analyses conducted by Tech Against Terrorism concludes that there is currently no unified global approach against terrorist-operated websites. They recommend that governments step in and create a strategy to disrupt such sites, based on collaborative engagement with web infrastructure providers and on human rights safeguards. What is clear from the findings is that responses to terrorist and violent extremist-operated websites can be severe in that they often constitute the removal or blocking of entire websites.

There are therefore several ethical challenges posed by tackling websites to ensure firm but fair responses are put in place and tighter regulation may be preferrable to more anti-terror legislation which, if used disproportionately, can have potential long-term damaging consequences on fundamental human rights.

As Lord Carlile, the UK's former Independent Reviewer of Terrorism Legislation, previously stated: "Terrorism law should be used only for terrorism purposes. Every step outside those purposes provides terrorists with an argument. All in authority are required never to forget that such laws are a step outside the norms of criminal justice legislation."

A way forward

> "The Tech Against Terrorism report concludes that there are deeper questions about what role infrastructure providers should play in 'moderating' the websites they support or host."

The Tech Against Terrorism report concludes that there are deeper questions about what role infrastructure providers should play in "moderating" the websites they support or host. It is their assessment that – partially due to a lack of strategic focus on terrorist and violent extremist-operated websites on the part of governments – these questions are often left for infrastructure providers to answer on a case-by- case basis.

While it is easy to highlight inconsistency from infrastructure providers in this regard, Tech Against Terrorism are right to argue that this should not be a decision that rests with them. As an inter-disciplinary team consisting of counter-terrorism experts and developers, Tech Against Terrorism continue to offer tech companies practical and operational support to help them implement effective mechanisms to respond to terrorist use of the internet.

Supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED) working with the global tech industry to tackle terrorist use of the internet while respecting human rights, Tech Against Terrorism provide unique insights to the threat from online terrorism, a danger that urgently requires further resource and investment from nations across the world to prevent the rise of terrorist and extremist violence.

Link to online article at Policing Insight: https://policinginsight.com/features/analysis/online-harms-the-threat-from-terrorist-and-extremist-operated-websites/

Andrew Staniforth is Director of Innovation at SAHER (Europe), a security research, training and consultancy operating at a global level, participating in the NOTIONES (*iNteracting netwOrk of inTelligence and securIty practitiOners with iNdustry and acadEmia actorS*) network, funded by the European Commission Horizon 2020 Programme (No. 101021853). Andrew is also an active Researcher of Cyber Threats at the Hillary Rodham Clinton School of Law and Criminology, University of Swansea. As a former Counter-Terrorism Detective, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch. **Contact:** Andy@saher-eu.com
To learn more about NOTIONES visit: https://www.notiones.eu