Tech Against Terrorism

–

Trends in Terrorist and Violent Extremist Use of the Internet | Q1-Q2 2021

July 2021

Tech Against Terrorism – An initiative supported by UN CTED

contact@techagainstterrorism.org

EXECUTIVE SUMMARY

This report covers key trends in terrorist and violent extremist use of the internet and is based on Tech Against Terrorism's open-source intelligence (OSINT) team's monitoring over the past six months. Most trends outlined in this report have arisen partly as a consequence of improved content moderation by tech platforms in recent years, as well as the continued resilience and adaptability of terrorist networks online. This report aims to highlight the shifts in terrorist behaviour and tactics online, and seeks to inform more comprehensive, cross-platform responses to countering terrorist exploitation of the internet.

The adversarial shifts outlined in this report are likely to have far-reaching and varied impacts on online counterterrorism efforts in the coming months. Our investigations indicate terrorist actors are growing more adept at exploiting emerging technologies and establishing their own online infrastructures. This presents challenges to many current online counterterrorism strategies, that are grounded in removing terrorist content from established sites and platforms. Terrorist exploitation of open-source software is likely to cause obstacles for current counterterrorism efforts. This is due to the inherent nature of open-source technologies, which is grounded in public accessibility and open distribution. Additionally, as terrorists grow more sophisticated at avoiding online content moderation, tech platforms must expand their knowledge and adapt their practices to combat the challenges posed by terrorist exploitation. Tech Against Terrorism strives to support platforms in tackling terrorist and violent extremist exploitation of their services, principally through our Mentorship Programme, The Knowledge Sharing Platform, and the Terrorist Content Analytics Platform (TCAP).

Increased use of "cloud platform" websites

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

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

Increased and diversified use of the decentralised web

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

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

Resurgence of terrorist operated websites

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

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

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

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

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

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

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

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

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

TVE supporter networks pose as news channels

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

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

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