STATE OF PLAY

tech against terrorism

TRENDS IN TERRORIST AND VIOLENT EXTREMIST USE OF THE INTERNET

2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ISLAMIST TERRORIST AND VIOLENT EXTREMIST NETWORKS

- Resurgence of terrorist operated websites
- Use of content moderation avoidance tactics on Big Tech
- Translation of propaganda into a wide range of languages

FAR-RIGHT TERRORIST AND VIOLENT EXTREMIST NETWORKS

- Gamification of terrorism and violent extremism
- "Goreposting," including support for Islamist TVE content
- Experimentation with wider range of platform types

CRISIS EVENTS AND ONLINE RESPONSE

- Targeting of gaming platforms to share attacker-made content
- Targeting of file sharing platforms to evade content moderation
- Insufficient support for small platforms in current response mechanisms

RUSSIAN INVASION OF UKRAINE

- Mixed response from far-right TVE networks on which side to support
- Documentation of war crimes by pro-Kremlin forces
- Financing of far-right TVE groups via cryptocurrencies

INTRODUCTION

This report covers key trends and developments in terrorist and violent extremist (TVE) use of the internet over 2022. It aims to highlight the principal shifts in TVE behaviour and tactics online, and to inform more comprehensive, cross-industry responses to countering TVE exploitation of the internet. TVE entities have expanded their exploitation of infrastructure providers through the ongoing creation and maintenance of terrorist and violent extremist operated websites (TOWs); despite the increasing prominence of TOWs in the online ecosystem, these service providers are frequently left out of the discussion of countering TVE exploitation of the internet. We have highlighted in this report some of our successes of 2022, which include domain-level disruption of TVE entities online as well as our broader support for the entire tech ecosystem.

Over 2022, we have identified shifts in how a range of TVE networks operate online, including both Islamist and far-right terrorist groups and individuals. These shifts include changes in the types of platforms they target, the methods of propaganda sharing, and in online responses to offline events. In summary, TVE entities have expanded their online capabilities through the exploitation of new platforms and platform types to share propaganda, communicate, and fundraise. Most trends in TVE behaviour outlined in this report are caused at least in part by improved content moderation in recent years by tech platforms and demonstrate the continued resilience and adaptability of TVE networks online.

Moving into 2023, Tech Against Terrorism will continue to support the tech sector in tackling and disrupting TVE exploitation of the internet, through tracking, analysing, and alerting TVE entities across the entire online ecosystem. We will particularly be focusing on expanding our support for infrastructure providers, increasing our crisis response abilities, and providing comprehensive support to tech companies of all sizes.

ACTION TAKEN BY TECH AGAINST TERRORISM IN 2022

Facilitated the disruption and removal of **6 terrorist operated websites**

Flagged **10,036 URLs** via the Terrorist Content Analytics Platform (TCAP) to **56 tech platforms**

Flagged an additional **557 URLs** containing terrorist and violent extremist content outside the scope of the TCAP to **38 tech platforms**

Collected, analysed, and disrupted the spread of attacker-produced propaganda following attacks in **Buffalo**, **Udaipur**, **Memphis**, and **Bratislava**

Identified and alerted **5 email addresses** being used by terrorist and violent extremist entities

Monitored far-right terrorist and violent extremist involvement in the Russian invasion of Ukraine

TECHNOLOGY TRENDS

Terrorist and Violent Extremist Operated Websites

Terrorist and violent extremist operated websites (TOWs) remain a popular tool for TVE actors seeking to establish or maintain a foothold online and continue to undermine broader efforts to combat TVE content on the surface web. The barrier to entry for website hosting and creation is low. There is also little international consensus on how to disrupt this threat effectively. TOWs have persisted throughout 2022.

Terrorist and violent extremist operated websites (TOWs) remained a significant and persistent threat throughout 2022, both on the "clear web" and on ".onion" sites hosted on Tor. TOWs in 2022 were used for a variety of purposes, including storage of official content, crowdfunding, and communications. Tech Against Terrorism currently monitors more than 200 TOWs, ranging from Islamist terrorist content translation sites to violent far-right communication hubs. Largely driven by greater levels of stability achievable when using a TOW as opposed to when hosting a location on larger-scale social media platforms, and having to move domains when required, online actors have exploited a lack of global consensus, variations in jurisdictional precedents, and higher thresholds for removing entire websites.[1] This lack of consensus, underpinned by jurisdictional and legal challenges to the effective removal of TOWs, has provided a space for website operators permitting the storage and sharing of officially produced terrorist content.

We frequently observed migrations to new domains, most probably as a result of disruption efforts, pre-arranged switches to new URLs, or top-level domain changes. This is facilitated by the low barrier to entry for TOW operators, if their intentions are not detected in the site registration process. Websites are cheap to create and maintain, and even more so if operators have made templates of the sites and their pages – removing the need to recreate the TOWs completely. In one

[1] "Report: The Threat of Terrorist and Violent Extremist Operated Websites" January 2022. Available at: https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/

notable example, a translation site for IS content has changed domains on at least eight occasions since we began our monitoring of it in late 2021. Despite this trend, many TOWs stay live on one domain for months or years without disruption. Prominent IS websites more frequently migrate to a new URL or top-level domain compared to other types of TOWs, likely due to inconsistent industry disruption efforts. In general, however, most sites will remain in the same location for considerable periods of time without disruption.

Big Tech

While official TVE content is often more concentrated on small and micro platforms, Big Tech platforms are still an integral part of the online TVE ecosystem due to their potential to reach a large, mainstream audience. As Big Tech platforms diversify their products, the risk of TVE exploitation is also incurred by online marketplaces, crowdfunding services, and encrypted communications software.

Big Tech platforms are a fundamental part of the online TVE ecosystem since they enable TVE entities to reach a large and mainstream audience. Despite TVE content concentrating on small platforms and self-hosted servers and websites, we identified multiple TVE networks seeking to exploit Big Tech platforms over 2022 for propaganda sharing, communicating, and selling merchandise. Big Tech platforms are typically understood as large social media and messaging platforms which have a high volume of users and typically a high capacity for both human and automated content moderation; examples include ***Facebook***, ***YouTube*** and ***Twitter***. TVE entities operating on Big Tech platforms typically employ a wide range of tactics to evade content moderation tactics in order to maintain their presence and potential reach. Some of these evasion tactics we observed over 2022, and consistent with 2021, are as simple as deliberate misspellings of key terms but also include more sophisticated techniques such as the removal of TVE logos and addition of legitimate logos (such as those of media entities) to videos.

There has been an increasing prevalence of IS and Al-Qaeda content on Big Tech platforms in languages other than English and Arabic. This is likely in part due to concerted efforts by these organisations and their core supporters to reach a broader audience internationally, but it is also likely due to difficulties experienced by tech companies to effectively detect and remove TVE content in multiple languages. While content in English and Arabic is moderated and removed consistently, content in other languages, especially lesser spoken languages and regional dialects, appears to be less likely to be automatically identified as TVE content. It is highly likely that the use of other languages allows TVE content to remain online for longer as the capacity to moderate content in all languages is not uniform within the tech sector.

Over 2022, we identified the development of TVE financing methods by the exploitation of marketplaces on Big Tech platforms. As the larger platforms increase their product diversity, the likelihood of TVE exploitation increases. We have identified Islamist and far-right TVE networks exploiting large social media marketplaces to sell merchandise explicitly relating to TVE groups, networks, and ideologies. TVE exploitation of Big Tech marketplaces appears to be currently rare and uncoordinated, however, and practised on a smaller scale than the exploitation of other online marketplaces and e-commerce platforms.

TVE opinion of ***Twitter*** following the Elon Musk takeover has shown a mixed response. Some TVE actors and entities have attempted to return to ***Twitter***, such as Rinaldo Nazzaro (the founder of The Base) and Anjem Choudary (a Specially Designated Global Terrorist). The removal of key staff responsible for Trust and Safety at ***Twitter*** has likely increased TVE actors' intent in operating on the platform, due to a perception of greater stability and security there. The upheaval in content moderation practices at the company is likely to undermine current efforts in removing and countering TVE content across the online ecosystem.

File Sharing Platforms

File sharing platforms continue to face a significant threat of exploitation by TVE actors, particularly networks affiliated with Islamist terrorist organisations. URLs relating to file sharing platforms comprised the majority of links submitted to the Terrorist Content Analytics Platform (TCAP) in 2022.[2] Far-right TVE content has also increasingly been uploaded to file sharing platforms following crisis events, when tech industry moderation efforts have been focused on the removal of attacker-produced content such as manifestos or livestreams.

File sharing platforms continued to be widely exploited by TVE actors in 2022, particularly by core networks of violent Islamists affiliated with IS and Al-Qaeda. Of the 18,000 URLs submitted to our Terrorist Content Analytics Platform (TCAP) containing terrorist content in 2022, 11,000 (61%) related to file sharing platforms. Most of them were content produced by IS, Al-Qaeda, or their official provinces and affiliates.

These organisations and their core supporter networks have persisted in their long-pursued strategy of uploading multimedia releases to multiple file sharing platforms simultaneously, before sharing the URLs in aggregated form on messaging apps or paste sites. This technique ensures the material will remain available for as long as it takes the slowest platform to take it down.

In 2022, we identified increasing TVE exploitation of micro file sharing platforms built using open-source code that is publicly available online. Several such sites have appeared more often in URL lists, particularly relating to official IS propaganda. This experimentation is likely an example of adversarial shift, as TVE actors migrate away from platforms which are removing their content more quickly than previously.

[2] “Terrorist Content Analytics Platform” January 2023. Available at: https://terrorismanalytics.org/

Far-right TVE networks have also increasingly turned to file sharing services in 2022, particularly at times when specific pieces of content are under scrutiny by tech companies, such as livestreams and manifestos produced by lone actor attack perpetrators. Links to this content are often then shared on larger tech platforms or messaging apps, likely as part of a content moderation evasion effort.

Gaming and Gaming-Adjacent Platforms

While gaming and gaming adjacent platforms are infrequently targeted to share TVE propaganda and official content, these platforms are increasingly important to far-right TVE networks as a means of providing ideological support to attack perpetrators. Gaming-adjacent platforms have also been exploited by far-right TVE networks to vet applicants, through voice and video chat functions, seeking entry to closed online spaces. It is likely these closed spaces are being used to recruit users into TVE movements and share propaganda material that is likely moderated elsewhere online.

Over 2022, we identified sporadic TVE exploitation of gaming and gaming-adjacent platforms. This exploitation has primarily been carried out by supporter networks of TVE entities and violent extremist networks that are not officially designated; exploitation has focused on providing ideological support for TVE attack perpetrators. On one gaming platform, we identified at least 40 computer-generated versions of offline attacks, including but not limited to Christchurch (2019), Buffalo (2022), Oslo and Utøya (2011), Bataclan, Paris (2015), and the Nairobi Westgate Mall (2013). The computer-generated versions of offline attacks all allowed users to take part in the simulated game, most of which allowed users to play as the original attack perpetrators. The Buffalo (2022) and Christchurch (2019) attacks are those most frequently recreated on gaming platforms based on our research, both attacks having been filmed using helmet-mounted cameras in deliberate emulation of popular first-person-shooter (FPS) games.

Far-right TVE networks have also exploited gaming-adjacent platforms, in conjunction with other platforms, to vet users before allowing them into closed and restricted online spaces. Some gaming-adjacent platforms have the ability for voice and video chats between users, allowing members of far-right TVE networks to interact with other users before allowing them into restricted spaces. It is highly likely that these restricted spaces are used to share propaganda which would be heavily moderated elsewhere online or in open spaces.

We also identified one TVE attack perpetrator who openly exploited gaming platforms to disseminate content. In May 2022, the Buffalo attack perpetrator publicised an online diary which they had created through a dedicated, private server hosted on ***Discord***. They claimed that they had previously played games on ***Roblox*** and even stated "I probably wouldn't be as nationalistic if it weren't for Blood and Iron on roblox." The online diary began at least six months before the attack and contained multiple details about the attacker's ideology and the attack itself, such as the proposed location, weapons, and plan.

Search Engines

While deliberate TVE exploitation of search engines is low, search engines can be used to circumvent content moderation efforts undertaken elsewhere online and contribute to the longevity and discoverability of TVE content. Search engines can greatly increase the audience reach of TVE content, primarily by redirecting users to TOWs.

Search engines can increase the discoverability of TVE content on the surface web and maximise its reach. We have seen no evidence to suggest that TVE entities seek to deliberately exploit search engines or manipulate search engine results to make TVE content more discoverable. However, TOWs and other pages hosting TVE content are often indexed in mainstream search engine results, allowing them to be accessible and easily discoverable for vulnerable individuals who are seeking

out the content. Even if a page on a platform is removed, an indexed search result can help a user find the content if the indexed result preview contains an outlink to another platform or page.

Result filtering is inconsistent between search engines, with some search engines more effectively downranking or removing indexed TVE content than others. Search terms in English are typically better filtered to downrank or remove TVE content when compared to search terms in Arabic and other languages. However, regardless of language, search engines often appear to struggle to effectively filtout or downrank TVE content including TOWs linked to a range of TVE entities. Indexed search results leading to TOWs almost certainly assist in the discoverability of TOWs, especially when the indexed result is available within the first page of results.

The Decentralised Web

TVE exploitation of decentralised (Dweb) services is primarily experimental, with Dweb services being used alongside (or as backups to) conventional, centralised platforms and services. As Dweb technology continues to innovate and the usership of Dweb platforms continues to grow, it is almost certain that terrorist motivation to exploit the Dweb will increase.

Terrorist exploitation of decentralised (Dweb) platforms both expanded and diversified in 2022. We saw frequent targeting of Dweb file and video sharing and messaging applications throughout the year, involving a diverse range of TVE actors. Both Al-Qaeda and Islamic State networks routinely use messaging servers based on Dweb technology, and some far-right TVE actors have been experimenting with Dweb services in the face of imminent or actual suspension by more conventional messaging applications.

We have also identified examples of TVE exploitation of the Dweb to host websites that are accessible on a conventional browser. In some cases, these have been

accessible via gateways for the ***Interplanetary File System (IPFS)***, a Dweb file storage system on which files can be accessed via gateway URLs on a standard HTTP browser (such as ***Chrome*** or ***Firefox***). This year a prominent pro-IS website, which acts as an online directory of IS-related resources across the web, experimented with a Dweb domain in addition to a version on the .onion network.

Terrorist financing and crowdfunding is also increasingly transacted in cryptocurrencies, particularly Monero, with terrorist actors sharing crypto wallets alongside propaganda and messaging channels. In particular, we have observed crowdfunding via crypto by far-right TVE networks fighting on the Russian side of the war in Ukraine.

In September, there was also a widely reported instance of IS propaganda being shared by a supporter of IS in the form of non-fungible tokens (NFTs). The images comprised anattack claim published by IS, an image purportedly showing bomb-making instructions, and an anti-smoking image. To our knowledge this was the first time that individuals associated with designated terrorist entities have exploited NFTs for propaganda purposes. This incident is best understood as an example of experimentation with new technologies, rather than the start of the widespread use of NFTs by terrorists, at least in the short term. The listing for the NFTs included links to copies of the images on a Dweb file sharing platform – we reported this to the operator and the links were suspended.

The Dark Web

Terrorists continued to operate propaganda websites on the dark web in 2022. Our research indicates that these are less prominent in the online terrorist ecosystem than sites on the surface web, comprising a minority of the total sites monitored by us over the past year. The primary use case for darkweb sites by terrorists has been to act as stable mirror versions of sites on the surface web, particularly when those sites have suffered repeated disruption.

Websites on the Tor network this year have continued to be used by online TVE propaganda networks as a stable location on which to back up their content. Most commonly, darkweb sites act as mirror versions of identical websites on the surface web. URLs to these darkweb sites are often promoted elsewhere online by TVE networks, presenting them as a stable alternative “back-up” where content will be more reliably found. In several cases in 2022 we witnessed TVE entities utilise darkweb sites in precisely this way, including those affiliated with IS-aligned chan boards, and actors who subscribe to militant accelerationist neo-fascist ideology.

Although the darkweb is also likely used for private internal communication by terrorists, our research indicates that it is not as extensively used as the wide range of secure, encrypted messaging apps and email services. These are comparatively easy to use, and provide a similar level of security, privacy and stability to sites on the Tor network.

It is nevertheless likely that the darkweb will be used more extensively by terrorists in the coming years, as online counter-terrorism efforts improve. This will mean that terrorist content on the internet is even more difficult to find, and reduces the likelihood that individuals may unintentionally be exposed to terrorist narratives. However, this scenario will also present further challenges to disrupting terrorist use of the internet, as it is more difficult to identify and disrupt darkweb sites than channels on messaging applications or conventional sites on the surface web.

TERRORIST ENTITY TRENDS

Islamic State

Islamic State (IS) networks have maintained a substantial presence online throughout 2022, despite increasing moderation by tech platforms. This is most likely to be a consequence of a proliferation of tactics to evade content moderation, as well as increased targeting of platforms with little to no content moderation capabilities. Specific exploitation of infrastructure providers to host IS-aligned websites has likely contributed to IS's resilient presence online.

Over 2022, we monitored the spread of both official and supporter-generated Islamic State (IS) propaganda online and identified ongoing migrations across platform types. IS and its official provinces continue to have a robust online presence which produces and disseminates a large volume of propaganda content. Content is typically shared via outlinks, where URLs to content stores are posted on central channels, such as websites, servers, and messaging channels to redirect users to propaganda hosted elsewhere. Throughout the year, we identified over 8,500 URLs containing official IS content across more than 100 platforms; this is almost identical to data from 2021. These URLs were submitted to the Terrorist Content Analytics Platform (TCAP), which was built by Tech Against Terrorism to identify and alert verified terrorist content online.

IS announced two new leaders, in March and December of 2022, via al-Furqan Foundation, an official propaganda outlet typically used for leadership messages. In March, we identified messages from 13 "provinces" (official regional divisions of IS), compared with similar messages from 16 "provinces" in December. Despite pledges of allegiance being carried by more provinces in December, the number of pieces of content we identified in that month (677 URLs) was greatly reduced compared to March (1,539 URLs). The reduction is highly likely due to IS networks' growing tendency to host content in-app on dedicated messaging channels, servers, and websites, rather than linking between multiple platforms where content is likely to be removed.

In November 2022, ***Hoop Messenger***, which IS-affiliated networks had previously used heavily to disseminate official and supporter-generated propaganda content, went offline. Since then, IS networks have experimented with multiple similar messaging platforms, creating a more diverse propaganda sharing network. The elimination of ***Hoop Messenger*** from IS's propaganda dissemination ecosystem is highly likely to only have a short-term impact on the availability of IS and pro-IS content online. In the long-term, it is likely that IS networks will continue to exploit similar messaging platforms simultaneously to ensure content longevity and discoverability. The decline of URLs shown in Figure 1 is likely due to a variety of reasons including: decline in official output, migration to hosting content in-app, and disruption of core IS networks online.

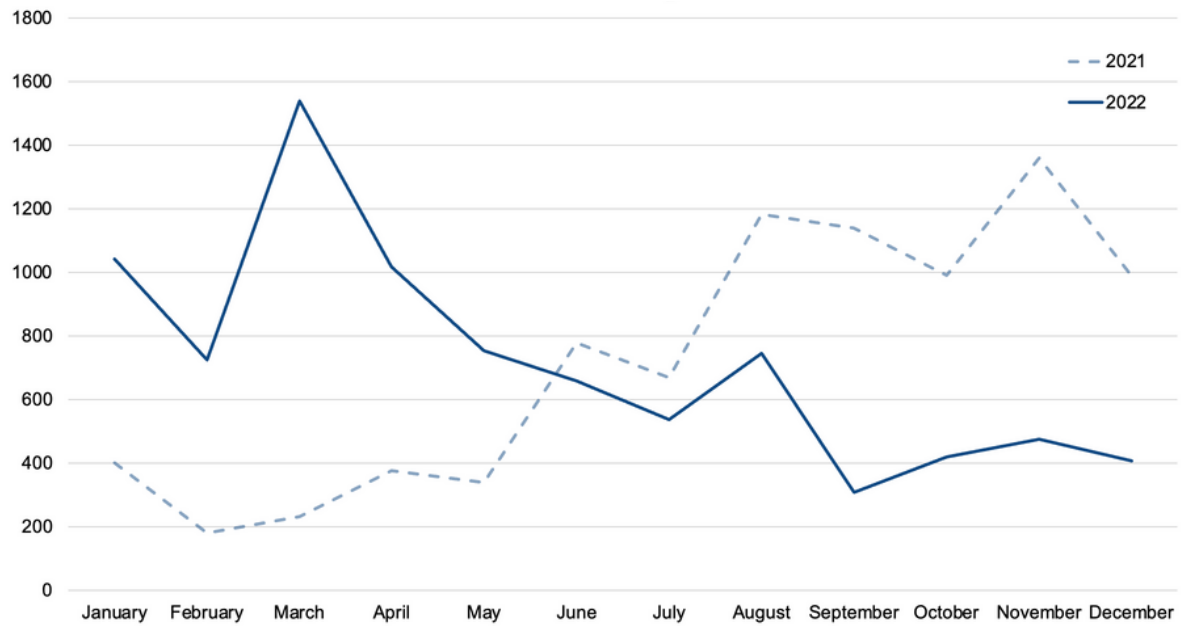

Figure 1: Number of URLs submitted to TCAP containing Islamic State content, 2021-2022

Our analysis of IS exploitation of platform types over 2022 shows a similar targeting in comparison to 2021. Primarily, core IS-affiliated entities targeted (typically small and micro) file sharing platforms to host content, and shared links to this content on messaging platforms as well as IS-affiliated channels, servers, and websites. In 2022, we observed a growth in the use of small and micro-scale file sharing platforms built using open-source code. These platforms typically lack any form of

effective and centralised content moderation and are likely targeted by IS networks to evade the moderation they face on larger file sharing platforms which have more effective moderation capabilities.

IS targeting of 'Big Tech' platforms occurs primarily by means of supporter networks sharing official and unofficial material, rather than as part of IS central media's online presence. IS networks are increasingly targeting websites and infrastructure providers in the course of their online activities, likely because of the relative stability and security of content there, as well as the facility to host large volumes of content on such platforms.

Al-Qaeda

Despite the death of al-Qaeda's leader in July 2022, al-Qaeda and its affiliates remain highly active online and are dedicated to disseminating official propaganda. The networks' methodologies have not significantly altered since 2021 and remain focused on exploiting smaller tech platforms and static websites to evade content moderation.

Al-Qaeda and its regional affiliates have maintained a consistent online presence throughout 2022. We observed official content published by networks and media organisations associated with al-Qaeda's official affiliates, with a diverse range of content including essays, obituaries, and "aid campaign" propaganda. The killing of the group's former leader Ayman al-Zawahiri in July 2022 did not substantively affect the overall frequency of propaganda dissemination of al-Qaeda and its affiliates; we observed a small decline, but not one indicative of a change in tactics, techniques or procedures.

Our monitoring indicates that al-Qaeda networks online have not significantly altered their dissemination strategies from 2021. Al-Qaeda entities continue to target primarily small-scale file sharing and video hosting platforms for the purpose of storing new and historic content. Links to this content are typically shared in channels on

messaging applications, social media and microblogging platforms, and dedicated servers. Al-Qaeda and its official affiliates also continue to operate a network of static websites, many of which have remained active without disruption throughout this year.

Al-Qaeda is also supported by a range of highly active translation sites, highly likely operated by supporter networks. These sites are dedicated to translating and republishing propaganda and extend to the translation of subtitles and the provision of transcripts for visual and audio media. As with official al-Qaeda content, these translated documents and transcriptions are often shared in dedicated spaces such as servers and messaging apps.

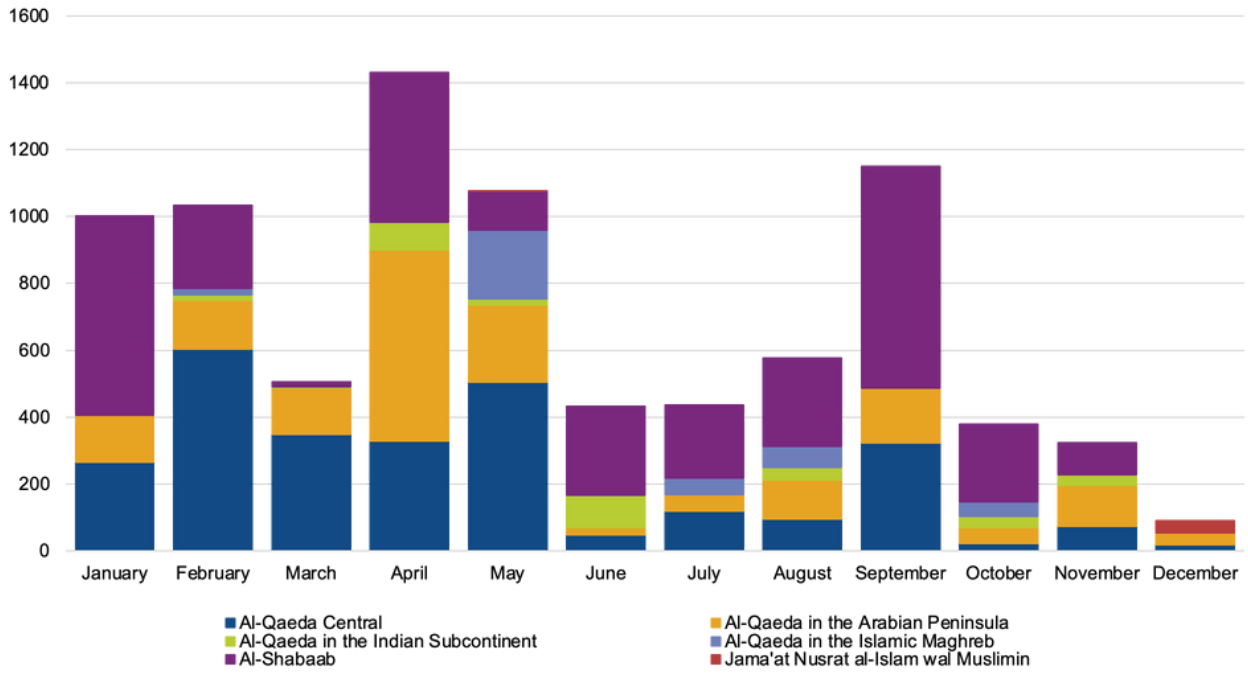

Figure 2: Number of URLs submitted to TCAP containing al-Qaeda content in 2022, categorised by group

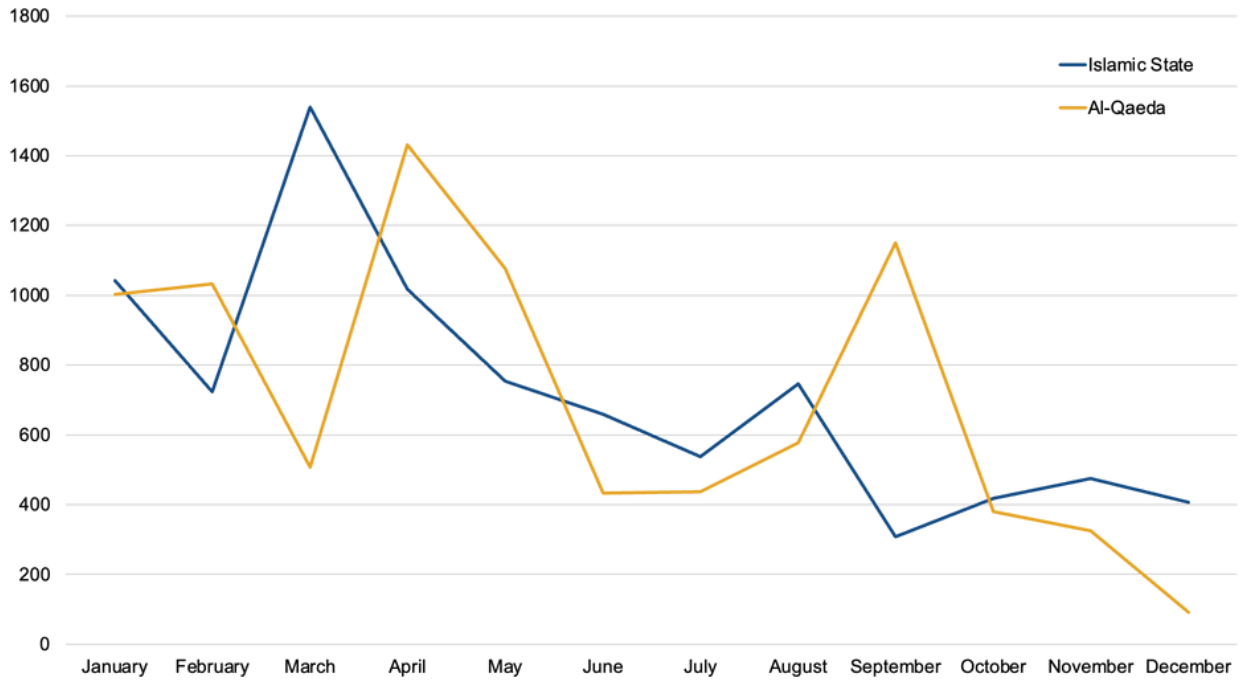

Figure 3: URLs submitted to TCAP comparing Islamic State and al-Qaeda content in 2022

The overall decline of URLs from both Islamic State and al-Qaeda shown in Figure 3 is likely due to a variety of reasons including: decline in official output, migration to hosting content in-app, and ongoing disruption of core propaganda networks online.

Far-Right Terrorist and Violent Extremist Networks

The online far-right TVE ecosystem is an amorphous network of interconnected communities and supports a range of sub-ideologies. The dispersed nature of the online ecosystem was prominent in 2022, with TVE entities increasing their exploitation of a range of platform types, including small file sharing platforms and static websites. Most prominently, core elements of far-right TVE networks have celebrated the perpetrators of lone actor attacks (see Crisis Events and Response), routinely hailing them as "saints" in propaganda.

Far-right TVE use of the internet continued in 2022 to be diffuse in its approach. Activity is undertaken across a significant number of platforms and services, although with more concentration on new and emerging platforms where counter terrorism policies and enforcement are either permissive or rudimentary. This is particularly the case with several "alt-tech" platforms, on which TVE entities exploit free speech-focused policies and platform cultures that resonate with their worldview. In what is likely an effort to maximise their audience and mitigate the impact of deplatforming, it is alsocommon for far-right TVE groups, entities, and networks to operate accounts on several platforms simultaneously.

Figure 4: "Terrortam" logo

Telegram Messenger has continued to face a significant threat of exploitation by far-right terrorist networks. The so-called "Terrorgram" collective released its third and fourth publications online in 2022 on the platform, comprising a digital magazine in July and a video in October. Both publications were preceded by histrionic promotional campaigns online by core members of the Terrorgram network, although neither were shared extensively beyond the core milieu.

"Terrorgram" comprises a network of far-right TVE actors operating tens of messaging channels, primarily on ***Telegram***. The network has been producing propaganda since at least 2019. They promote a narrative that is overtly supportive of terrorism and other forms of political violence, to further their militant accelerationist goals. Due to the network's repeated and obvious violations of ***Telegrams***' Terms of Service, many associated channels were suspended frequently in 2022.

Although such channels have persistently re-emerged on the platform, often in private, in August core elements of the Terrorgram network announced a presence on ***TamTam***, a Russian application with very similar features to ***Telegram***. The network's behaviour on ***TamTam*** closely resembled that on ***Telegram***, with channels using the same names and hosting similar content. However, its subscribership on ***TamTam*** was smaller, and in early December almost all channels monitored by Tech Against Terrorism were suspended from the platform. Since then, the network has been experimenting with several alternative platforms, including ***Matrix***.

Although the material produced by Terrorgram in 2022 reached a relatively small audience online, its messaging remains influential. The perpetrator of a mass shooting at an LGBTQIA+ bar in Bratislava, Slovakia in October specifically cited Terrorgram in his manifesto as an inspiration, thanking them for their "incredible writing and art, political texts [and] practical guides". Terrorgram's propaganda output is specifically intended to encourage lone actors to mount attacks; within its community the perpetrators of far-right TVE attacks are venerated as "saints," with the intention of encouraging an ongoing series of far-right terrorist attacks that mimic and draw inspiration from each other.

Far-right TVE online networks continue to be identifiable more by their community specific slang, common countercultural references and adulation of individual terrorists or ideologues, rather by than their affiliation with (or membership of) hierarchical organisations. These networks have continued to be most concentrated on "alt-

tech” platforms, where they exploit content policies that are more lenient than mainstream alternatives. They have also experimented with Dweb platforms, such as blockchain-based video sharing and livestreaming services. Much of their most egregious content is often saved in libraries on archiving services.

“Goreposting” has also been widespread within far-right TVE communities in 2022. This refers to the practice of sharing extremely graphic or violent content, often unrelated to any given ideological cause, either for entertainment or to desensitise viewers to violence. This has particularly been the case with neo-Nazi networks sharing graphic excerpts or compilations from IS propaganda. File sharing services are also increasingly exploited by the extreme far-right for content that is most likely to be removed from social media or messaging apps, particularly in the immediate aftermath of attacks in which the perpetrator has produced content, such as a livestream or manifesto.

Coinciding with the trend of imitative far-right terrorist attacks by lone actors, hierarchical groups and organisations are continuing to decline in prominence in the broader far-right terrorist online ecosystem. This is likely in part related to the explicit strategy of “leaderless resistance” that has long been pursued and subscribed to by far-right terrorists, but it is also likely influenced by the impact of designation and other forms of legal action against those far-right groups that engage in or advocate for violence.

It is also the case that groups or other named entities which engaged actively in the production of propaganda in 2022 are becoming increasingly ephemeral. Multiple spin-offs of Atomwaffen Division (AWD) and its affiliates appeared online over the course of the year, although many did not last more than a few months. In June, we covered a case study of one such example in detail in a collaborative report with the Center on Terrorism, Extremism and Counter-Terrorism (CTEC) [3]: National Socialist Order (NSO), an organisation comprising former AWD members,

[3] “A Case Study in Neo Fascist Accelerationist Coalition Building Online” June 2022. Available at: https://www.techagainstterrorism.org/2022/06/07/report-a-case-study-in-neo-fascist-accelerationist-coalition-building-online/

splintered into two spinoff organisations, each citing ideological disagreements over Satanism. Neither organisation has yet gained a significant following or maintained a consistent and widespread online presence in producing propaganda content.

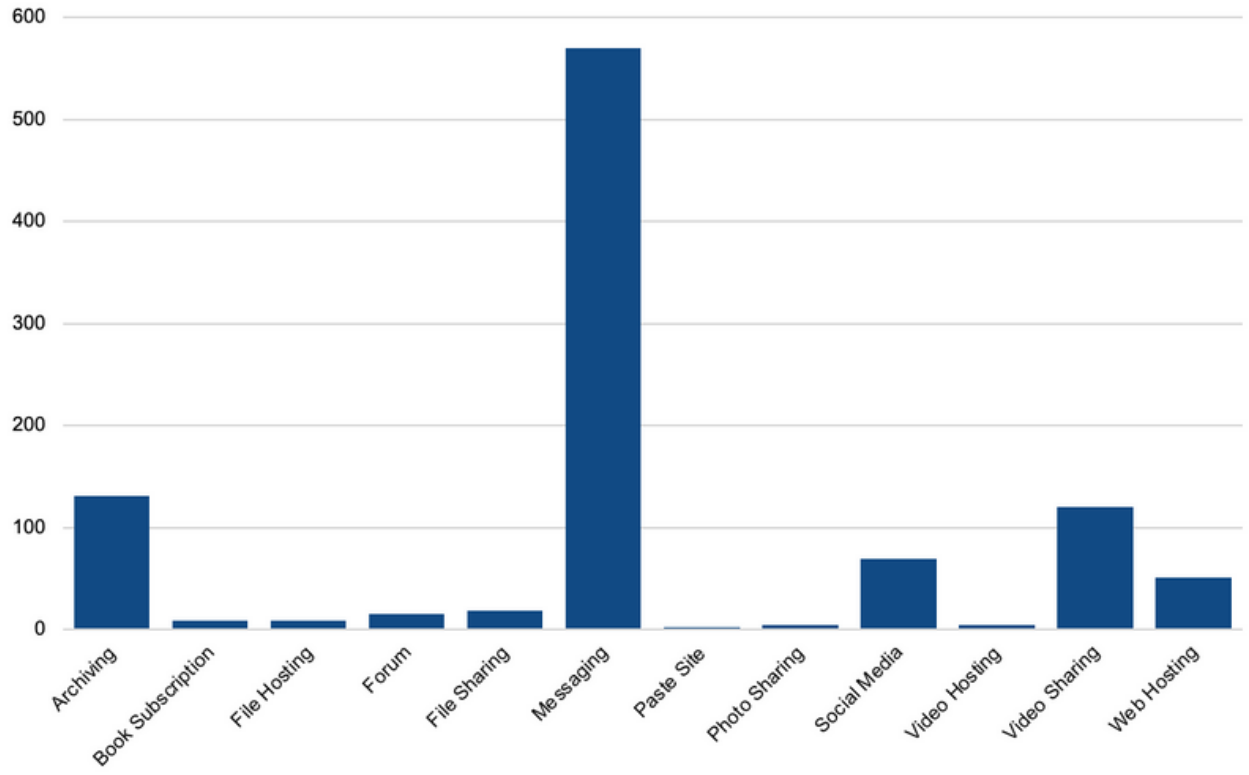

Figure 5: URLs submitted to TCAP containing far-right terrorist material, categorised by platform type, 2022

CRISIS EVENTS AND ONLINE RESPONSE

Responses to TVE content associated with crisis events are not sufficiently supporting or engaging with smaller tech companies. While crisis response mechanisms have begun to address the disparity in the tech sector response to crisis events, these mechanisms typically do not effectively address the threat posed to small and micro tech platforms, the prominence of emerging and evolving technology exploitation, and the resilience of crisis content online long after an attack has occurred.

There were multiple instances in 2022 of attacks in which the perpetrator produced content online to maximise their message, such as a livestream or manifesto. In this section, we examine the essential features of this trend, and we draw on three key case studies showing the impact and spread of the attacker-produced content. We also discuss some current gaps in crisis response workflows in responding to these events.

Figure 6: Terrorist attacks involving attacker-produced content, 2022

Big Tech platforms are typically quicker to respond to attacker-produced propaganda compared to smaller tech companies, due to their automated detection methods and ability to analyse viral content quickly. Current crisis response mechanisms also focus heavily on rapidly disseminated content on Big Tech platforms, which can risk failing to effectively support smaller tech platforms. Automated detection methods on larger platforms also struggle with effectively identifying edited versions of crisis material, which is increasingly common in crisis events. Crisis response should also more effectively consider hostile or uncooperative platforms and TOWs.

With each TVE attack, attack perpetrators are learning from what has worked and what is likely to be effective in ensuring the longevity and wide availability of their online content following their attacks. Far-right TVE attacks often emulate the modus operandi of past attackers and seek to imitate their actions both online and offline, including in weapon choices, livestreaming, target selection, logistical planning, and the documentation of ideology which is typically then published in a manifesto.

CASE STUDY #1
BUFFALO, NEW YORK USA

On 14 May 2022, a person committed an attack with a firearm which killed 10 and injured three others at a supermarket in Buffalo, New York, USA. The attack perpetrator livestreamed the attack on ***Twitch***, released a manifesto detailing their motivation for the attack on ***Google Drive***, and posted a transcript of an online diary originally hosted on ***Discord***. Copies of a livestream, manifesto, and online diary produced by the attack perpetrator spread rapidly across the internet.

Case study #1 involved the spread of a manifesto and livestream across platform types and online communities, in a similar fashion to the dissemination of attacker material following an attack in Christchurch, New Zealand in 2019. The manifesto and livestream created by the Buffalo attack perpetrator were spread widely online

by far-right TVE networks, primarily through messaging platforms, but also through video sharing platforms, social media, and the limited exploitation of file sharing services.

The response from large platforms which moved to identify and moderate the content meant that a large proportion of it was removed quickly, thereby reducing its impact and audience reach. However multiple copies of the material was also uploaded to smaller, more niche services that lacked the same detection capacity, meaning that the material was still accessible online and discoverable via search engines. For example, one copy of the livestream hosted on a small video hosting platform received over three million views before it was taken down by content moderators, over 48 hours after it was published.

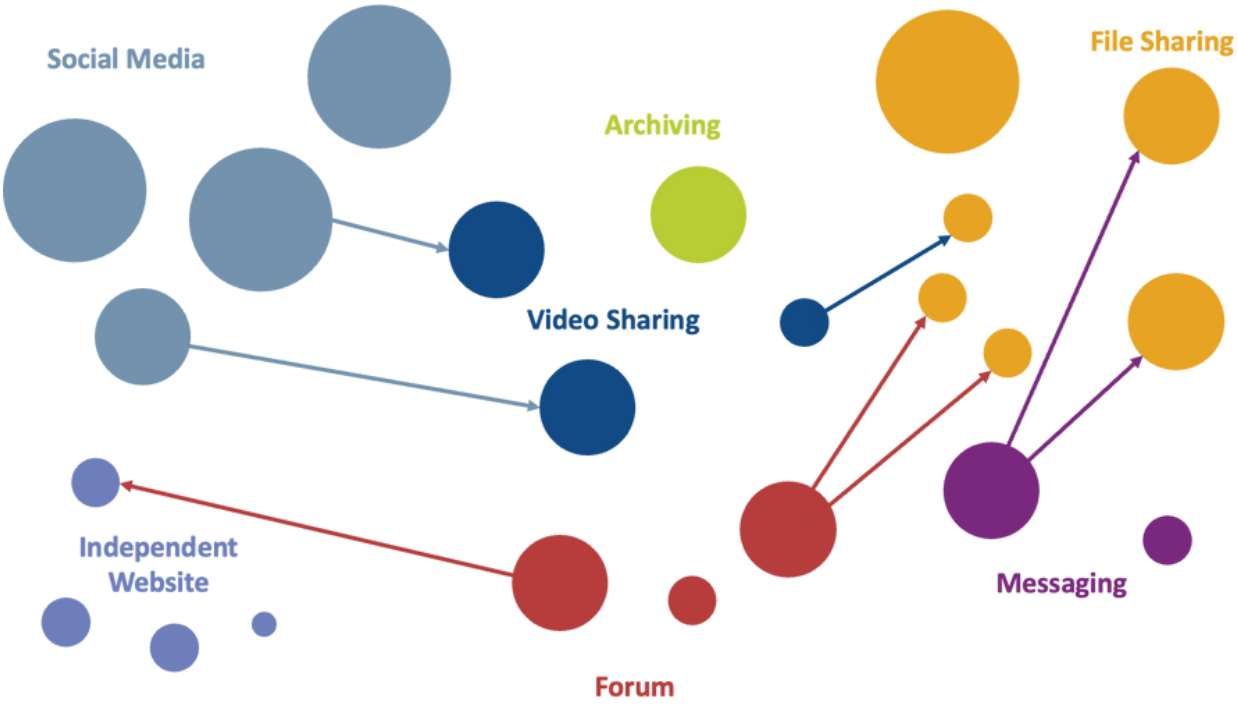

Figure 7: Network analysis of the spread of the Buffalo attacker's manifesto, indicating platform size

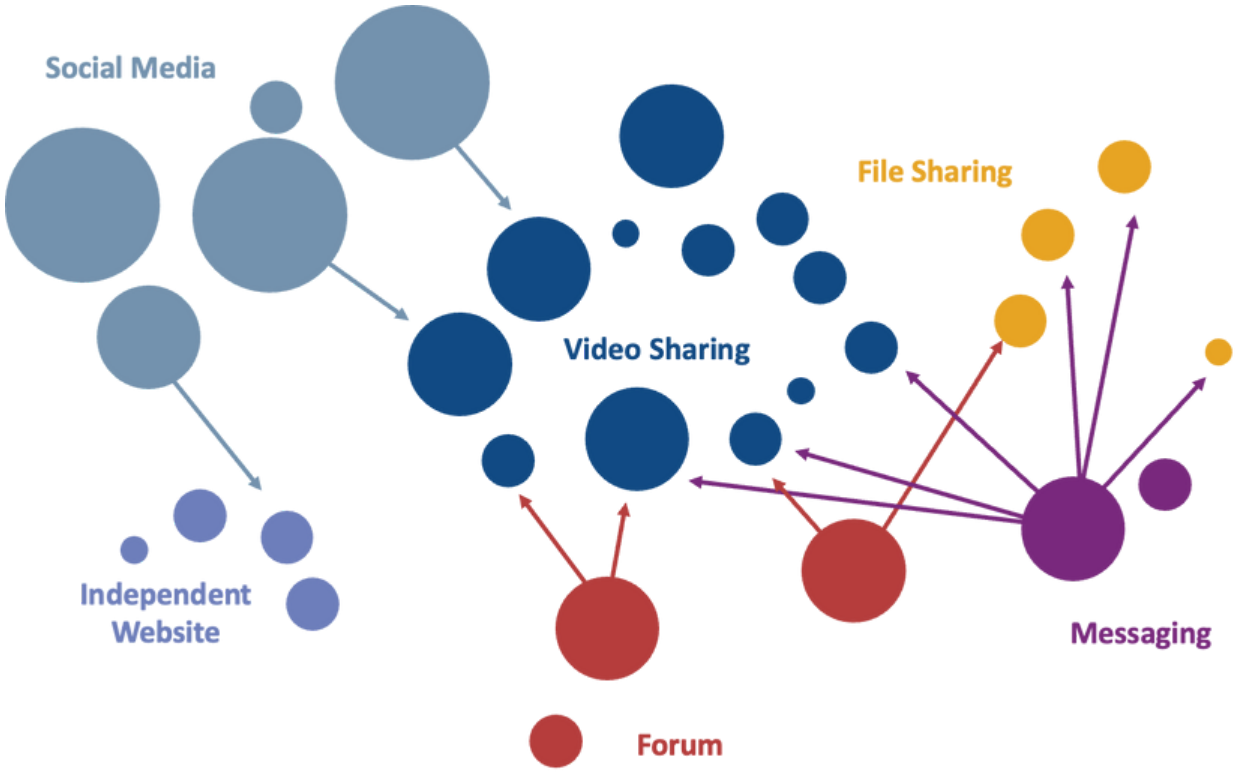

Figure 8: Network analysis of the spread of the Buffalo attacker's livestream, indicating platform size

The exploitation of Big Tech platforms varies between crisis events in terms of the platforms targeted and the scope and reach of material and reflects the variable moderation of crisis content. TVE entities and their supporters have targeted large tech platforms in the aftermath of an attack to share content due to the large audience reach and potential virality of content. Moderation of crisis content by Big Tech platforms is also highly variable. Content relating to Case Study #2 was highly discoverable on Big Tech platforms in the immediate aftermath of the attack, despite being produced by the attackers to amplify their message, and depicting scenes of graphic violence. Most of this content was not uploaded by supporters of the perpetrators, but by small, regional media outlets and independent journalists. We identified a large volume of content, most of which had been edited by users to add media logos, brandings, and watermarks. The use of content editing likely contributed to the longer-term availability of the attack footage as it was not identified automatically, and therefore required human identification and moderation.

CASE STUDY #2
UDAIPUR, RAJASTHAN, INDIA

On 28 June 2022, two people committed an attack against a Hindu shopkeeper in Udaipur, Rajasthan, India. The attack perpetrators released three separate videos concerning the attack: one filmed as a threat before the attack; one depicting the attack; and one filmed after the attack, claiming responsibility. It is unclear which platforms the attack perpetrators used to originally circulate the content. The three videos spread prominently on ***Twitter*** and were also highly posted on regional social media platforms such as ***Koo***.

While the use of file sharing platforms for regular propaganda output by far-right TVE entities has been experimental and sporadic, we have identified an increased reliance on these platforms in the immediate aftermath of crisis events. As demonstrated in Case Study #3, far-right TVE attack perpetrators and their supporter networks increasingly rely on small file sharing platforms due to anticipated moderation by larger social media and messaging platforms. In exploiting small file sharing platforms, these actors are highly likely attempting to ensure the longevity of content online by targeting a diverse range of platforms with limited moderation abilities. It is likely that future attack perpetrators will learn from what has worked in past attacks and will adopt a multi-platform dissemination strategy to counteract expected content moderation. It is probable that far-right TVE entities and networks have observed the propaganda dissemination strategies of Islamist TVE entities, and both mimicked their behaviour and learned what tactics are effective.

CASE STUDY #3
BRATISLAVA, SLOVAKIA

On 12 October 2022, a far-right terrorist killed two people at an LGBTQIA+ friendly bar in Bratislava, Slovakia. The perpetrator released a manifesto online prior to mounting the attack. The manifesto was initially hosted on six file sharing platforms, ***Filemail***, ***Zippyshare***, ***Files.safe***, ***Delegao***, ***Mediafire***, and ***Anonfiles***, which the attack perpetrator linked on their ***Twitter*** profile. The attack perpetrator also interacted with users on ***4chan***'s white nationalist /pol/ board after the attack, before committing suicide.

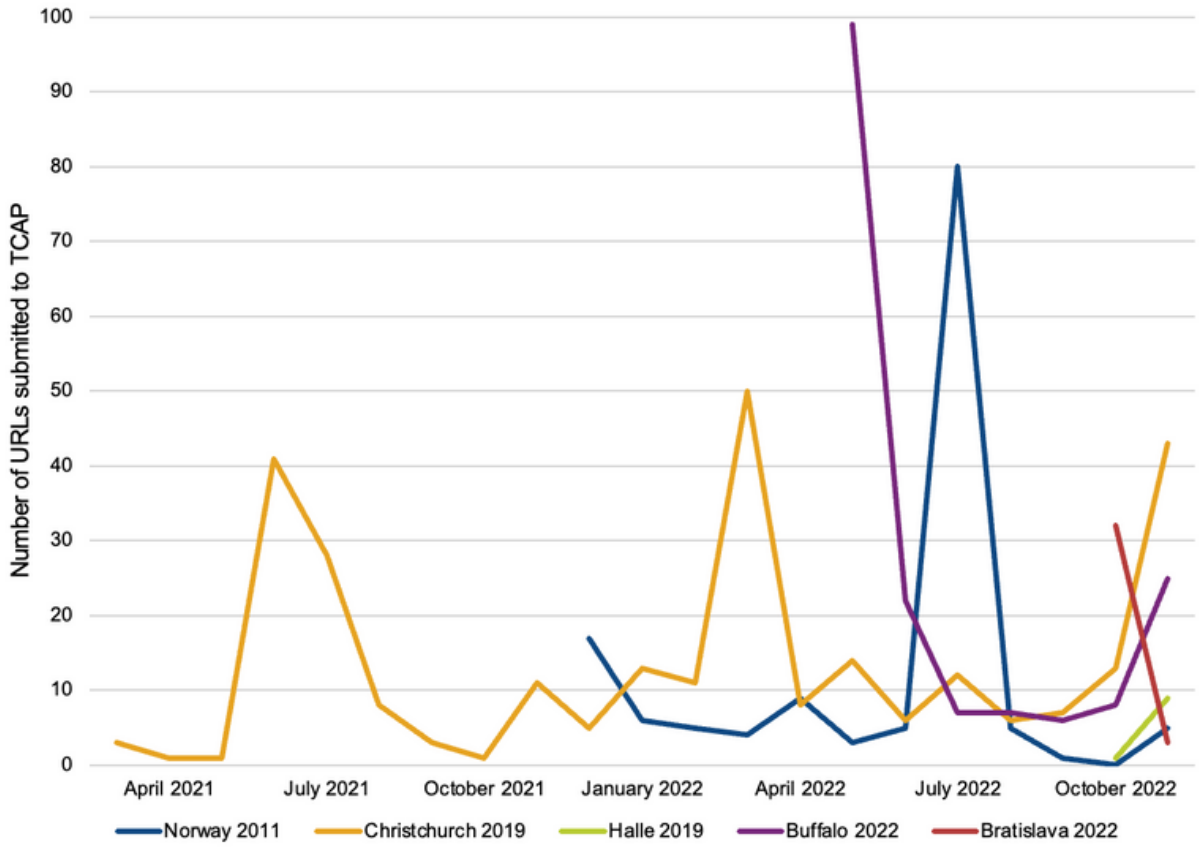

Figure 9: URLs submitted to TCAP containing attacker-produced content

GLOBAL EVENTS

The Russian Invasion of Ukraine

The Russian invasion of Ukraine galvanised support for far-right violent extremist pro-Kremlin networks, which will almost certainly grow as the war goes on. Coordinated disruption of these networks will be better enabled by terrorist designations and further sanctions.

The Russian invasion of Ukraine has had a significant impact on the online threat landscape, particularly among far-right violent extremist networks. The purported "denazification" of Ukraine as claimed by the Russian Federation galvanised some far-right violent extremist users and confused others. A significant proportion of these channels, and pro-Kremlin networks in general, frequently espoused long-standing far-right violent extremist rhetoric, such as antisemitism. Some networks, however, were less confident of how to interpret Russia's invasion, seeing it instead as a hindrance to white unity, or were confused about who to support. This split is driven by multiple factors, including pro-Ukraine networks seeing Ukraine as a heroic underdog in a fight to defend 'white Europe' from 'non-white' Russian forces; Western pro-Russia far-right extremist networks supporting the Russian Federation against NATO, which they perceive as a common enemy characterised by 'degenerate' liberal democracy; and negative perceptions of Volodomyr Zelenskyy, driven by antisemitism. Further points of division and confusion among far-right TVE networks is the perception that Russia is neo-Bolshevik, and the notion that two predominantly white nations are fighting wastefully instead of uniting against their common enemies in 'non-white' nations.

Some networks and extremist commentators of the conflict, most notably on Telegram, have grown their online presence and audience since the invasion. Subscribers to channels and pages affiliated with the Russian private military contractor (PMC) organisation "Wagner Group", for example, have swelled in membership since the invasion. A prominent pro-Wagner Group ***Telegram*** channel

maintained around 70,000 subscribers in July 2022; at the time of writing, the channel had over 260,000 subscribers. We also observed similarly dramatic increases in audience sizes for two extreme far-right “news” channels covering the war.

We have identified incitement to war crimes in multiple networks and channels, and in some cases, visual evidence of these crimes was provided as propaganda in support of this incitement.[4] In addition to these egregious cases, there has been a lack of consistency in tech sector responses, with no identifiable consensus on how to moderate extreme pro-Kremlin networks.

Despite financial sanctions against some groups active in Ukraine, such as the neo-Nazi DShRG Rusich paramilitary organisation, many of the unit’s members and backers maintain profiles on multiple tech platforms – including Big Tech - and routinely use those spaces to enable crowdfunding attempts for equipment and supplies. Almost all instances of the crowdfunding efforts we identified contained cryptocurrency addresses, likely to avoid sanctions and enhance operational security measures.

As the war in Ukraine continues, far-right violent extremist pro-Kremlin networks will almost certainly continue to grow their online presence, particularly when effective and co-ordinated disruption is delayed.

[4] “Russian mercenaries in Ukraine linked to far-right extremists” March 2022. Available at: https://www.theguardian.com/world/2022/mar/20/russian-mercenaries-in-ukraine-linked-to-far-right-extremists

ABOUT TECH AGAINST TERRORISM

Tech Against Terrorism supports technology companies to counter the terrorist use of the internet. It is an independent public-private partnership initiated by the UN Security Council.

Our research shows that terrorist groups - both jihadist and far-right terrorists - consistently exploit smaller tech platforms when disseminating propaganda. At Tech Against Terrorism, our mission is to support smaller tech companies in tackling this threat whilst respecting human rights and to provide companies with practical tools to facilitate this process.

As a public-private partnership, the initiative works with the United Nations Counter Terrorism Executive Directorate (UN CTED) and has been supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of Spain, Switzerland, the Republic of Korea, and Canada.

contact@techagainstterrorism.org