EXAMINING ONLINE MIGRATION TO TERRORIST AND VIOLENT EXTREMIST-OWNED DOMAINS

TECH AGAINST TERRORISM
ARTHUR BRADLEY and DEEBA SHADNIA

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

tech against terrorism

2000 Pennsylvania Avenue NW
Washington, D.C. 20006
https://www.extremism.gwu.edu

About Tech Against Terrorism

Tech Against Terrorism (TAT) is the world's leading organization in providing not-for-profit support for global tech companies in disrupting terrorist use of their platforms. TAT was launched in 2017 with support from UN CTED to support the global tech sector in tackling terrorist use of the internet whilst respecting human rights, and has been recognized by the UN Security Council. TAT's support mechanisms for the tech industry span across bespoke training, mentorship, capacity-building, threat reports, software and product development, and operational support. Since its inception in 2017, TAT has engaged with more than 400 global tech platforms. TAT also works closely with the Global Internet Forum to Counter Terrorism (GIFCT), and has to date received government funding from Spain, Switzerland, Republic of Korea, Canada, and the United Kingdom (Home Office).

TAT's open-source intelligence (OSINT) team monitors terrorist activity across online platforms, and analyses terrorist content for flagging to tech platforms. In 2021, TAT's OSINT team facilitated the removal of more than 700+ pieces of terrorist content via targeted reporting to tech platforms. The TAT OSINT team also analyses and verifies content included in the Terrorist Content Analytics Platform (TCAP). Launched in 2020, the TCAP is assembling the world's largest database of verified terrorist content collected in real-time from verified terrorist channels on messaging platforms and apps. The TCAP automates the detection and analysis of verified terrorist content on smaller internet platforms, and alerts tech companies to support improved moderation of terrorist content online. To date (June 2022), the TCAP has alerted almost 18,000 URLs containing terrorist content to 70 platforms.

About the Program on Extremism

The Program on Extremism at George Washington University provides analysis on issues related to violent and nonviolent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public. The views and conclusions contained in this document are those of the authors alone and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Program on Extremism or George Washington University. The details contained in the court documents are allegations. Defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

Table of Contents

Introduction

This paper analyzes the use of terrorist and violent extremist (TVE) operated websites and platforms on the Domain Name System (DNS), as part of a multi-platform approach within terrorist exploitation of the internet. In particular, this paper situates the resurgent exploitation of internet infrastructure within the context of improved content moderation by tech companies, and a growing trend of terrorist and violent extremist dispersion across more niche online platforms, where the audience reach of these actors is limited.

This paper considers how terrorist and violent extremist actors could respond to industry improvements in content removal policies on websites and self-operated platforms on the surface web, including potential migration to decentralized web hosting technologies and the dark web. It argues that counter-terrorism practitioners, researchers, governments, and the tech sector should pay more attention to terrorist and violent extremist operated websites and platforms, after several years of focusing on the exploitation of social media and messaging platforms used by the wider general public.

Methodology and Definitions

When analyzing TVE-owned domains, distinguishing between websites and platforms is important because they serve different functions in the online TVE ecosystem. Specifically, the nature of the threat they pose can differ. TVE-operated websites primarily provide a unidirectional content or information flow, whereas platforms act as spaces or tools through which users can build a community, interact, or utilize for the sharing of user-generated content.

The use of the domain-name system by TVE actors is not a new phenomenon; it dates back to the early days of the internet. In a context of improving online counter-terrorism policy and implementation by tech platforms, the creation and operation of domains is being used by TVE actors to evade censorship and maintain a stable and discoverable online presence.

Justifications

Before this paper critically assesses how TVE-owned domains play a role in the wider online TVE ecosystem, it first outlines what exactly constitutes a domain, beginning first with the Domain Name System (DNS).

Cloudflare, a leading web infrastructure and website security company, gives the following definition for a DNS:

> *"The Domain Name System (DNS) is **the phonebook of the Internet**. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources."*[1]

This paper focuses on two types of domains – namely, websites and platforms. While there are many technical definitions for what constitutes a website, this paper categorizes websites as online spaces that do not facilitate user-generated content or interactions. Websites are a static collection of pages that simply provide a one-way stream of interaction between the site and the user.

In this context, a potential example of a TVE-operated website would be a domain managed by Islamic State supporters that routinely publishes the group's official propaganda content in 15 languages.

[1] "What is DNS? | How DNS Works" n.d. Cloudflare. Accessed April 7, 2022. https://www.cloudflare.com/en-gb/learning/dns/what-is dns/#:~:text=The%20Domain%20Name%20System%20(DNS,browsers%20can%20load%20Internet%20resources.

Under our definition, this would constitute a website because it does not allow for visitors to the site to interact with the space in any way, other than simply browsing through the pages.

This paper defines platforms as dynamic online spaces that allow for user-generated content or interactions. These can include social media, video streaming, and messaging platforms. Unlike static websites platforms are interactive, allowing for user-generated content and communication to be posted and shared. An example of a TVE-operated platform would be Fascist Forge, a now-defunct forum that was active between 2018 and 2019. The platform was described by its founder as aiming to help fascists "communicate among themselves without the worry of censorship or attacks by the enemy in addition to a plethora of online resources."[2] The platform was taken down by its domain registrar in February 2019.[3]

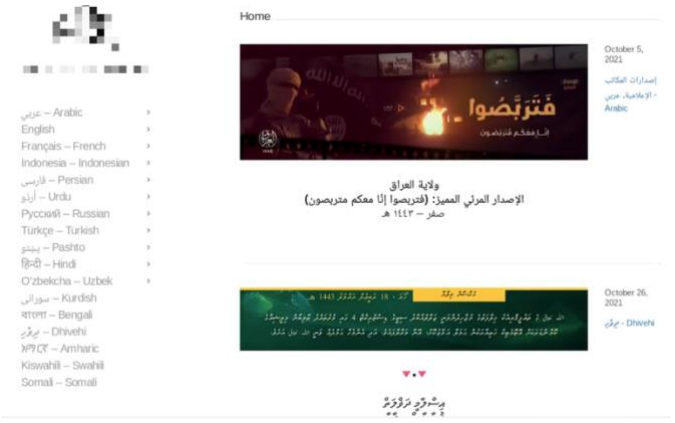

Figure 1. A pro-IS website that hosts propaganda in multiple languages, February 2022.

Our research has identified tens of platforms that we assess to be likely to be run by terrorists, violent extremists, or their sympathizers from both the violent far-right and violent Islamists. Over the past year, we have also collected a dataset of more than 200 domains that are likely TVE-owned, relating to both platforms and websites. We included these on the basis of an assessment, which takes into consideration factors including content hosted on the site, endorsements, or promotion by wider online TVE networks, and a lack of content moderation of illegal content by the site's administrators.[4]

Limitations

Investigating and verifying TVE-owned domains is not without its limitations. It is often difficult to verify the identity of an owner of a domain with absolute certainty. In almost all cases, suspected TVE website owners utilize domain name privacy, meaning their details are not included in the domain's records. This is a straightforward service offered by most domain registrars in which the domain owner's details are not included in public records. It is also common for websites' host and IP address

[2] Mack Lamoureux and Ben Makuch, "Online Neo-Nazis are increasingly embracing terror tactics", *Vice,* January 28, 2019, https://www.vice.com/en/article/8xynq4/online-neo-nazis-are-increasingly-embracing-terror-tactics.
[3] Mack Lamoureux, "Fascist Forge, the online neo-Nazi recruitment forum, is down", *Vice,* February 15, 2019, https://www.vice.com/en/article/43zn8j/fascist-forge-the-online-neo-nazi-recruitment-forum-is-down.
[4] "The Threat of Terrorist and Violent Extremist-Operated Websites", *Tech Against Terrorism,* January 2022, https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf.

to be hidden from domain records via the use of services such as a Content Delivery Network (CDN), the most common of which is Cloudflare.

Another obstacle in understanding TVE use of domains is the difficulty in ascertaining the ideological beliefs of a given website or platform's administrator. The growing selection of smaller alternative platforms listed on the domain name system in recent years includes a number of platforms that host high volumes of TVE content, particularly relating to violent far-right extremism. This is often due to a lack of capacity by the company to effectively moderate their platform, but it can also be due to a lack of willingness or even sympathies with extremist viewpoints. This can lead to challenges in classifying whether a lack of moderation on a given platform is due to the owner's views on freedom of speech, or because it is run by actors that are sympathetic to terrorism or violent extremism.[5]

These difficulties are compounded in the case of some websites operated by TVE actors that deliberately misrepresent themselves, or otherwise hide their group or ideological affiliation. Al-Shabaab, for example, operates a network of affiliated media organizations with affiliated domains, many of which present themselves as independent and legitimate news outlets. These websites do, however, often base their reporting on official Al-Shabaab propaganda, and some of these sites operate as unofficial mouthpieces for the group.[6] It has also become common for websites, channel or social media pages administered by far-right extremists to include "disclaimers", in which they deny any affiliation with violence or extremist beliefs. The extreme far-right Daily Stormer website, for example, includes a message on its homepage stating that its administrators are "opposed to violence" adding that they "seek revolution through the education of the masses."[7]

Before discussing the issue of TVE-owned domains, this paper provides an overview of how terrorists are using the internet across platforms, including social media, messaging apps, file-sharing services, and video-sharing platforms, and how these platforms are used for communication and the dissemination of TVE material.

[5] Joe Mulhall, "I'll be back: The Rise of Far-right Alt-Tech", *Hope Not Hate,* March 17, 2022, https://hopenothate.org.uk/2022/03/17/ill-be-back-the-rise-of-far-right-alt-tech/.

[6] Evan Matos, "Al-Shaabab: Information Operations Strategy Overview", *Small Wars Journal*, August 29, 2019, https://smallwarsjournal.com/jrnl/art/al-shabaab-information-operations-strategy-overview; "Trends in Terrorist and Violent Extremist Use of the Internet | Q1-Q2 2021", *Tech Against Terrorism,* July 30, 2021, https://www.techagainstterrorism.org/2021/07/30/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/.

[7] "Daily Stormer," Daily Stormer, accessed April 28, 2022, https://stormer-daily.rw/.

Overview: How Terrorists Use the Internet

Since the introduction of the first generation of the internet, TVE actors have made use of online spaces for a host of operational and strategic purposes. These have included spreading propaganda content, recruiting new members, and communicating internally. TVE actors from across the ideological spectrum occupy complex and wide-reaching online ecosystems. A 2019 study by Ali Fisher, Nico Prucha and Emily Winterbotham identifies three main uses of platforms by terrorists online. These are categorized in terms of beacons, content stores and aggregators.[8] To this, we add a fourth category: circumventors.

Beacons are platforms used by TVE actors to project their content to the widest audience possible, acting as centrally located lighthouses or signposts to where the content can be found. Examples of a beacon could be a channel on a messaging app such as Telegram or Element Messenger. Content stores refer to platforms on which TVE content is hosted, including text and audio files, as well as audiovisual material. URLs posted on beacon platforms often link to such content stores. Examples of content stores include file-sharing services such as Dropbox or Files.fm. Aggregators are sites or platforms that are used by TVE actors to gather together links to content located elsewhere online; Justpaste.it, for example, has been used for this purpose by TVE actors.[9] Finally, circumventors are online tools or platforms that enable TVE actors to evade detection or content moderation, such as the use of Virtual Private Networks (VPNs), which hide an internet users' IP address and enables them to access content that may have been blocked in a given region. Another example is archiving services, which can be used by TVE actors to create back-ups for webpages before they are taken down.[10]

[8] Ali Fisher, Nico Prucha and Emily Winterbotham, 'Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability,' 2019, *Global Research Network on Terrorism and Technology*, Paper No. 6, https://static.rusi.org/20190716_grntt_paper_06.pdf.

[9] Gabriel Weimann and Asia Vellante, "The Dead Drops of Online Terrorism", *Perspectives on Terrorism,* Vol. 15, No. 4, (August 2021), pp. 39-53, https://www.jstor.org/stable/pdf/27044234.pdf.

[10] Tech Against Terrorism, "Terrorist use of the internet", *Counter Terror Business*, December 23, 2020, https://counterterrorbusiness.com/features/terrorist-use-internet.

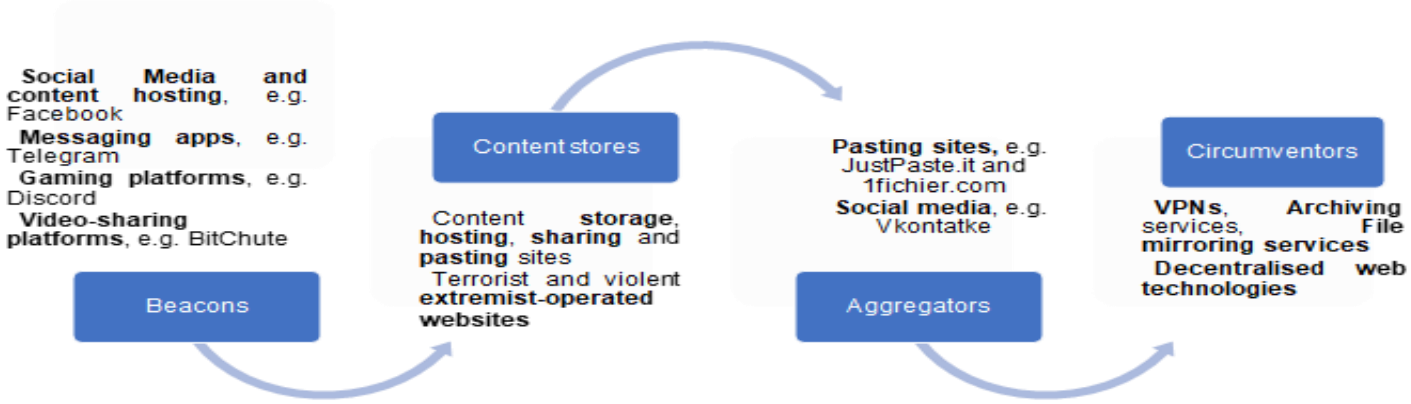

Figure 2. Eco-system of online platforms used by terrorists and violent extremists in a multiplatform approach, with examples.

In general, TVE actors – particularly violent Islamist organizations, such as al-Qaeda and Islamic State and their supporter networks – pursue a multiplatform approach to ensure both the rapid sharing of content and a resilient online presence. For example, online networks affiliated with both Islamic State and Al-Qaeda have long published multimedia releases on several file- and video- sharing platforms simultaneously, before sharing the links to the content in aggregated form on their beacon channels.[11] This approach helps TVE actors to be more resilient to moderation efforts and takedown attempts.

TVE actors' ability to reach a wide audience is inhibited on more niche platforms, and they do still face deplatforming in these spaces. TVE actors are continually forced to be highly agile and creative in their use of the internet, to ensure maximum reach of their propaganda and the ongoing availability of their content online. They therefore usually operate through a multiplatform approach, in which they utilize several online platforms simultaneously to maintain an online presence that is as stable and wide-reaching as possible.

Violent far-right actors online also engage in a multiplatform approach in their use of the internet, although rarely do they publish content via long lists of outlinks like violent Islamist actors do. Instead, violent far-right actors mostly congregate on platforms where they believe their content is less likely to be removed. These platforms include alt-tech "free speech" based social media and video-sharing sites, archiving services, encrypted messaging apps, and email services.[12]

[11] Nico Prucha, "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram", *Perspectives on Terrorism* 10 No. 6 (2016): 48-58.
[12] Maura Conway, Ryan Scrivens, Logan Macnair, "Right-wing extremists' persistent online presence: history and contemporary trends", *International Centre for Counter-Terrorism,* October 2019, https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

Violent far-right groups, entities, or influencers will often promote and maintain accounts across several platforms simultaneously, likely to reach as wide an audience as possible. Furthermore, the violent far-right are also building their own platforms hosted with their own domains. This is leading to increasingly blurred lines between "alt-tech" and TVE-operated websites or platforms, raising questions around what the threshold should be for action at the domain level.

Despite ongoing content moderation efforts by mainstream tech platforms, TVE content still appears on these online spaces. However, in recent years as more resources and technology have been applied to mainstream content moderation efforts, TVE actors have been forced to become increasingly creative in their evasion tactics to avoid moderation.

While the improvements have by no means made all content moderation on mainstream online spaces perfect, the improvements have broadly forced TVE actors to congregate on a greater number of smaller, less regulated alternatives. In these smaller online spaces, TVE actors are able to operate with a greater degree of impunity, due to either a lack of capacity or willingness by such tech platforms to moderate content in a timely and effective manner.[13]

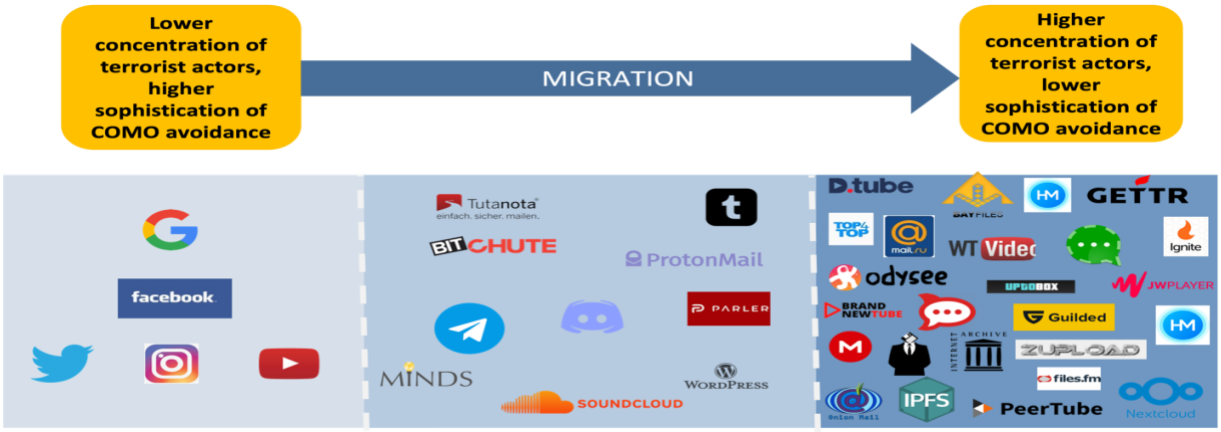

Figure 3. A visual depiction of terrorist migration from large to smaller tech platforms.

This online status quo is one in which TVE actors are continually forced to engage in content moderation evasion tactics or operate on smaller platforms where audience reach is limited. This is likely to be encouraging the move by some towards supplementing their online presence by operating their own platforms or websites.

[13] Mulhall, March 2022.

Terrorist and Violent Extremist-Owned Domains

TVE-owned domains play an increasingly important role in the wider ecosystem of online terrorist exploitation. Terrorist owned domains are providing TVE organizations and their supporters with relatively stable, easily discoverable pages on the surface web, often serving to mitigate the negative effects of their forced migration onto smaller or lesser-known platforms where their ability to reach a broad audience is likely relatively low. Tech Against Terrorism is currently tracking more than 200 domains suspected to be owned by terrorist actors, based on open-source intelligence (OSINT) investigations.[14] This number is likely to be only a fraction of the total number of TVE websites globally.

Content on these domains facilitates multiple activities including recruitment, fundraising, disseminating and viewing multimedia content, and communication. They also can serve as directories of links for TVE pages or groups elsewhere on the internet, acting as gateways or checkpoints for access into the more niche online spaces that may otherwise be more difficult to find.[15]

Terrorist-operated websites present a variety of benefits and disadvantages to TVE actors attempting to exploit the internet to further their cause, summarized in the table on the next page:

[14] *Tech Against Terrorism*, "The Threat of Terrorist and Violent Extremist-Operated Websites"
[15] *Ibid.*

Benefits	Disadvantages
● Publicly available, often indexed by search engines ● Give TVE actors the ability to curate content with branded aesthetics, creating veneer of professionalism ● Often little or no need for content sanitization or automated content moderation avoidance tactics ● Often offers more surface web stability than on platforms managed by large tech companies ● Threshold for content removal by infrastructure providers is often higher than tech companies ● Less consensus about provider responsibilities among infrastructure companies than social media and messaging apps, providing opportunities for terrorists to exploit loopholes ● Registrant identity can be protected and made private; some providers do not require any personally identifiable information to register	● Tend to be accessed only by individuals who either already know the domain or who come across it whilst actively seeking out TVE material ● Difficult to reach audience outside of supporter networks or those seeking out the material ● Requires some technical ability to administer and run

Explaining Migration to TVE-Owned Domains

Although the exploitation of the domain name system by TVE actors is an issue that has persisted since the early days of the internet, its evolving use in recent years can be linked to a number of contributing factors. We divide these here into "push" and "pull" factors.

By push factors, this paper refers to trends or incidents that dissuade TVE actors from attempting to operate on platforms run by legitimate tech companies, such as Twitter, YouTube, Telegram, or Facebook. "Pull factors" in this context refers to the characteristics of website or platform creation that are attractive to TVE actors.

Push Factors

The primary focus in public policy debates around countering TVE use of the internet in the past few years has been on social media and messaging platforms. To an extent, this makes sense: terrorist content on popular social networking, video-sharing, and messaging platforms has the potential to reach a significant audience, including the wider general public.

Terrorists still operate on these larger tech platforms,[16] but broad improvements in the enforcement of platform counter-terrorism policies mean that hostile actors are often forced to evade moderation. These can vary in sophistication, but terrorists increasingly utilize methods such as the redaction of incriminating keywords and imagery from content, the creation of multiple throwaway accounts, and shifting to the use of private spaces instead of public ones, in order to remain active on a given platform. From a terrorists' perspective, being forced to resort to complex evasion tactics is undesirable: it makes it more difficult for their content to be found by their supporters and prospective recruits, particularly when their core channels undergo frequent removal.

Many TVE actors also deliberately avoid the use of certain larger tech platforms for ideological reasons. This particularly relates to violent far-right extremists, who perceive the content moderation practices of mainstream tech platforms such as Facebook, Instagram, and YouTube as tantamount to censorship. This perception is often heightened during real-world incidents that trigger a new wave of platform moderation enforcement, such as the storming of the U.S. Capitol in January 2021. Multiple tech platforms responded to the incident by policy changes and enforcement, which contributed to platform migration among significant numbers of far-right violent extremists from big tech platforms to smaller alternatives.[17] Traffic to BitChute doubled in the week following January 6, for example, and there were significant increases in subscribers to several prominent extreme far-right Telegram channels over the same period.[18]

---

[16]Mark Scott, "Islamic extremists sidestep Facebook's content police", *Politico,* December 19, 2021, https://www.politico.eu/article/islamic-extremists-facebook-content-social-media-islamic-state-terrorism/; Jamie Grierson, "Neo-Nazi groups use Instagram to recruit young people, warns Hope Not Hate", *The Guardian,* March 22, 2021, https://www.theguardian.com/world/2021/mar/22/neo-nazi-groups-use-instagram-to-recruit-young-people-warns-hope-not-hate; Ruchira Sharma, "How terrorist recruiters are editing extremist content to evade moderation on Instagram and YouTube", *iNews,* November 17, 2021, https://inews.co.uk/news/terrorist-recruiters-extremist-content-evade-moderation-instagram-youtube-1304006.

[17] Jared Holt, "After the insurrection: How domestic extremists adapted and evolved after the January 6 US Capitol attack", *Atlantic Council,* January 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/after-the-insurrection-how-domestic-extremists-adapted-and-evolved-after-the-january-6-us-capitol-attack/.

[18]Mark Townsend, "How Trump supporters are radicalised by the far right", *The Guardian*, January 17, 2021, https://www.theguardian.com/technology/2021/jan/17/how-trump-supporters-are-radicalised-by-the-far-right; Joshua Zitser, "Following Trump's YouTube ban, it is feared his supporters are migrating to a "Wild West" of video-sharing,

By congregating on smaller platforms, terrorists are likely to find it more difficult to recruit new members and to spread their message. Many of the online spaces in which TVE actors now post their content are not indexed by mainstream search engines, such as in private Facebook groups, Telegram channels, or Discord chat servers. This creates a need among TVE actors to achieve an overt, discoverable presence on the surface web. Websites or platforms on the domain-name system serve this purpose.

Pull Factors

The creation of standalone platforms or websites on the domain name system is attractive to TVE actors for several reasons. First, publicly accessible websites will typically appear in mainstream search engine results, making them more easily discoverable than channels or groups on the deep web. Second, rarely do the administrators of TVE websites make any attempt to obscure the purpose or affiliation of their website; there appears to be little or no need for sophisticated content moderation avoidance tactics. Many of the websites in the dataset collected and analyzed by Tech Against Terrorism remained online for significant periods of time without disruption, despite high volumes of unredacted terrorist content being hosted there.[19]

Website and platform creation on the domain name system by TVE actors also affords these actors a wide choice of potential features and purposes, as well as the ability to curate their own content. The quality of the finished product is contingent on the technical capability of the group or actors in question, but many such websites or platforms can be created using intuitive tools or open-source software (OSS) like NextCloud or WordPress.

TVE-Owned Domains: Analysis of Case Studies

TVE actors utilize the domain name system for a wide variety of purposes. A large proportion of TVE owned domains monitored by Tech Against Terrorism are traditional static websites, meaning that they operate a unidirectional flow of content and are not built with features that enable user interaction or user-generated content.[20] These most often include multimedia content such as propaganda and other external messaging, as well as text-based material including blog posts and

mingling with far-right and neo-Nazi terror groups", *Business Insider,* January 17, 2021, https://www.businessinsider.com/trump-supporters-migrating-to-a-wild-west-of-youtube-alternatives-2021-1?r=US&IR=T

[19] *Tech Against Terrorism,* "The Threat of Terrorist and Violent Extremist-Operated Websites",

[20] *Ibid.*

official statements. They also often include information on further contact with the site's administrators, such as via end-to-end encrypted email addresses or users, channels, or groups on messaging apps such as Telegram.

However, TVE actors have also experimented with other domains that offer far more user interaction than traditional static websites. Below we outline five case studies of more innovative use cases for the domain name system by TVE actors. All of these are in our assessment a manifestation of adversarial shift, and an attempt by violent actors to ensure their content remains visible and discoverable on the surface web.

Aggregators

In a context of constant deplatforming and subversive content moderation avoidance tactics by TVE networks operating online, it has become increasingly difficult for supporters to locate and follow their content. Hostile actors have deliberately utilized websites to mitigate this problem, aggregating links to channels, groups, and pages that are either not indexed by search engines or whose names are intentionally unrelated to the content posted within them.

An example can be found in a website launched in early March 2022 and run by supporters of Islamic State (IS). The site, which required an email address to access, was promoted in pro-IS online networks as a resource to "help everyone who lost the channels of the supporters after the recent deletion campaigns." It contained more than 150 links to IS-affiliated accounts, groups and channels on Facebook, Twitter, Telegram, Hoop Messenger, Instagram, and Element Messenger, as well as a list of other TVE-owned domains affiliated with IS. The website also included interactive features, allowing its users to update and add to the links listed there.

Figure 4. A redacted screengrab of an IS-affiliated website that operates as an index of IS accounts, channels, and groups across multiple online platforms, March 2022.

Cloud Platforms

In 2021, Tech Against Terrorism identified the growing exploitation of open-source software by violent Islamist organizations including al-Qaeda and Islamic State (IS) to create "cloud platform" websites to store their content.[21] These are password-protected websites that enable terrorists to store content and share it across the internet via URLs. These cloud platforms are typically less liable to takedowns compared to platforms run and moderated by legitimate companies. Many of these contain an extensive and regularly updated archive of terrorist material. At the time of writing, Tech Against Terrorism had recorded six terrorist-operated cloud platform websites including ones likely affiliated with or run by Islamic State, al-Qaeda Central, al-Shabaab, and al-Qaeda in the Islamic Maghreb (AQIM). All of these platforms exploit open-source software developed by the Germany-based company NextCloud.

For example, in April 2021 a prominent IS-affiliated operational security group announced the creation of its own cloud storage platform. A poster promoting the platform, along with its own "secure messenger," had appeared in pro-IS channels elsewhere online, claiming that it had been developed "in light of recent developments in the media arena and the restriction of technology companies to [violent Islamist] content." It added that the group had therefore "resorted to developing solutions that provide a space for propagation between [Islamic State] supporters and the general Muslim community."

Figure 5. Screengrab of an IS-affiliated "cloud platform," featuring an extensive and downloadable archive of content.

[21] "Trends in terrorist and violent extremist use of the internet | Q1-Q2 2021", *Tech Against Terrorism*, July 30, 2021, https://www.techagainstterrorism.org/2021/07/30/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/.

The development of the platform was a response to an increased ability among smaller file-sharing platforms to remove their content efficiently and effectively. Publishing content on multiple platforms simultaneously does often increase the content's online lifespan: it remains available for as long as it takes the slowest platform to take it down.

However, smaller file sharing platforms are becoming increasingly efficient at removing this content, in part due to initiatives such as Tech Against Terrorism's Terrorist Content Analytics Platform (TCAP), which captures lists of outlinks in bulk and automatically alerts the respective companies to the presence of the content.[22] In the case of content on terrorist-owned domains, however, removal requests must be directed towards infrastructure companies, who do not always act based on content alone. Tech Against Terrorism facilitated the suspension of the IS-affiliated cloud platform in Spring 2021 via an abuse report to its domain registrar.

Terrorist-operated paste sites

TVE actors have also exploited the domain name system to host their own paste sites, which are platforms that enable users to upload and share text or images online. A paste site regularly exploited for propaganda sharing by IS networks, for example, was operational on the surface web at the time of writing. It bore similar aesthetics and features to legitimate paste sites like JustPaste.it, but content hosted there was almost exclusively IS propaganda. The site had no terms of service, nor indications of any attempts by its administrators at content moderation. Registration required neither an email address or phone number, and a message on the site encouraged users to donate to the project using Bitcoin. Very little information on the website was discernible on WHOIS records relating to the domain.

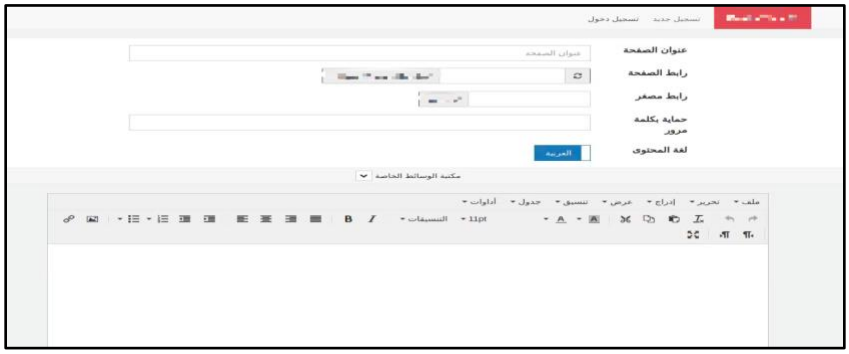

Figure 6. Content submission page on a suspected IS-linked paste site, March 2022.

[22] "Terrorist Content Analytics Platform," Terrorist Content Analytics Platform, accessed May 26, 2022, https://www.terrorismanalytics.org/.

The site featured a straightforward submission page, including the ability to add text, images and documents, a page title, and password protection. Once content is uploaded, the site generates a link for the content as it appears on the website, which can then be used to share the content across the internet. At the time of writing, it was being used daily by pro-IS networks to share the latest attack claims and multimedia content produced by IS central in aggregated form. A similar site likely operated by Al-Qaeda is used by the group and its official affiliates to aggregate links to copies of almost all its official multimedia releases across multiple small video and file-sharing platforms.

Terrorist-operated chat servers

A joint counter-terrorism operation in November 2019 between Europol and Telegram Messenger largely decimated violent Islamist networks on the platform following several years of relative stability.[23] The operation had the side-effect of scattering IS networks across multiple other alternative messaging apps and platforms including TamTam, Blockchain Messenger (BCM), Hoop Messenger, and Matrix.[24] Networks affiliated with Islamic State and Al-Qaeda have since returned to Telegram, but these channels are supplemented with a presence across multiple other messaging platforms, including dedicated servers with their own domain names.

In the case of Al-Qaeda, since late 2019 its primary and centralized platform for the dissemination of material from its official media outlets is on a chat server built with open-source Rocket Chat code. It requires an email address and password to access and contains more than 100 channels dedicated primarily to propaganda dissemination, as well as discussion groups and IT support channels. The platform's terms of service states that it is intended only for supporters of Al-Qaeda and its trusted supporter networks: "users uncovered as dogs of the Crusaders and Zionists, and apostates, and Rafidiah, and Kharawij by the administrators, [sic] will be immediately banned without warning." The server has remained available with infrequent outages since its launch in late 2019; it changed domains without explanation in November 2021. It was unclear whether the domain was disrupted by a third-party or the site's administrators deliberately changed it.

[23] "Europol and Telegram take on terrorist propaganda online", *Europol,* November 25, 2019, accessed 29 April 2022, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.
[24] Héni Nsaibia and Rida Lyammouri, "The Digital Transformations of Al-Qaeda and Islamic State in the Battle against online propaganda", *Global Network on Extremism & Technology,* May 19, 2021, https://gnet-research.org/2021/05/19/the-digital-transformations-of-al-qaeda-and-islamic-state-in-the-battle-against-online-propaganda/

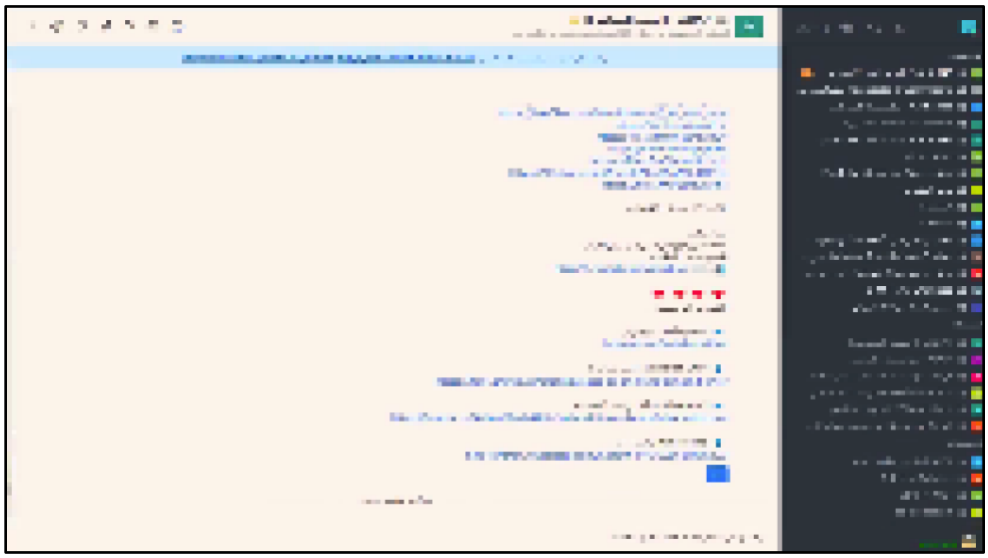

Figure 7. A pixelated screengrab of an al-Qaeda affiliated server built using Rocket Chat software. Channels are listed on the right of the image, content posted in a channel is visible on the left. Screengrab taken March 2022.

Audio-visual streaming platforms

Deplatforming from mainstream and alt-tech audiovisual streaming services is also leading some TVE actors to create and run their own alternatives. These platforms are typically aesthetically similar to others like YouTube and BitChute, but are operated and administered by TVE actors. They typically either have very lenient terms of service that permit content produced by TVE actors, or none at all. All are founded on expansive definitions of "freedom of speech."

The extreme far-right Nordic Resistance Movement (NRM), for example, operates its own video-sharing platform on the surface web. At the time of writing the platform hosted 2,220 videos, totaling more than 1,000 gigabytes of content. Almost all of it was official propaganda produced by the NRM. It had a total of more than 343,000 video views, according to data displayed on the "about" page of the site.

The site is built using decentralized, open-source software developed by a French company, which enables users to create and administer their own websites. The NRM publicized the site frequently on its social media channels between 2020 and 2022, including in the wake of bans from certain platforms. In February 2021, for example, audio streaming platform Spreaker suspended accounts affiliated with the NRM's podcast, Nordic Frontier. Following the ban, the NRM said it was moving all future episodes to its own website. It encouraged subscribers and supporters to spread the word "so that we can make the migration as fast and successful as possible."

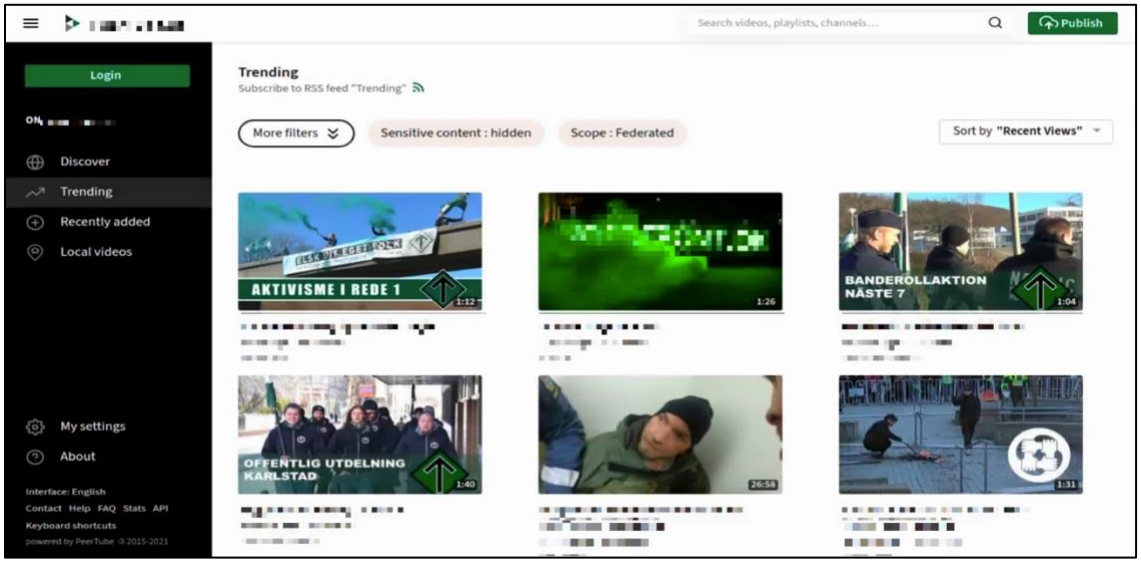

Figure 8. Screenshot of a video-sharing platform likely run by the far-right extremist Nordic Resistance Movement (NRM).

Assessing Future Trends in TVE-Owned Domains

An increase in the frequency of suspensions of TVE-owned domains is highly likely to lead to adversarial shift in overall trends of TVE use of the internet. In this section, we consider tactics and technologies that are likely to be used in a more widespread manner for the hosting of TVE websites in the medium to long term. This includes the Tor network or "dark web," and decentralized hosting technologies.

Increased migration to the dark web

There have been multiple instances of TVE domains on the dark web, including at the time of writing. However, to date there has been little requirement for TVE actors online to migrate to the dark web *en masse*. This is likely because of the vast selection of platforms and websites on the surface and deep web, where TVE actors have been able to operate in recent years with relative stability, security, and audience reach. This is despite content moderation efforts forcing TVE actors to engage in complex online avoidance tactics and platform migrations.

Nevertheless, surface and deep web platforms are also typically easier to use than the dark web, which requires a specialist browser, and internet users hoping to access dark web websites must have prior knowledge of their unintuitive domain names to access them. This is because dark web domains are not indexed by search engines like Google, Bing, and DuckDuckGo.

Based on our research, the most common function of TVE-operated darkweb sites is to act as stable back-ups for mirror websites that already exist (or existed) on the surface web. These hidden versions serve the function of preserving and archiving content hosted on the surface web, likely in anticipation of the suspension of the public web version. In several instances we have seen administrators of TVE websites publicly advertise their dark web domains in this way, including sites such as the neo-Nazi website the Daily Stormer, a multilingual pro-IS propaganda entity, and a pro-IS website that acts as an aggregator of links to other IS-affiliated domains across the internet.

Figure 9. A darkweb site used by a neo-Nazi operational security advisory group, May 2021.

Increased exploitation of Dweb to host TOWs

The decentralized web (Dweb), which differs from the traditional worldwide web in that it is based on blockchain technology and no longer relies on large intermediaries or services to function, has been exploited by TVE actors since at least 2017. This includes ZeroNet, file sharing services such as the Interplanetary File System (IPFS) and Skynet, as well as multiple Dweb tech platforms including Element, Odysee, Peertube, and D.Tube.[25] More recently, however, there have been an increasing number of examples of TVE exploitation of the Dweb to host websites accessible on a conventional browser. Some of these have been accessible via gateways for the Interplanetary File System (IPFS), a peer-to-peer hypermedia protocol that enables content hosting and can be accessed via URLs on a conventional HTTP browser.[26]

There has also been experimentation by TVE actors of Dweb-based domain name systems such as "Unstoppable Domains," which replace long and unintuitive domain addresses with memorable and easily readable domain names. For example, in December 2020, a prominent pro-IS propaganda archive website that had been subject to frequent domain suspensions on the surface web promoted a secondary domain that it said "cannot be stopped." By using the Unstoppable Domains extension, a user could enter the short domain and be redirected to a landing page on the Dweb, where the latest

[25] Lorand Bodo, "Decentralised Terrorism: The Next big step for the so-called Islamic State (IS)?", *Vox Pol,* December 12, 2018, https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is/.
[26] "IPFS Powers the Distributed Web," accessed April 26, 2022, https://ipfs.io/.

link to the propaganda archive could be found. Although the page was still live at the time of writing, the link listed there no longer directed to an active website, and had not been updated since January 2021.

As pressure on traditional, centrally hosted TVE websites increases, and the usability and popularity of decentralized web hosting services further improves, terrorists are likely to look to migrate their websites to Dweb technology on a larger scale. This is likely to be driven further by an ongoing perception among TVE actors that content supported by Dweb technologies cannot be removed, despite the ability of Dweb providers to make content inaccessible by blocking the URLs that direct to it.

Conclusion

TVE-operated websites and platforms are an understudied issue in the wider landscape of their exploitation of the internet. Research and public policy discussions often focus on issues relating to large social media and messaging platforms, neglecting to effectively consider how the ongoing resilience of traditional websites operated by TVE actors are undermining global online counter-terrorism efforts.

This paper serves to highlight key reasons for terrorist migration from social media and messaging platforms to websites and self-administered platforms on the domain name system, framing it as a form of adversarial shift in the face of improving counter-terrorism efforts by big tech companies. The websites and platforms are providing TVE actors with relatively stable and easily accessible spaces on the surface web with which to propagate their message, host propaganda, and recruit.

More research should be done into the issue of TVE-operated websites and platforms, and their role in the wider online ecosystem inhabited by TVE actors. This research should in particular assess the risks associated with the adverse shifts in behavior that the removal of these sites could potentially cause.

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

tech
against
terrorism