THE THREAT OF TERRORIST AND VIOLENT EXTREMIST-OPERATED WEBSITES

JANUARY 2022

tech against terrorism

TABLE OF CONTENTS

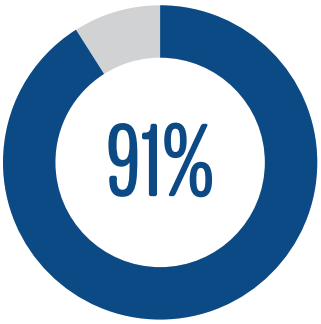
1. EXECUTIVE SUMMARY

Since January 2021, Tech Against Terrorism has identified **198 websites** that we assess to be operated by terrorist actors, or by violent extremists that pose a credible and urgent threat to society.

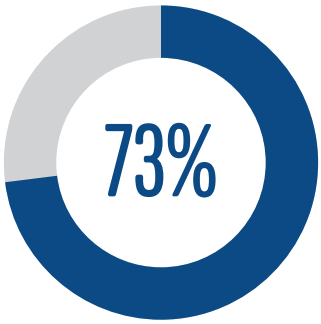
79 of these sites relate to violent Sunni Islamist actors, 18 to violent Shia Islamist actors and 101 linked to the violent far-right.

In 2021 **we facilitated the removal of 16** of these sites that linked to accelerationist neo-Nazi actors, the Taliban and the Islamic State.

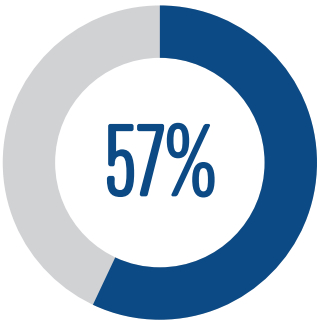
From a representative sample of 33 terrorist- and violent extremist-operated websites, we found that:



displayed audio/ visual propaganda



had an archive of historic content



included a communication feature

The total average monthly visits to these 33 sites is 1.54 million.

- Tech Against Terrorism has been tracking the widespread use of terrorist and violent extremist operated websites (T/VEOWs) from across the ideological spectrum since early January 2020. **We assess that T/VEOWs pose one of the most significant threats to global efforts in tackling terrorist use of the internet by governments, the tech sector, law enforcement and NGOs.**

- Our database tracking the use of these sites includes **198 unique domains** relating to actors such as al-Qaeda, Islamic State, Atomwaffen Division, Combat 18, Order of the Nine Angles, Hezbollah and the Taliban. The database includes sites that promote violent extremist ideologies such as neo-Nazism, violent insurrectionary accelerationism, violent far-left actors and the Incel ideology.

- T/VEOWs are primarily used to disseminate and archive propaganda material, as well as to recruit and communicate internally. These websites exist on the surface web and are often easily discoverable through search engines. This discoverability undermines the significant improvements being made across the tech industry in disrupting online terrorist propaganda campaigns and activity.

- The reliance on T/VEOWs has grown in recent years due to several factors. Broad improvements in the detection and removal of terrorist content on mainstream social media platforms has pushed such actors onto smaller online spaces. T/VE actors have consequently grown increasingly creative in exploiting the internet, and many have once again returned to relying on websites for their online activities.

- Most government-led initiatives on countering terrorist use of the internet is still largely concentrated on mainstream social media platforms. The continued existence of T/VEOWs risks undermining such efforts and making such initiatives largely redundant. A lack of global consensus around who should be responsible for disrupting or removing such sites has hindered the effective management of the threat to date.

- There are few international mechanisms in place to support the tech sector – specifically internet service providers – to counter the threat of T/VEOWs. Tech Against Terrorism recommends improved collaboration between governments and website infrastructure companies, without compromising human rights principles and fundamental freedoms, in identifying and responding to the threat of T/VEOWs.

2. RECOMMENDATIONS

Whilst much progress has been made to tackle terrorist use of the internet, T/VEOWs have – based on our assessment of activity in the online counterterrorism space – in recent years arguably been a blind spot for policymakers, practitioners, and researchers. In our view, this is potentially dangerous as it risks undermining positive action taken elsewhere across the tech eco-system to disrupt online terrorist activity. Below, we provide recommendations for governments, infrastructure companies, researchers, civil society and multistakeholder forums to mitigate the threat stemming from T/VEOWs.

A) Recommendations for governments

1. Prioritise T/VEOWs in policy and regulatory discussions concerning terrorist use of the internet

Governments and multinational institutions should intensify their focus on T/VEOWs in their online counterterrorism efforts. Unfortunately, by contrast with government focus on social media platforms, insufficient attention is devoted to T/VEOWs specifically in public policy approaches to tackling terrorist use of the internet, despite the central role such sites played in disseminating terrorist propaganda.

2. Develop a global mitigation strategy to tackle T/VEOWs by more targeted and proportionate action

Due to the prominence of T/VEOWs in online propaganda campaigns, action to disrupt them should be a priority for all stakeholders invested in countering terrorist use of the internet. We note that to date, based on publicly accessible information, there has been insufficient government coordination against T/VEOWs.

Action against these sites should be based on improved engagement with web infrastructure providers to encourage action where appropriate. This activity will need to be coordinated carefully in line with the international norms of human rights and fundamental freedoms. Any strategy to counter T/VEOWs will need to avoid approaches fragmented by jurisdictions, which risks undermining effective and proportionate action.

The strategy should be developed in accordance with the following principles:

> **a. Coordination and deconfliction:** the strategy should emphasise coordination and deconfliction to avoid disrupting ongoing investigations and intelligence gathering. Coordinated action prior to removal or blocking should also allow the collection of evidence for prosecutions of war crimes and/or terrorist offences.

b. Rule of law: action should be underpinned by international legal consensus that specific groups and actors warrant designation as terrorists. The group inclusion policy developed for the Terrorist Content Analytics Platform (TCAP) can serve as one possible criterion for determining whether a suspected T/VEOW is in scope.[1]

c. Evidence base: action against suspected T/VEOWs should be taken only once the purpose of the website has been ascertained to a high evidential standard. The association with criminal activity should be clearly in proof to avoid the unlawful suppression of legal and legitimate speech; providers should make available appropriate mechanisms by which to appeal removal decisions. Such a test could comprise the elements below:

o Has the group / actor in question been designated as terrorist in nature either
- internationally, in in the Consolidated United Nations Security Council Sanctions List and/or among Five Eyes and EU members, or;
- domestically, by democratic nation states?

o Is there proof that the suspected T/VEOW is managed by:
- Core members of a terrorist group, or;
- supporters of a terrorist group?[2]

o Is the website's main purpose provably to disseminate terrorist propaganda or otherwise benefit a terrorist group?

d. Human rights and freedom of expression: all activity will need to be measured against potential negative implications for freedom of expression.

e. Segmented engagement by platform type: the strategy should consider a segmented engagement model based on the Internet Jurisdiction and Policy Network's due diligence guide for notifiers of technical abuse at the DNS level.[3]

3. Ensure that activity tackling T/VEOWs is carried out with the fullest respect for human rights and fundamental freedoms, including for online freedom of expression.[4]

4. Improve the designation of terrorist groups by reference to human rights and fundamental freedoms

Governments should seek to improve designation of terrorist groups in order to provide a clearer basis for action from tech companies, including against T/VEOWs. A clear legal basis for disruption significantly improves tech company action against terrorist content and activity online, and is likely to have significant positive impact on infrastructure company action against T/VEOWs.

[1] https://www.terrorismanalytics.org/inclusion-policy
[2] See below for Tech Against Terrorism's methodology in assessing suspected T/VEOWs.
[3] https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-113-Due-Diligence-Guide-for-Notifiers.pdf
[4] Future Tech Against Terrorism research will explore models for ensuring human rights compliance in T/VEOW responses.

B) Recommendations for infrastructure providers

1. Include explicit prohibition of terrorism in Terms of Service
Infrastructure providers should explicitly prohibit terrorist use of their services in their Terms of Service to facilitate action against suspected T/VEOWs. Such prohibitions should make provisions for freedom of expression and have regard for due process, and should clarify what actors constitutes terrorists as envisaged by the Terms; for example, by referencing international or national designation lists.

2. Work with governments and law enforcement to act against T/VEOWs
Infrastructure providers should, in conformity with international norms and the UN Guiding Principles on Business and Human Rights, work collaboratively with governments, law enforcement, and online counterterrorism practitioners to take action against T/VEOWs. It is paramount that all actors undertake this activity with respect for human rights and fundamental freedoms.

3. Produce transparency reports, as recommended by Tech Against Terrorism
Infrastructure providers should produce transparency reports on the actions they take to disrupt T/VEOWs. Such transparency should be based on the Tech Against Terrorism Guidelines[5] on transparency reporting on online counterterrorism efforts, as well as on the Santa Clara Principles.[6]

C) Recommendations for researchers and civil society

1. Increase research on T/VEOWs and on the potential impact of their removal
We note that, to date, there has been a lack of research on T/VEOWs and their role in the online ecosystem inhabited by online terrorists and violent extremists. While we hope that this report in part addresses this gap, we encourage expert researchers to intensify their efforts in this area, and in particular to assess the risks associated with the adverse shifts in behaviour that T/VEOW removal could potentially cause.

2. Report suspected T/VEOWs to infrastructure providers and/or law enforcement
Whilst we appreciate the research value of keeping terrorist content online, we encourage researchers to report such sites to infrastructure providers and/or law enforcement as applicable, and to work with Tech Against Terrorism to archive such material, by means either of the Terrorist Content Analytics Platform (TCAP) or the academic research hub Jihadology.[7]

3. Scrutinise T/VEOW removals
Civil society groups and expert researchers should monitor T/VEOW removals and hold governments and infrastructure providers accountable should such activity impact adversely on human rights and fundamental freedoms.

[5] https://transparency.techagainstterrorism.org/
[6] https://santaclaraprinciples.org/
[7] https://jihadology.net/

3. INTRODUCTION

T/VE-operated websites are severely undermining global efforts to counter terrorist use of the internet. Since early 2020, Tech Against Terrorism has been compiling a database of terrorist- and violent extremist-operated websites (T/VEOWs). To date, we have identified **198 domains** relating to T/VE actors. These sites provide terrorists and violent extremists with relatively stable online spaces to conduct their activities in pursuance of their strategic objectives. Between January-November 2021, **Tech Against Terrorism facilitated the removal of 16 T/VEOWs operated** by various T/VE actors including Atomwaffen Division, the Taliban and the Islamic State. All takedowns were conducted in partnership with infrastructure companies.

T/VEOWs pose a significant threat to society. These sites on the surface web provide terrorist actors with a stable and accessible space in which to, among other activities, host propaganda content, recruit new members, and raise funds. T/VEOWs are not the exclusive practice of any single ideology or group. Violent far-right and violent Islamist groups both utilise such sites in similar ways.

What threats do T/VEOWs pose?

T/VEOWs are publicly available, often indexed by search engines

They often have little or **no need for content sanitisation** or automated content moderation avoidance tactics

Often T/VEOWs offer more surface **web stability** than platforms managed by large tech companies

The threshold for T/VEOW removal by infrastructure providers is often higher than social media companies

Registrant **identity can be protected** and made private; some providers do not require any personally identifiable information to register

Tech Against Terrorism identifies a site as a T/VEOW if it meets one or more of the following criteria:

- **The website is highly likely to be run by members or supporters of an organisation that has been designated as terrorist by at least one democratic government. Examples include sites that are run by members or supporters of actors including al-Qaeda, Islamic State, Atomwaffen Division or Blood and Honour.**

- **The website espouses or praises violent extremist ideologies, whether it be associated with a group, individual, or movement. In general, websites included on the basis of this criterion are run by actors not yet designated as terrorists. Examples include websites relating to actors such as Order of the Nine Angles and multiple violent neo-Nazi groups.**

We assess whether a website is terrorist or violent extremist-operated based on a combination of several factors, which include but are not limited to:

- **Evidence that the administrator(s) of a website are promoting terrorism or violent extremism, such as URLs to other online terrorist or violent extremist networks**

- **The proportion of content on the website that we identify as being produced by or in support of a terrorist or violent extremist organisation**

- **No indication that the site's administrator actively tries to counter online terrorist content, or engages in preventing or countering the radicalisation of the site's users**

- **Promotion or endorsement of the website by TVE organisations or their affiliated networks elsewhere online**

- **Evidence that the website hosts or promotes outlinks to other terrorist or violent extremist online spaces**

- **Identification by reputable third-party organisations or counterterrorism researchers that the website is run for terrorist or violent extremist purposes**

T/VEOWs are not a new phenomenon. They have been used since the development of the internet in the mid 1990s. During this time, violent far-right actors began utilising online forums to achieve their operational and strategic goals. Additionally, in the early 2000s, unofficial "jihadi forums" became central to the online ecosystem of violent Islamists.[8]

[8] https://www.ynetnews.com/articles/0,7340,L-4422349,00.html

As the internet diversified, so too did the way terrorists instrumentalise online spaces. With the rise of social media platforms in the late 2000s, terrorist actors sought to exploit this shift, and consistently attempted to take advantage of the many features that these new online spaces had to offer, including their potential for reaching a wide audience and straightforward and efficient means of disseminating terrorist media and communications.

Broad improvements in content moderation by large social media platforms have in recent years forced T/VE actors to continually adapt their behaviours and tactics to maintain stability and visibility. As such, terrorists have been pushed onto increasingly niche online spaces where their reach is more limited. As a result, many T/VE actors have supplemented their lack of presence on large platforms with presences on smaller platforms, as well as websites and bespoke apps.

Tech Against Terrorism believes that the global tech sector and governments need to collaborate more proactively in order to better counter the threat posed by T/VEOWs, while still respecting human rights and freedom of speech.

Currently, the process of removing T/VEOWs differs from country to country, and there are few clear laws regarding responsibilities around T/VEOW removal. A media report regarding a collaborative takedown of 27 T/VEOWs by German and UK police in November 2021, for example, underlined that "fewer than half the number of sites originally flagged… were taken down because law enforcers currently rely on voluntary co-operation with the service provider community."[9]

Widespread and persistent global improvements in T/VEOW removal are likely to cause adverse shifts in terrorist use of the internet, and would not necessarily address the issue of T/VEOW recidivism. If terrorist actors are prevented from successfully exploiting internet infrastructure, they may as a result grow more reliant on using alternative spaces such as the dark web, or decentralised hosting technologies.

Tech Against Terrorism acknowledges that some of these sites may not be removed for the operational counterterrorism purposes of intelligence agencies. However, given the lack of available data on which T/VEOWs may be being used for such reasons, Tech Against Terrorism identifies T/VEOWs as a credible threat that warrants disruption.

[9] https://www.europol.europa.eu/newsroom/news/germany-uk-and-europol-target-violent-jihadist-websites

What is website infrastructure?

Website infrastructure refers to anything that interconnects computers and users on the Internet, including physical hardware, transmission media and software.

Given that terrorists exploit a wide range of infrastructure providers when building a website, mitigation of this exploitation is exceedingly complex given each of these providers will have their own unique set of challenges. Below are some examples of such infrastructure providers and what they do:

Web hosting providers: companies that provide websites with server space and internet connection. These services can be suspended (and take a website offline) when a website is hosting criminal content (depending on the jurisdiction) or violates a hosting provider's Terms of Service

DNS registries: organisations managing top-level domains, setting guidelines for domain names, and working with DNS registrars to sell domain names

Domain Name System (DNS) registrars: companies authorised by DNS registries to allocate domain names to websites, which website operators purchase from registrars. DNS registrars play an important role in directing users to websites. Without a domain name, users would need to know a site's IP number to access it. DNS registrars can remove a domain and therefore largely disable access to sites, however this will technically not take the website offline

4. WEBSITE ANALYSIS

Scope of our research

Since January 2021, Tech Against Terrorism has conducted open-source intelligence (OSINT) research into the threat of T/VEOWs. Our methodology comprises of keyword searches across several mainstream and niche social media and messaging apps, as well as search engines and bespoke apps. We mostly conducted searches in English and Arabic, though also in Dari, Pashto and Russian.

We also identified T/VEOWs through daily monitoring of online terrorist spaces that are likely to promote such sites, such as social media platforms and messaging platforms. Our daily monitoring encompasses both mainstream and niche social media, video sharing platforms, and messaging platforms.

Our research focused firstly on websites that are likely to be run by terrorist organisations designated as such by democratic nation states and multinational institutions. Secondly, we investigated supporter-run websites whose content or purpose was to further the goals of designated terrorist organisations. Thirdly, we looked at websites operating in support of networks, ideologies or entities not yet designated as terrorist or extremist, but which in our assessment present a violent threat to society on the basis of their rhetoric or links to real-world violence.

At the time of writing, Tech Against Terrorism's T/VEOW tracker included:

198 T/VEOWs
- 79 violent Sunni Islamist
- 18 violent Shia Islamist
- 101 violent far-right

30 Domain Name Registrar companies listed in the tracker, and 28 Website Server companies

In 2021, **Tech Against Terrorism facilitated the removal of 16 T/VEOWs** relating to violent far-right actors, the Taliban and the Islamic State.

Common features of T/VEOWs

The following statistics are based on a representative sample set of 33 sites chosen from the Tech Against Terrorism T/VEOW tracker. The sample was chosen to reflect the widest possible array of actors across the violent far-right and violent Islamist landscape. Of these 33 T/VEOWs, all were live at the time of writing. Furthermore:

- 17 domains pertain to violent Islamist T/VE actors.[10] Within these, 7 were linked to al-Qaeda, 4 to IS, and 4 to violent-Shia Islamist actors.

- 16 sites relate to the violent far-right, including to actors such as Blood and Honour, Combat-18, affiliates of Atomwaffen Division and Order of the Nine Angles.

The 17 Islamist T/VEOWs were mostly viewed by audiences in Algeria, Pakistan and Turkey.[11]

The 16 violent far-right T/VEOWs were mostly viewed by audiences in the United States, Germany, the United Kingdom and Czech Republic.[12]

[10] Within the 17 violent Islamist T/VEOWs in the dataset, 4 were linked to the Islamic State and 7 were linked to al-Qaeda.
[11] This relates to the total audience geography across the 17 websites. Data taken from Similarweb Pro. All data is approximate.
[12] This relates to the total audience geography across the 16 websites. Data taken from Similarweb Pro. All data is approximate.

The most significant findings from the dataset are:

The total number of monthly visits recorded across these 33 T/VEOWs is 1.54 mn

91% of T/VEOWs in the dataset displayed some form of audio-visual propaganda. This includes images, videos, music, audio-clips

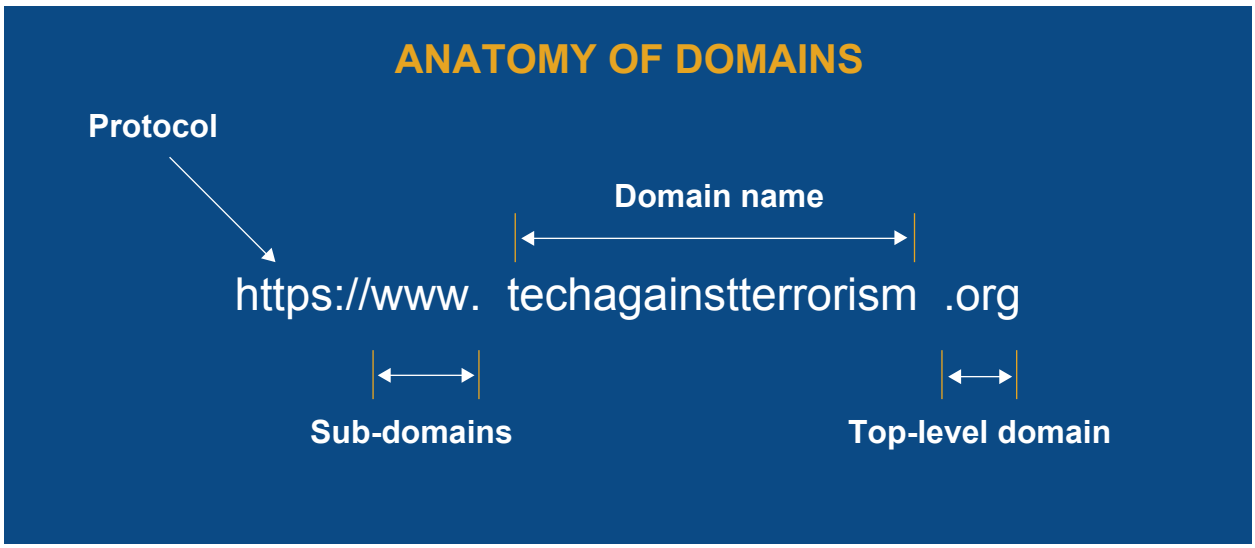
73% of the sites included an archive of historic content on the site

57% of the websites included a contact address form, allowing users to communicate securely and privately with the site administrators

Below, we break down the results of our sample set of the 33 T/VEOWs according to their ideological grouping:

Sample 33 T/VEOWs:	Audio/visual propaganda	Downloadable content	Books/PDFs	Blogposts	Fundraising	Merchandise
Violent Islamist	94%	82%	53%	35%	12%	0%
Violent far-right	88%	38%	38%	50%	56%	31%

Sample 33 T/VEOWs:	Links to deep/dark web	Links to other T/VEOWs	Comments section	Archive of content	Contact form	Multiple languages
Violent Islamist	35%	12%	53%	12%	41%	35%
Violent far-right	13%	13%	6%	75%	75%	19%



Changes to T/VEOW domain names

One way in which T/VEOWs can be disrupted is in domain name and top-level domain name changes. In the last year, Tech Against Terrorism has identified several instances of T/VEOWs going offline and re-appearing days or weeks later at a new top-level domain name.

In these instances, it is unclear who or what has facilitated the disruption of these T/VEOWs, and Tech Against Terrorism cannot be certain that proactive counterterrorism efforts are responsible for these changes in domain names.

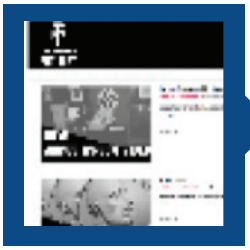
It is unlikely – though not impossible – that T/VE actors would voluntarily suspend their own domains. This is because frequent domain or top-level domain name changes can make a website much harder to find by T/VE actors and their supporter networks. T/VE actors on the whole seek to exploit online spaces for as long as possible in order to ensure longevity of their activity.

In our monitoring of T/VEOW domain and top-level domain changes, we did not identify any significant trends or patterns in behaviour. Some T/VEOWs remain online for long periods of time without interruption, such as al-Qaeda's as-Sahab Media site outlined in our Case Studies. On the other hand, other T/VEOWs are frequently interrupted and often re-appear on new top-level domain names every few weeks. One such example is the IS-supporter media translation site.

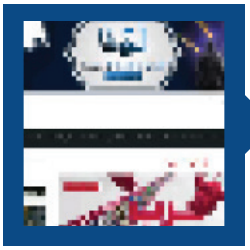
Below we include examples of four websites that have undergone domain name changes in the past year, including sites affiliated with IS, Al-Qaeda and the violent far-right.

Since January 2021, Tech Against Terrorism has noted that:

An IS-affiliated website which provides translations in 18 different languages receives around **9,781monthly visits**. It has **changed domains at least four times since first appearing online in July 2021**. The domain name has remained the same, but the top-level domain has changed.



This website is associated with two designated far-right terrorist entities, and subscribes to a violent accelerationist ideology. It receives around **142,758 monthly visits**. It has **changed its domain at least once** since it was created in November 2021.



Another pro-IS propaganda archive website **changed domains at least 25 times over the past year** – including changes to the domain name and the top-level domain. Websites analytics for this site were unavailable at the time of writing, as the domain was not live.

A neo-Nazi accelerationist website, which was first created in November 2021. Precise data on the site's monthly visits is not available, as it has fewer than 5,000 visits per month. It has since **changed top-level domain at least twice**. It supports the work and ideology of James Mason, and hosts a significant volume of propaganda that incites violence.

This terrorist-operated chat server is used by al-Qaeda and its affiliates to spread propaganda and communicate internally. Precise data on the site's monthly visits is not available, as it has fewer than 5,000 visits per month. It has **changed domains at least once** since it was created in early 2020.

5. CASE STUDIES

Tech Against Terrorism chose the following case studies to highlight that a broad range of actors utilise T/VEOWs for a number of different strategic and operational purposes. The case studies were taken from Tech Against Terrorism's T/VEOW tracker, which includes 198 different domains. Some details of the case studies in question have been omitted in order to avoid amplifying the sites or the content they host and promote.

As the Atomwaffen Division-linked domain was no longer active at the time of writing, Tech Against Terrorism could not verify website analytics statistics for this domain. This highlights the gap in available data on historic T/VEOWs that hinder research and analysis on their use and function in the online terrorist ecosystem.

Domain	Monthly Visits	Age of Domain (at the time of writing)	Geography of Audience
Atomwaffen Division site[13]	N/A	N/A	N/A
As-Sahab Media	9,060	1 Year, 2 Months	Pakistan, Oman, Lebanon, Turkey, Morocco
Hezbollah	32,545	24 Years, 11 Months	Lebanon, Iran, US Hungary, Belgium
IS OPSEC Group	14,200	4 months	Netherlands, UK, Tunisia, Egypt, Spain
IS Supporter Propaganda Archive	<5,000	2 Years, 1 Month	Israel, Saudi Arabia, Algeria, Egypt, Netherlands
Nationalist Socialist Alliance	<5,000	N/A	US, Brazil

Source on website monthly visits: Similarweb Pro.

Atomwaffen Division

In June 2021, Tech Against Terrorism facilitated the removal of a website claiming to be the official site of Atomwaffen Division, an accelerationist Neo-Nazi accelerationist terrorist group officially designated as such by the UK and Canada. Atomwaffen Division is a largely US-based internationally proscribed terrorist entity with a multinational following and associated offshoot groups that have also been designated as terrorist entities in multiple countries.[14] The group has been linked to several murders in the US.[15]

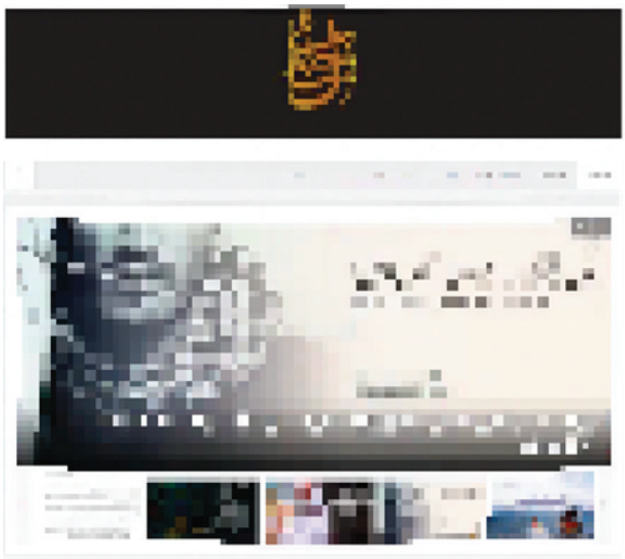
[13] As the domain was no longer active at the time of writing, Tech Against Terrorism could not verify website statistics for this domain.
[14] https://www.terrorismanalytics.org/group-inclusion-policy
[15] https://www.theguardian.com/world/2020/mar/06/neo-nazi-arrests-deals-blow-us-group-atomwaffen-division ; https://www.npr.org/2018/03/06/590292705/5-killings-3-states-and-1-common-neo-nazi-link?t=1638355721582

The site claimed to be the "Official Website of the Atomwaffen Division", and contained links to propaganda produced by the group and affiliated violent far-right actors, although much of this had been removed at the time of discovery.

The site also provided a membership application form for prospective members of the group to fill out.

As-Sahab Media

Al-Qaeda's official media outlet As-Sahab is active across a number of online spaces, including social media platforms, messaging apps as well as on its own dedicated website. The website was first registered in October 2020, and hosts hundreds of pieces of propaganda content. While the vast majority of the content on the site is in Arabic, some content also has translations in English. The site remained live at the time of writing.

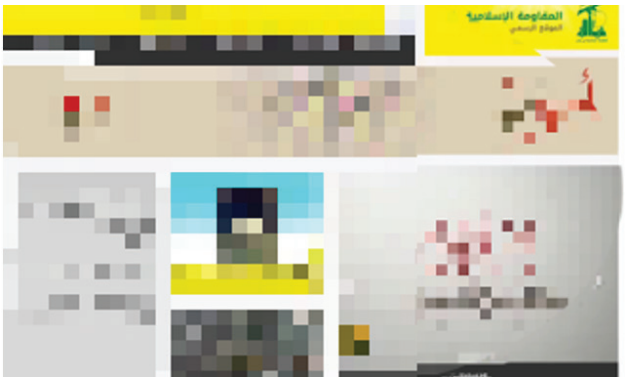


The content on the site is regularly updated and includes videos by al-Qaeda leader Ayman al-Zawahiri and mixed text-image media such as articles.

The website also links to other al-Qaeda-linked sites online. Our teams constantly find links to as-Sahab's site in other official and non-official al-Qaeda online spaces, on both messaging apps and social media platforms.

Hezbollah

Hezbollah is a designated Islamist terrorist group and political organisation that exerts significant influence across Lebanon, and to a lesser degree in Syria. The group has been designated as terrorist and proscribed by several governments including Germany, France, the US, and the UK. Many other countries observe a distinction between the group's "military wing" and the rest of the organisation.



Hezbollah makes extremely diverse use of the internet. The group uses a broad variety of websites, as well as messaging and social media platforms, for various operational and strategic purposes. Despite the group being banned from several social media platforms,28 Hezbollah supporters and members have extensive presence across mainstream online spaces. Supporters disseminate a significant volume of content in support of the group and its leader, Hassan Nasrallah. Hezbollah have in addition to a main, central website that acts as a main hub of news relating to the group, commemorations of its deceased fighters, and propaganda content, the group has several official and unofficial media entities, as well as multiple other dedicated websites. Hezbollah is less reliant on websites than other TVE actors due to its ability to reach a mass audience via traditional media outlets through which it receives coverage as a political entity.

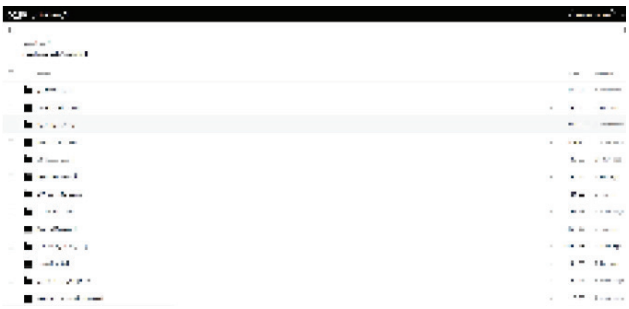
Islamic State Operational Security Group

This website is run by a prominent pro-IS tech support group concerned primarily with increasing cyber security awareness among Islamic State supporters, with the probable aim of assisting them to avoid detection and arrest by law enforcement. The group regularly produces guides for specific apps, platforms and tools in Arabic, English and French, many of which are hosted on its website.

The group's site was removed in April 2021 following a report by Tech against Terrorism to a website infrastructure provider. However, the website was later recreated with a different domain. At the time of writing, the domain was active.

Islamic State Propaganda Archive

This Islamic State propaganda archive site is an IS-supporter run cloud domain platform.[16] At the time of writing, the site hosted 1.9 terabytes of propaganda content that spans across multiple languages and types of content. All of the content on the website is easily downloadable by its users via a "download" button.

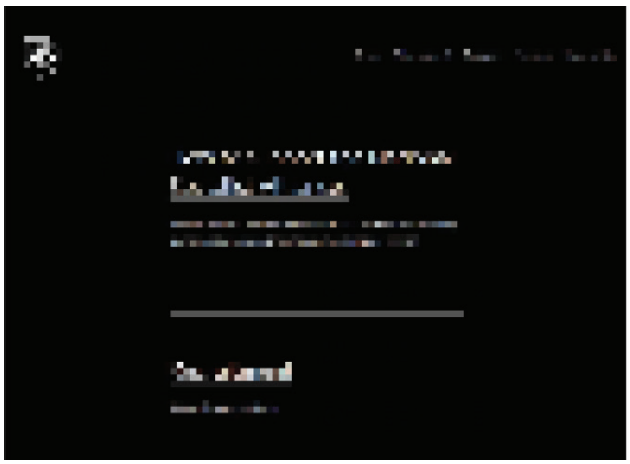


The site is password protected, and access is granted via contacting a bot on encrypted messaging apps. However, links with tokens granting access without login are regularly shared in pro-IS channels in other IS online spaces, although such links only provide access to that specific entry point.

Tech Against Terrorism helped facilitate this site in 2020, however it later returned on a new top-level domain name. Since then, the site has stayed relatively stable, and therefore plays a crucial role in keeping IS propaganda active online. The fact that the site is still accessible allows for mirrored versions of the site to be created and make its contents available to broader masses.

[16] https://www.techagainstterrorism.org/2021/07/30/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/

Nationalist Socialist Alliance



Nationalist Socialist Alliance is a self-described accelerationist Neo-Nazi online group that is actively recruiting new members. NSA announced an "alliance" with another new violent far-right extremist group calling itself the International White Syndicate (IWS) in mid-October. Their respective channels broadly subscribe to the white supremacist ideology propagated by neo-Nazi James Mason in his book Siege; its propaganda and suggested readings include references to Charles Manson, Oswald Mosley, and William Luther Pierce's The Turner Diaries. The online group also has a dedicated domain for promoting their aims and ideology, and for recruitment drives.

The website has an area dedicated to "Propaganda" – at the time of writing, this only included two posters which directed visitors to an inactive Telegram channel. During our research, NSA's top-level domain changed twice. This is likely because the original iteration of the site had been removed, though it is unclear how it was removed or by whom. NSA also has a mirrored site on the dark web, which likely serves as a backup for content.

6. WIDER THREAT LANDSCAPE

The terrorist online landscape

Whilst terrorist content can still be found on larger tech platforms, T/VE actors are forced to be increasingly creative to avoid platforms' efforts at content moderation. Terrorists often deploy a number of different evasive tactics like obscuring incriminating keywords with special characters or symbols, or presenting themselves as legitimate posters such as journalists in order to escape detection.

If terrorists were able to maintain a stable and overt presence on mainstream social media platforms, they almost certainly would do so. This is because mainstream social media platforms have large userbases that T/VE actors would wish to exploit for the purpose of disseminating propaganda to as wide an audience as possible.

Larger tech platforms have in recent years expanded their capability to moderate TVE content effectively. Furthermore, governments have also invested in attempts made by online platforms to tackle terrorist use of the internet by, for example, collaborative arrangements such as Internet Referral Units.[17]

This approach, broadly speaking, has forced TVE actors to congregate on a greater number of smaller, more niche and less regulated alternatives. In these smaller online spaces TVE actors tend to be less inhibited by content moderation due to platforms' lack of either capacity or willingness to moderate content swiftly and effectively.

[17] Internet Referral Units (IRUs) are specialised law enforcement units which refer suspected terrorist content to tech platforms. Such units are operational in (for example) the EU (Europol), the UK, France, the Netherlands, and Israel.

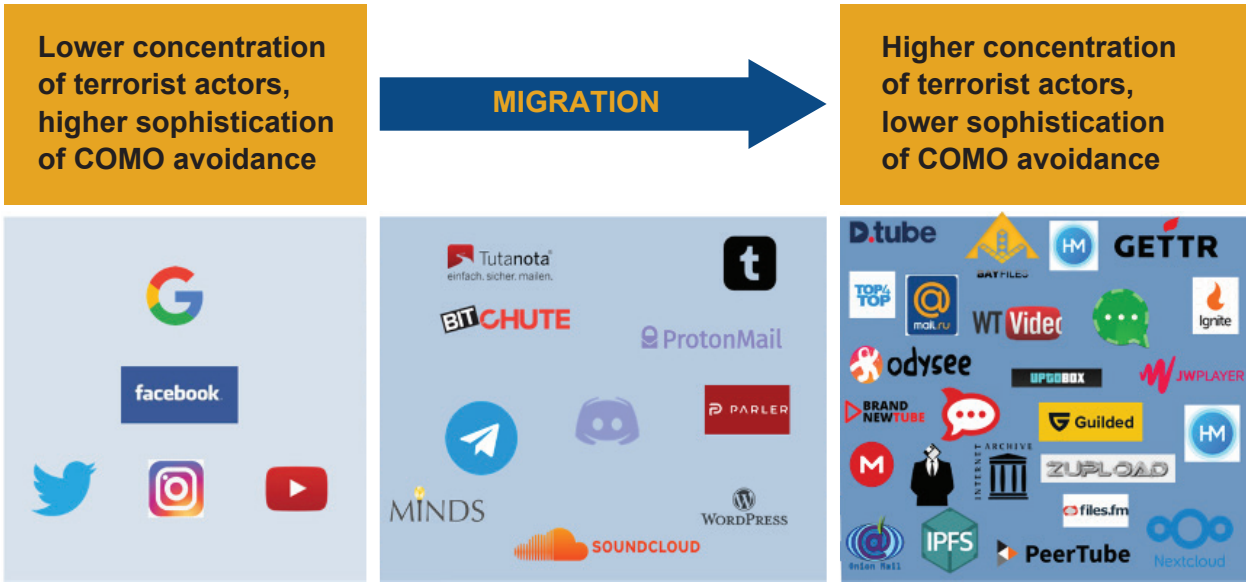


Figure 1: A visual depiction of terrorist migration from large to smaller tech platforms. Companies listed are included as examples only.

The ability of T/VE actors to reach a wide audience is restricted on more niche platforms, and such actors can still face deplatforming from these spaces. T/VE actors are continually forced to be creative in their use of the internet to ensure the maximum reach of their propaganda and the ongoing availability of their content online. They therefore usually operate through a multiplatform approach, where they employ several online platforms simultaneously to maintain an online presence that is as stable and wide-reaching as possible.

This approach is most extensively used by violent Islamist actors. Groups such as al-Qaeda, IS and their supporter networks typically publish new multimedia releases to as many as 100 separate online locations simultaneously, and then share the content on messaging apps, paste sites and archiving services in aggregated URL lists that lead to copies of the original content.

Violent far-right actors online also engage in a multiplatform approach, although rarely do they publish content via long lists of outlinks like violent Islamist actors do. Instead, far-right actors disseminate content largely via loosely affiliated ad hoc content creators. The violent-far right tend to congregate on platforms where they believe their content is less likely to be removed. These platforms include alt-tech social media and video-sharing sites, archiving services, encrypted messaging apps and email services.[18]

Violent far-right actors will often promote and maintain accounts across several platforms simultaneously to reach as wide an audience as possible. Furthermore, the violent far-right are also increasingly building their own platforms hosted on the Domain Name System (DNS). Given the growing number of alt-tech platforms hosting varying degrees of terrorist or violent extremist content on the internet, this can lead to increasingly blurred lines between some platforms that present themselves as being "alt-tech" and are not doing enough to tackle terrorist and violent extremist use of their services, and those that are run by violent extremist or terrorist sympathisers.

[18] Alt-tech online spaces have positioned themselves as providing alternative spaces to the mainstream online media landscape. Alt-tech spaces usually position themselves as championing "free speech" in their approach toward content moderation, and include platforms such as Gab, Parler, Gettr and others.

Terrorist and violent extremist-operated websites play an increasingly important role in the wider ecosystem of online terrorist exploitation. Amid broad improvements in the moderation of content by mainstream platforms, T/VEOWs provide terrorist and violent extremist organisations, and their supporters, with relatively stable, easily discoverable pages on the surface web which often serve to mitigate the negative effects of their forced migration onto smaller or lesser-known platforms whose audience reach is likely to be relatively low.

Function of T/VEOWs

T/VEOWs play an increasingly important role in the online terrorist information eco-system as they often act as a centralised and easily accessible archives of content that would have otherwise been removed from social media and messaging platforms. One such example is the Islamic State (IS)-run website as outlined in the Case Studies, which contains an archive of more than 90,000 items of propaganda and which was live at the time of writing.[19]

T/VEOWs grant terrorists more control over their content and communication than they otherwise would have on a third-party-run site or platform. This is because terrorist actors can curate the content on a website that they operate, with less need to obfuscate content or otherwise evade detection in order to comply with a website's ToS.

Besides undisturbed content hosting, T/VEOWs perform several different functions to T/VE actors and their supporter networks, including but not limited to the following:

Dissemination of propaganda content

Websites provide terrorist actors with a platform to disseminate propaganda in various mediums including text, videos and images. There are no inherent restrictions on the type of media that can be disseminated via a website, which allows for a hub of uncensored terrorist content.

Archiving of content

T/VEOWs can also act as an archive of historic terrorist content, that would otherwise have been removed from other online spaces, such as messaging and social media platforms. The IS online archive is one such example of a terrorist actor successfully using a website to archive terabytes of content.

Communicating with other TVE actors

Websites also provide online users with a space where they can communicate, albeit largely publicly, and usually in an unsecured way. For example, a site hosting propaganda videos may allow users to leave comments, or there may be a "Contact" page on a site for prospective recruits to use.

Means of generating revenue

Websites can also act as a means of generating income for T/VE actors, whether by selling merchandise or soliciting donations. Some T/VEOWs utilise the mechanisms underpinning cryptocurrency, which can make disrupting their online revenue streams more difficult.

[19] Tech Against Terrorism facilitated the removal of this site in April 2021. However, the site returned on a different domain name. At the time of writing, the new domain was live.

7. COUNTERING THE THREAT OF T/VEOWs

Overview of current approaches to disrupting T/VEOWs

There are numerous ways to make T/VEOWs inaccessible to the public, including by removing the site itself or by making it more difficult to find. Outlined below are some of the most common site removal methods used by infrastructure companies and governments.

Disruption by DNS registrars

T/VEOWs can be disrupted by Domain Name System (DNS) Registrars, which can render a website inaccessible by deregistering its domain name. This can be initiated by the registrar themselves or via third-party reports such as from law enforcement, NGOs, civil society groups, or private individuals, all of whom can send an Abuse Report to the registrar with evidence that the site is a T/VEOW.[20]

In 2021 alone, Tech Against Terrorism sent 16 Abuse Reports regarding T/VEOWs to multiple registrar companies. At the time of writing, the registrar companies had removed 15 of these sites.

In some cases, if a registrar does not respond to an Abuse Report or states in response to one that they cannot take action, an Abuse Report may be sent to the DNS hosting service. The DNS hosting service can then block the IP address link associated with the website, which severs the link between the URL and the website. In this case, the domain name is still registered with the registrar, but will show an error message when searched for, as the DNS will not redirect to the website.

Disruption by hosting provider

Web hosting providers have the right to suspend a website for many reasons including malware infection, spam content and other violations of their policies, including the hosting of terrorist content.[21]

When a web host provider suspends an account, it means that the website has been taken offline. This method of removal is more robust than simply deregistering a domain name. This is because, website administrators can easily create a new domain or top-level domain name for their site – however, if a website has been taken down by a site host, then the contents of that site has also been removed.

Search engine delisting

Should website infrastructure companies be unwilling or unable to take down a T/VEOW, it is also possible for search engines to delist the websites – however, as with the approach above, this does not remove the site entirely.

Delisting by a search engine means that any user searching for the T/VEOW on that search engine will not be shown a result. While this does not remove the site entirely, it makes it much more difficult to find for users who do not already know the site's domain – whether those users are members of the general public or T/VE actors and their supporter networks. Due to the growing number of search engines, a site that has been delisted from one search index may still be discoverable through other engines.

[20] For further details about the necessary information to include in Abuse Notices, see here: https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-113-Due-Diligence-Guide-for-Notifiers.pdf ; https://www.internetjurisdiction.net/uploads/pdfs/Briefing-Note-IJPN-Toolkit-DNS-Level-Action-to-Address-Abuse-2021.pdf

[21] https://www.malcare.com/blog/web-host-suspended-site/

In some cases, results on a search engine may be restricted at the request of governments or in accordance with domestic law, such as the blocking of websites containing Nazi material in Germany. While this does not remove the website URL from the search engine entirely, it places a geo-restriction on the URL so it cannot be accessed by users in certain locations.

Government seizures of domains

In some cases, governments may seize the domain of a website if it is considered a national security threat.[22] This has on occasion been carried out by the US Department of Justice[23] such as in 2021 when the government seized domains relating to Iran's Islamic Revolutionary Guards Corps, and the Iran-backed, Iraq-based militia Kataeb Hezbollah – both of which are designated as terrorists by the US.[24]

The US government also has the legal right to seize a domain if it is administered by an actor that is officially designated as a terrorist entity, or there is sufficient evidence that the actor is engaged in terrorist activity. In line with the US government's "Operation In Our Sites" project – which seeks to detect and hinder intellectual property violations on the Internet – the government can seize a domain name's title and rights.[25]

Social media platforms blocking URLs

Social media platforms are also able to disrupt the activities of T/VEOWs online. A social media platform can prevent a specific URL from being disseminated in content, posts, and comments. This strategy means that users of the social media platform are not redirected to a T/VEOW from within the platform. Like search engine delisting this method does not remove the website at all, but prevents users from a particular online space from discovering or sharing the URL. This content moderation tactic could also easily be circumvented by users seeking to disseminate the T/VEOW URL by using link shorteners.

The Terrorist Content Analytics Platform (TCAP)

Tech Against Terrorism is actively helping the tech sector identify verified URLs relating to content from terrorist groups via the Terrorism Content Analytics Tool (TCAP).

The TCAP tracks, verifies, and analyses terrorist content from across the internet, and alerts it to tech companies that have signed up to receive alerts from the tool.

At the time of writing, the TCAP has identified 21,894 URLs of verified terrorist content, of which 12,751 have been alerted to 68 different tech platforms. At least 93% of all alerted content has since been removed. For full details see: **terrorismanalytics.org**

[22] The US government stated in 2012 that it has the right to seize any top-level domain ending in .com, .net and .org, because the companies that have the contracts to administer them are US based. https://www.wired.com/2012/03/feds-seize-foreign-sites/
[23] https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps
[24] https://edition.cnn.com/2021/06/22/politics/us-seizes-iran-website-domains/index.html
[25] https://btlj.org/data/articles2015/vol28/28_AR/28-berkeley-tech-l-j-0859-0900.pdf

Industry-led approaches

To Tech Against Terrorism's knowledge, there are no established tech-industry level approaches to countering T/VEOWs specifically. However, for over a decade various stakeholders have engaged in dialogue to define and mitigate DNS-related security threats.[26]

The Internet Corporation for Assigned Names and Numbers (ICANN) has played a central role in ensuring the secure operation of the internet's unique identifier systems,[27] but has no mandate to regulate the services or content that use this infrastructure.[28] ICANN works alongside multiple stakeholders to address DNS abuse including the Internet & Jurisdiction Policy Network, the Global Cyber Alliance,[29] the DNS Abuse Institute,[30] Verisign,[31] and ECO DNS Abuse Initiative.[32] One particular industry initiative which offers guidance to infrastructure providers on abusive and illegal content is the DNS Abuse Framework by ECO.[33] There are currently 48 infrastructure providers who are signatories to the Framework and actively seeking to disrupt the abuse of infrastructure services.

The Internet & Jurisdiction Policy Network has also developed a toolkit for addressing abuse at the DNS level. While this is not a specific industry approach with input from all infrastructure providers, the toolkit aims to consolidate current approaches to countering the abuse of infrastructure services and address at policy level the abuse of infrastructure services. The toolkit specifically states that abuse includes "content that depicts graphic violence, encourages violent action, endorses a terrorist organization or its acts, or encourages people to join such groups." This joint examination of both T/VEOWs and terrorist use of infrastructure services provides a solid policy foundation for the disruption of such activity and takedown of the sites hosting it.

Infrastructure providers' Terms of Service (ToS)

In a review of the most widely used infrastructure providers' Terms of Service (ToS), Tech Against Terrorism found that few infrastructure providers, specifically Domain Name Registrars, explicitly prohibit terrorist use of their services. Some providers outline specific content which they will not allow users to post, including content pertaining to "terrorism" or "terrorist activities."

However, often these ToS do not detail what national or international proscription lists the provider consults to determine what constitutes terrorism. Further, many also do not clearly define what constitutes "terrorist activities."

With no clear inclusion criteria for what constitutes "terrorism" or "terrorist activity," the threshold for removal of T/VEOWs on the part of infrastructure providers is currently unclear. It is highly likely that infrastructure providers define "terrorism" in the same way as their host governments do, to ensure they meet the legislative requirements within their jurisdiction.

[26] https://circleid.com/posts/20211206-ongoing-community-work-to-mitigate-domain-name-system-security-threats
[27] ICANN addresses DNS security threats and infrastructure abuse.
[28] https://www.icann.org/resources/pages/governance/bylaws-en/
[29] https://www.globalcyberalliance.org/
[30] https://dnsabuseinstitute.org/
[31] https://www.verisign.com/
[32] https://international.eco.de/
[33] https://dnsabuseframework.org/

Some websites are likely to be illegal in different countries due to differing standards of designating entities as terrorist. However, due to the global nature of the internet, websites will often still be accessible in jurisdictions where they have been banned, unless they have been blocked on the basis of geo-restriction. Of the 20 infrastructure providers' ToS that we evaluated, six contained explicit mention of terrorism and terrorist activity.

9. REMOVING T/VEOWs: RELEVANT POLICY CONSIDERATIONS

Disrupting T/VEOWs: Considerations and challenges

Responses to terrorist- and violent-extremist operated websites can be severe in that they often constitute the removal or blocking of entire websites. There are therefore several ethical challenges posed by tackling T/VEOWs. Furthermore, there are deeper questions about what role infrastructure providers should play in "moderating" the sites they support or host.[34]

It is our assessment that – partially due to a lack of strategic focus on T/VEOWs on the part of governments – these questions are often left for infrastructure providers to answer on a case-by-case basis. Whilst it is easy to highlight inconsistency from infrastructure providers in this regard, it should arguably not be a decision that rests with them in the first place.

Addressing these crucial questions in the detail they merit is outside the scope of this report. However, it is important to provide an overview of some of the considerations and challenges associated with T/VEOW removal to better ground possible countermeasures. Below we highlight some of the key challenges and considerations:

1. Risks to freedom of expression and digital rights

Digital rights advocates are rightfully wary of content moderation measures at the "stack" level.[35] This is mainly because, unlike when content or an account is removed from a platform, removal across various levels of the stack could have more far-reaching consequences.

For example, an internet service provider (ISP) could decide to reject services to an individual, which – particularly due to the general lack of provider competition on ISP level and or lack of alternatives based on where one lives – might mean that that individual is prevented from all internet access. Likewise, it could be argued that removal on the DNS level prevents individuals from exercising their right to seek information.[36] There are also concerns with how states may use counterterrorism (or perceived threats of other criminal activity) as justification for limiting access to website. There are examples of non-democratic and democratic states blocking or seeking to block access to entire websites in a way that is inconsistent with their obligations to international human rights law.[37] Any measure seeking to effect the removal of T/VEOWs will need to take into account the potential for these negative consequences.

2. Evidence base: assessing illegal content vs illegal website admins

There are different approaches that infrastructure providers might take towards sites that they provide services for. Whilst hosting providers might act when there is evidence of illegal material or content that violate their policies,[38] DNS registrars might instead need certainty that the actual site operator is part of an illegal entity, such as a designated terrorist group, before taking action. Assessing whether content is "terrorist" in nature is difficult in and of itself, and establishing

[34] https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content/
[35] https://www.eff.org/deeplinks/2021/04/content-moderation-losing-battle-infrastructure-companies-should-refuse-join-fight ; https://www.techdirt.com/articles/20211004/11314147696/infrastructure-content-moderation-challenges-opportunities.shtml
[36] https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[37] https://www.accessnow.org/keepiton/; https://gnet-research.org/2022/01/17/manipulating-access-to-communication-technology-government-repression-or-counterterrorism/; https://www.reuters.com/article/us-egypt-censorship-idUSKBN18K307
[38] https://www.theverge.com/2018/10/28/18034126/gab-social-network-stripe-joyent-deplatforming-hate-speech-pittsburgh-shooting

whether a designated terrorist group or actor is operating a specific site is not necessarily an exercise for which infrastructure providers are consistently equipped or trained. Importantly, even if providers do have the relevant resources and expertise, it is not clear what the evidential threshold for action should be.

3. Effectiveness

As discussed above, removed websites risk appearing as mirrored versions hosted by other providers or DNS registrars. They might also re-appear using providers with an ideological commitment to maintaining websites that have been thought to take a lax approach to terrorist or violent extremist content online.[39] Whilst this report argues that accurate removal is preferable to no action at all, it is still necessary to interrogate the efficacy of such responses in disrupting terrorist use of the internet.

4. Lack of certainty around jurisdiction and coordination

There are a number of barriers that currently frustrate action against T/VEOWs. The most significant barrier consists perhaps in the jurisdictional gaps between governments, within governments, and between governments and tech companies as to who should lead, request, and coordinate action against T/VEOWs. Based on our assessment and understanding, it is not always clear what legal powers governments have to support action against such sites. Furthermore, much like the general online regulatory landscape,[40] there is fragmentation in how different states choose to address the issue of illegal activity on an infrastructure level (if at all). Due to the lack of a global common approach, as well as global consensus around key legal mechanisms such as designation of terrorist groups, infrastructure companies often have limited guidance as to what actions they should take, and most publicly known action against T/VEOWs or hostile websites has to date been taken on the initiative of infrastructure providers themselves based on their own Terms of Service.

[39] This is something that has occurred with platforms such as Gab and 8chan.
[40] https://www.techagainstterrorism.org/2021/07/16/the-online-regulation-series-the-handbook/

10. CURRENT LEGISLATION ON COUNTERING T/VEOWs

Below we outline some legislative approaches to tackle T/VEOWs that governments are currently undertaking or have proposed. Whilst the list is not exhaustive, it is clear that not many states have a dedicated policy or instrument aimed at disrupting T/VEOWs.

Multiple states have legal provisions that allow for action against websites found to host illegal material. Whilst it is undeniably good that states have considered measures that can be used to disrupt T/VEOWs, it should be noted that the majority of the of the laws outlined below have been criticised by digital rights due to concerns over human rights and freedom of expression.

To see a more comprehensive summary of these concerns, see Tech Against Terrorism's Online Regulation Series Handbook.[41] Furthermore, the cases below demonstrate that there is little coordination between governments on approaches to T/VEOWs.

Australia

The 2021 Australian Online Safety Bill[42] includes provisions that bestow the country's e-Safety Commissioner with the authority to request the blocking or disabling of access to websites, platforms, or apps if such services are found to host illegal content or material likely to cause "serious harm". The Commissioner can issue a "link deletion notice" which requires search engines to restrict access to specific URLs via their services. The Commissioner may also issue an app removal notice compelling app distribution services to remove apps from their platforms. If material is found to depict "abhorrent violent conduct", the Commissioner can issue a blocking request to the site or platform hosting it. Blocking requests can order providers to take steps to block domain names, URLs, and IP addresses that provide access to abhorrent violent conduct material.

Canada

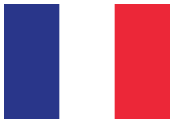
In 2021, Canada unveiled plans for ambitious legislation seeking to curb "online harms" such as terrorist content, incitement to violence, hate speech, child sexual abuse material, and non-consensual sharing of intimate images.[43] Amongst the many instruments this proposal suggests is a Digital Safety Commission, to petition the Canadian Federal Court to issue blocking orders to prevent access to websites and online platforms in Canada.

European Union

The 2015 EU Open Internet rules on net neutrality prohibit ISPs blocking access to websites, unless ordered to do so by courts.[44] However there have been high-profile cases which involve website blocking. The 2017 Court of Justice of the European Union (CJEU) decision regarding a case involving file downloading site Pirate Bay, effectively sanctioned website blocking as a proportionate response to copyright infringement.[45]

[41] https://www.techagainstterrorism.org/2021/07/16/the-online-regulation-series-the-handbook/
[42] https://www.infrastructure.gov.au/sites/default/files/documents/exposure-draft-online-safety-bill2020.pdf ; https://www.techagainstterrorism.org/2021/11/18/november-2021-update-to-australias-regulatory-framework/
[43] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html ; https://www.techagainstterrorism.org/2021/11/24/the-online-regulation-series-2021-canada-update/
[44] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=EN
[45] https://www.twobirds.com/en/news/articles/2017/global/cjeu-decision-in-ziggo-pirate-bay-does-communicate-to-the-public

While the EU's terrorist content online regulation,[46] which will come into effect in 2022, does not apply to infrastructure providers, the forthcoming Digital Services Act (DSA) might. The draft DSA places additional responsibilities on all internet companies to improve their response to illegal content. The proposal is currently in the negotiation stage, and could create the basis of a legal framework to facilitate action against T/VEOWs in the future.



France

The French 2004 law on confidence in the digital economy allows French judicial authorities to issue removal orders for websites that host material illegal under French law.[47] The law was amended in 2021 to enable what the government views as improved action on "mirror versions" of removed sites.[48] While there is little available information on how many websites France has blocked under this law, an Automatic Transparency Report notes France as one of the most frequent blockers of WordPress websites,[49] with the country having blocked 61 websites prior to June 2021.[50] The majority of WordPress websites blocked by France are suspected to have functioned primarily as al-Qaeda and Islamic State propaganda sites.[51]

Indonesia

Indonesia's Law No. 19 of 2016 regulates internet service providers operating in Indonesia and empowers the government to terminate access to websites or order an internet service provider to do so if content on a website is found to violate Indonesian law.[52]

New Zealand

New Zealand's Films, Videos, and Publications Classifications Act of 1993 covers websites that are operated or updated from New Zealand. If a New Zealand resident uploads or operates a T/VEOW, they can be prosecuted under the Classification Act. Further, the Department of Internal Affairs' Digital Safety Team, facilitates an online reporting form where the public can report websites suspected to be "made by terrorist or extremist organisations".

[46] https://www.techagainstterrorism.org/wp-content/uploads/2021/06/Tech-Against-Terrorism-response-to-EU-TCO-June-2021-1.pdf
[47] https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/ ;
[48] https://www.numerama.com/politique/702015-le-gouvernement-a-un-plan-pour-que-la-justice-bloque-mieux-les-sites-web.html ;
[49] France is behind countries like Turkey, Pakistan, and Russia, but ahead of countries such as Kazakhstan and Azerbaijan. See more on: https://transparency.automattic.com/country-block-list-october-2021/
[50] https://transparency.automattic.com/country-block-list-october-2021/
[51] Some of the websites blocked by France are available in other jurisdictions, however several have been taken down globally due to violating Automatic's Terms of Service.
[52] https://www.whitecase.com/publications/alert/indonesian-electronic-information-and-transactions-law-amended ; https://www.techagainstterrorism.org/2021/11/17/the-online-regulation-series-indonesia/

Turkey

Turkey's Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication, 2007, also known as the "Internet Law 5651" or "Law No. 5651" regulates prohibited content online, such as child abuse images and obscenity, and enables the removal and/or blocking of sites hosted in Turkey and filtering of websites hosted abroad.[53]

United Kingdom

Website blocking in the UK is relatively extensive compared to other Western countries. Since the early 2010s,[54] the UK's Counter Terrorism Internet Referral Unit (CTIRU) has compiled a list of websites which if shared by individuals within the UK, could make such individuals liable under the Terrorism Act 2006.[55] The list only includes websites hosted outside of the UK. While information on the list is scarce, in 2014 it was announced that major UK ISPs would incorporate the CTIRU list into their website filters.[56] The CTIRU can ask Nominet, who manages the .uk domains, to suspend domains suspected of hosting terrorist content.[57]

United States

The United States Department of Justice has the authority to "seize" websites controlled by terrorist-designated entities and individuals on the top-level domain level provided the domain is operated by a US company. In 2020 and 2021, such measures have been taken against websites operated by the Iranian Islamic Revolutionary Guards Corps – a branch of the Iranian armed forces designated by the US Department of State as a foreign terrorist organisation in 2019 – and Kataeb Hezbollah – an Iranian-backed Iraq-based militia, designated by both the Department of State and the Treasury in 2009.[58]

[53] https://www.techagainstterrorism.org/2020/10/23/the-online-regulation-series-turkey/ ; https://wilmap.stanford.edu/entries/omnibus-bill-no-524-first-introduced-june-26-2013-amending-provisions-various-laws and ; https://www.hrw.org/news/2014/09/02/turkey-internet-freedom-rights-sharp-decline

[54] https://www.legislation.gov.uk/ukpga/1988/48/section/97

[55] https://www.whatdotheyknow.com/request/160774/response/404100/attach/html/3/attachment.pdf.html

[56] https://www.theguardian.com/technology/2014/nov/14/uk-isps-to-introduce-jihadi-and-terror-content-reporting-button

[57] https://www.nominet.uk/wp-content/uploads/2021/02/Criminal-Practices-Policy-1-12-20-2.pdf

[58] https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps ; https://www.justice.gov/opa/pr/united-states-seizes-more-domain-names-used-foreign-terrorist-organization

BACKGROUND TO TECH AGAINST TERRORISM

Tech Against Terrorism is a public-private partnership supported by the United Nations Counter-Terrorism Executive Directorate (UN CTED). Tech Against Terrorism was launched in April 2017 at the United Nations Headquarters in New York and is implemented by the Online Harms Foundation. In this form, the initiative has been supported by the Global Internet Forum to Counter Terrorism (GIFCT) and the governments of Spain, Switzerland, the Republic of Korea, Canada, and the United Kingdom.

Our research shows that terrorist groups consistently exploit smaller tech platforms when disseminating propaganda. At Tech Against Terrorism, our mission is to support smaller tech companies to tackle this threat whilst respecting human rights, and to provide companies with the practical tools to facilitate these processes.