tech against terrorism

STRATEGY PAPER

RESPONDING TO TERRORIST OPERATED WEBSITES

JULY 2022

EXECUTIVE SUMMARY

1. Terrorist and violent extremist operated websites (TOWs) play an instrumental role in online terrorist messaging and tactical operations. TOWs are increasingly used by Islamist and far-right terrorist and violent extremist groups, and provide stable propaganda outlets, and many TOWs have remained online undisrupted for several years. At the time of writing, Tech Against Terrorism were tracking 212 domains that we suspect to be TOWs, many of which remained online. In a January 2022 Tech Against Terrorism report,[1] analysis of 33 of these show an average of 1.54 million monthly visitors

2. There is a lack of global targeted mitigation activity against TOWs. Further, this issue is largely absent from government-led policy discussions on disrupting terrorist use of the internet. As a result, there is no common global mitigation strategy to disrupt TOWs

3. There are multiple factors that complicate action against TOWs. Firstly, whilst individual governments have legal and operational mechanisms in place that can be used to disrupt TOWs, this creates a myriad of regulatory and operational (and contradictory) approaches that infrastructure providers need to navigate in order to ascertain their responsibility vis-à-vis potential TOWs. Second, the evidentiary threshold for accurately identifying a TOW is arguably higher than on most social media or messaging platforms. This is in large part because given that assessments identifying TOWs must entail ascertaining the website administrator's identity, as opposed to assessing content hosted on the site. Without guidance, this can make any abuse mitigation difficult for web infrastructure providers

4. Given the significant threat posed by TOWs, there should be increased action to tackle the use of TOWs by terrorists, as such action can significantly disrupt terrorist online operations. We encourage improved strategic leadership from governments in this regard

5. In the absence of a global mitigation strategy against TOWs, Tech Against recommends improved engagement with web infrastructure companies to help alert them to suspected TOWs and empower informed moderation decisions. In this paper we present our strategy for improving such activity. Engagement with infrastructure companies should be based on the principles of rule of law and freedom of expression, and any recommended action from a notifier should be supported by a strong evidence base. In Annex 1 we provide the template reporting form Tech Against Terrorism uses when reporting suspected TOWs to infrastructure providers

[1] https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/

TABLE OF CONTENTS

BACKGROUND: TERRORIST OPERATED WEBSITES

Definitions and current threat picture

A terrorist operated website (TOW) is a website operated by terrorist and/or violent extremist (TVE) entities with the aim of furthering the entity's strategic aims. Tech Against Terrorism identifies a site as a TOW if it meets one or both 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.[2]
- The website espouses or praises violent extremist ideologies, whether it be associated with a group, individual, or movement. In general, these websites are run by actors not yet designated as terrorists.[3]

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 discernible support for or links 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

At the time of writing, Tech Against Terrorism had identified 212 TOWs. A more detailed breakdown of a majority of these sites and the role they play in the online TVE propaganda eco-system is available in Tech Against Terrorism's report "The Threat of Terrorist and Violent Extremist Operated Websites",[4] published on 28 January 2022. To date, Tech Against Terrorism has facilitated the removal of 16 TOWs via engagement with infrastructure providers.

[2] Examples include sites that are run by members or supporters of actors including al-Qaeda, Islamic State, Atomwaffen Division or Blood and Honour.
[3] Examples include websites relating to actors such as Order of the Nine Angles and multiple violent neo-Nazi groups.
[4] https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/

RESPONDING TO TERRORIST OPERATED WEBSITE

Tech company types in scope

Generally, four types of web infrastructure providers should be engaged in disrupting TOWs:

1. Search engines[5]
2. Web hosting providers[6]
3. Domain Name System (DNS) registrars[7]
4. DNS registries[8]

Practical challenges associated with disrupting TOWs

There are several challenges and considerations associated with disrupting TOWs:

- **Assessing illegal content vs illegal website admins:** whilst hosting providers might act when there is evidence of illegal content, DNS registrars might instead need certainty that the actual site operator is part of an illegal entity, such as a terrorist group, before taking action. This presents challenges with regards to evidence basis for action since there may need to be some degree of certainty around the presumed identity and affiliation of website administrators.
- **Efficiency:** removed websites risk reappearing as mirrors hosted by other providers or DNS registrars, or re-appear hosted by providers with an ideological commitment to keeping websites hosting terrorist and/or violent extremist content online
- **Potential negative implications for freedom of expression:** there should be a high level of certainty of criminal and/or harmful activity to avoid undue takedown of legal and legitimate speech, and providers should provide appropriate course to redress

Current barriers to action

There are several barriers that currently complicate action on TOWs. The perhaps most significant barrier is the fact there are jurisdictional gaps between governments, within governments, and between governments and tech companies as to who should lead, request, and coordinate action on TOWs. Although some countries have legal mechanisms that in theory allow for action against TOWs,[9] it is not always clear what exact mandate governments have to support action on such sites. Similarly, infrastructure providers have limited guidance as to what actions they are required to take. To date, action against TOWs or hostile websites has, in the absence of a legal framework, been taken on the initiative of infrastructure providers themselves in line with their Terms of Service.

[5] Software systems designed to facilitate the identification of websites and content via search functions.
[6] 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
[7] 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
[8] Organisations managing top-level domains, setting guidelines for domain names, and working with DNS registrars to sell domain names
[9] For a summary of some current mitigation mechanisms, please see our report: https://www.techagainstterrorism.org/2022/01/28/report-the-threat-of-terrorist-and-violent-extremist-operated-websites/

Given the significant threat that TOWs constitute, there are several benefits to taking action to limit the prevalence of TOWs. Below we list some key benefits:

1. Disruption of key propaganda outlets
    a. Removed access to TOWs
    b. Breaking of previously shared URLs to TOWs[10]
2. Manageable removal campaigns: Whilst there is a risk of TOWs reappearing under new names or with different infrastructure providers, such reappearances will occur on a one-to-one ratio. This makes such a "whack-a-mole" effort comparatively more manageable than similar campaigns on social media platforms, where removal risk result in the multiplying of propaganda sources
3. Forcing increased effort and long-term migration from terrorists: Even if terrorist groups manage to re-establish their websites, disruptive pressure is in itself worthwhile as it might force terrorist groups to re-evaluate their presence on surface web platforms

[10] Due to the TVE groups prominent use of URL sharing via beacon and content aggregator channels, breaking URLs known TOWs can be instrumental in limit dissemination of TVE propaganda online.

OUR MITIGATION STRATEGY

Whilst awaiting strategic leadership from governments in developing a global TOW mitigation strategy, there is a need to work with infrastructure providers to facilitate action against TOWs. Such action should be based on improved engagement with web infrastructure providers to (where appropriate) encourage action, including but not limited to removal and/or suspension of services to a website.

Underlying principles

Engagement with web infrastructure should be based on the following principles:

- **Rule of law:** recommendations for action (including removal or suspension of service) should be underpinned by international legal consensus around the designated terrorist status of specific groups and actors
- **Freedom of expression:** all potential adverse impact on freedom of expression should be considered in line with the Tech Against Terrorism Pledge[11]
- **Evidence base:** all recommended action should be underpinned by evidence. Tech Against Terrorism only engages companies once we have a high degree of certainty that a website is operated by a terrorist group. All companies engaged will be provided a dossier (see Annex) based on open-source intelligence (OSINT)-based analysis and threat intelligence assessments to inform potential action
- **Procedural rigour:** all engagement with web infrastructure providers should occur whilst paying appropriate respect to process and ensure that companies are adequately informed
- **Transparency and accountability:** Tech Against Terrorism will encourage infrastructure providers to be transparent about their actions and allow for appropriate appeal and redress mechanisms in line with our guidelines on transparency reporting[12]
- **Safeguarding neutrality of key forums:** forums like ICANN should remain a neutral ground that is not subject to politicised debate regarding removal of specific websites
- **Suitability and proportionality:** DNS registrars should ideally avoid having to make content moderation decisions. However, should such action be necessary it should be proportionate and only occur after other options have been exhausted
- **Deconfliction:** engagement with infrastructure providers around mitigation of TOWs should be deconflicted with relevant law enforcement agencies

[11] https://www.techagainstterrorism.org/membership/pledge/
[12] https://transparency.techagainstterrorism.org/

Building capacity and assessing risk

It is important that collaborative mechanisms around capacity-building and knowledge sharing that have proved successful amongst other parts of the tech industry are scaled across infrastructure providers. To that end, Tech Against Terrorism prioritises outreach to infrastructure providers. This work is underpinned by the knowledge sharing and in-person training approach used in Tech Against Terrorism's Mentorship Programme, Knowledge Sharing Platform (KSP), global workshops, and webinars, and focusses on increasing awareness of terrorist use of the internet amongst infrastructure providers. This work is informed by our OSINT risk assessments of TOWs. This approach will complement the targeted actions specified below.

Threshold for action

Due to the potentially significant global freedom of expression impact of removing a website, the threshold for recommended action against a suspected TOW should be high. We suggest that all of the following criteria should be met before recommending action against TOWs:

1. Terrorist designation of the group / actor in question
   a. Definite case: international designation, either via the Consolidated United Nations Security Council Sanctions List or consensus in Five Eyes and EU designation
   b. Indefinite (but potentially warranted): national designation by democratic nation states
2. Strong evidence base that the suspected TOW is managed by:
   a. Terrorists
   b. Terrorist supporters
3. Strong evidence that the website's main purpose is to disseminate terrorist propaganda or otherwise benefit a terrorist group

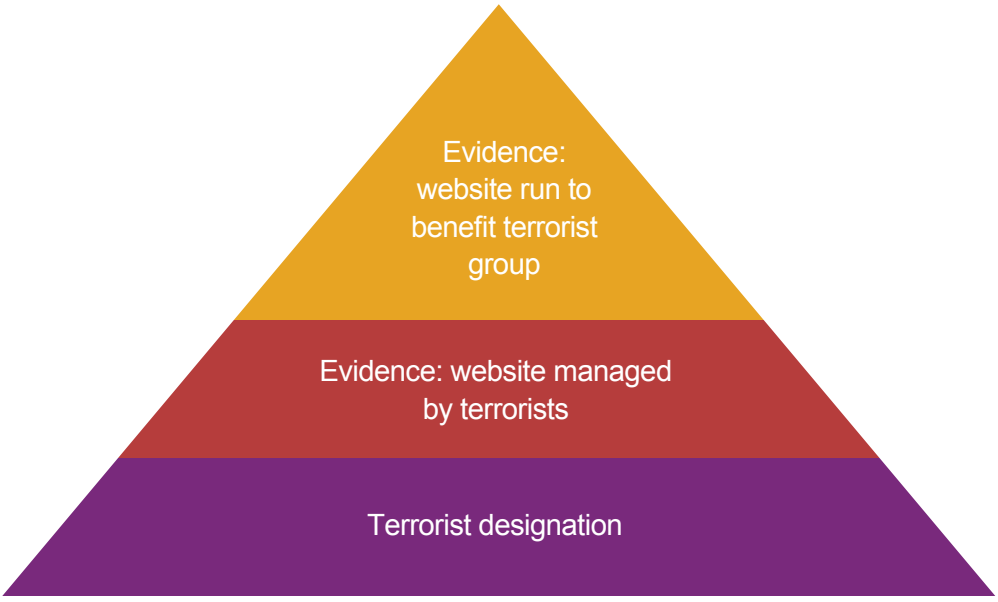

Figure 1: Threshold for action against TOWs.

Prioritisation framework: TOWs

Tech Against Terrorism is developing a framework to support prioritisation on which TOWs to alert infrastructure providers to as high-risk websites. This prioritisation framework will be based on our assessment of (in addition to the above):

1. The TOW's significance in a group's online propaganda dissemination eco-system
2. The amount of traffic to the site
3. The amount of outlinks leading to the site on core TVE entity beacon channels
4. The volume of illegal content hosted on the site
5. Presence of content related to, and in support of, ongoing or recently occurred terrorist attack

Prioritisation workflow: infrastructure providers

Based on the above principles, and in line with recommendations made by the Internet Jurisdiction Policy Network,[13] we suggest the following order of engagement with web infrastructure companies:

Workflow: segmented engagement with infrastructure provider

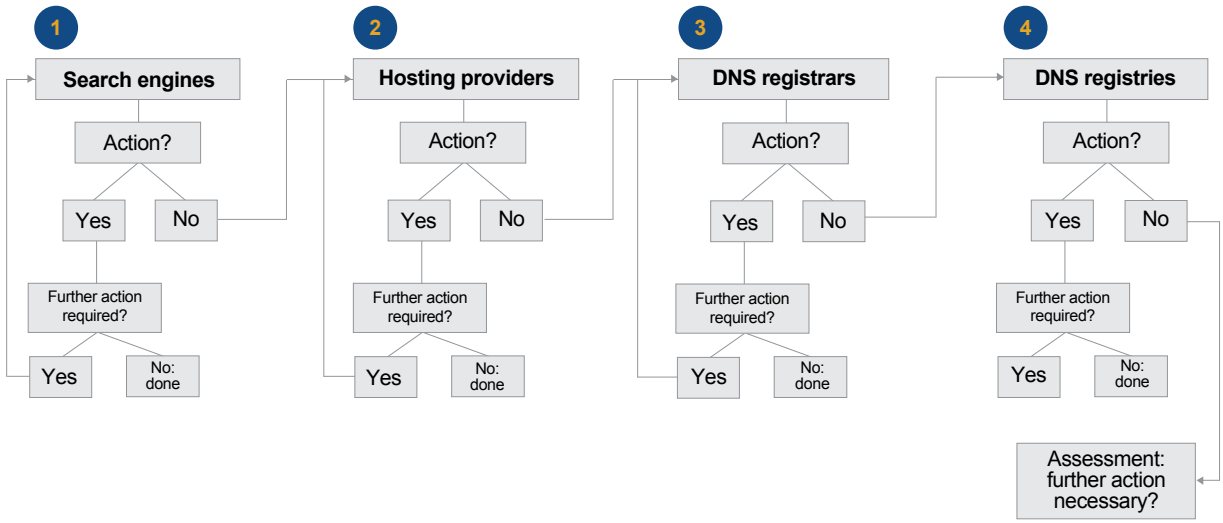

Figure 2: Segmented engagement with infrastructure providers

Since TOWs mainly concern terrorist content rather than technical abuse, search engines and web hosting providers should be engaged first. DNS registrars should be engaged either after initial (unsuccessful) engagement with search engines and hosting providers, or as part of a multilateral approach. Whilst the threshold for action should be high for each, it needs to be especially high on DNS level given the global disruptive effects of action. As a last resort, DNS registries should be engaged.

However, should cases be urgent or severe, we also recommend simultaneous engagement with infrastructure providers.

[13] https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-113-Due-Diligence-Guide-for-Notifiers.pdf

Workflow: Simultaneous engagement with infrastructure providers

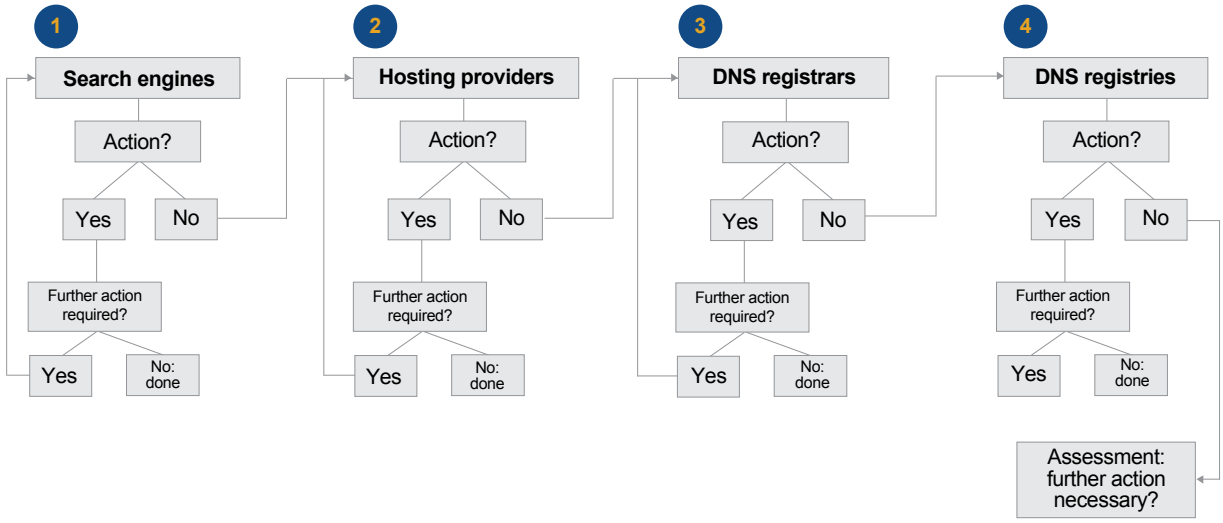

Figure 3: simultaneous engagement with infrastructure providers

Recommended actions per company type

Type	Recommended actions	Benefits of action on this level	Downsides of action on this level
Search engines	• Redirection to counternarrative resources • Deprioritise results for suspected TOWs • Remove all search results for suspected TOWs	• Decreases serendipitous discoverability • Arguably less freedom of expression impact than below alternatives	• Limited effect in decreasing de facto access to TOWs
Hosting providers	• Warning (to be issued to site operator) • Blocking or disruption of service • Suspension of service	• Restricts access to TOWs • Appropriate engagement level regarding terrorist content	• Risk of forcing displacement and migration to infrastructure companies committed to platforming TVE material
DNS registrars	• Removal of website • Locking of domain name • Redirection from domain name to counternarrative and/or educational resources	• Restricts discoverability of TOWs • Breaks existing URLs to TOWs	• Removal does not take website offline • Inappropriate level for content-related concerns
DNS registries	• Removal of website • Disciplinary action against registrar	• Restricts discoverability of TOWs • Breaks existing URLs to TOWs • Sends message to other registrars	• Removal does not take website offline • Inappropriate level for content-related concerns • Risk of politicisation of neutral forums

ANNEX

Annex 1. Template abuse report used by Tech Against Terrorism when alerting infrastructure companies to TOWs

Notice: terrorist operated website – [URL]

Date: [complete]
Domain: [complete]
IP Address: [complete]
Registrar: [complete]
Registry: [complete]
Host: [complete]

Key Information	
Threat summary	• Summary of key information about group operating it • Summary of website and its content • Summary of legal status of group • Note on recipient's terms of service, and how the site breaks this (if applicable).
Evidence summary	• Evidence to prove that the website is run by a proscribed/banned terrorist organisation, or by supporters of a banned/proscribed terrorist organisation • Does the content encourage violence, contain graphic violence, endorse a proscribed terrorist organisation, or encourage people to join a proscribed organisation? • Volume and nature of content stored there, and the likely intended purpose/function of the website. • Proportion of the content on the site that is illegal and/or terrorist/violent extremist • Assessment of impact of and/or threat posed by the website
Legal basis	• Designation by o UNSCL o EU o Five eyes o Democratic nation state national designation • Other relevant laws in democratic states/international organisations making the domain's contents/purpose illegal.
Due diligence [Applicable only to DNS Registrars/Registries]	Brief outline of previous actions – what has TAT done in advance of this report? This could include: Successful de-platforming of previous iterations of the domain. - (unsuccessful) reporting of domain to hosting providers. - Removal of site from search engine results - Blacklisting of domain

Suggested Action(s) [Delete as applicable]

[For hosting providers]

1.) Warning to site operator
2.) Blocking/disruption of service
3.) Suspension of service

[For DNS registrars/registries]

1.) Redirection from domain name to counter-narrative and/or educational resources
2.) Locking of domain name
3.) Removal of website

Anticipated Impact of Action

Example: "We acknowledge that the site is likely to reappear, given that its core infrastructure will not be affected. But given the threat posed by the domain, we consider this action to be proportionate, particularly when applied as part of a TaT's multilateral approach to tackling terrorist operated websites – blacklisting, removal from search engines, etc.

Removal of the site would (a) prevent terrorist actors from accessing content (b) prevent internal users from being exposed to the content (c) inhibit ability of X terrorist group to recruit, inflict fear, etc."

Supporting Evidence

[screenshot description]	[screenshot of website]
[screenshot description]	[screenshot of website]
[screenshot description]	[screenshot of website]
[screenshot description]	[screenshot of website]
[screenshot description]	[screenshot of links/references to website on third-party platforms, if applicable]

ANNEX 2. ENGAGEMENT STRATEGY PER COMPANY TYPE

Search engines: engagement strategy

Summary	
Threshold for engagement	Evidence of TOW being easily discoverable via search engine results.
Threshold for recommending specific action	Strong evidence of the site being operated by a designated terrorist group or hosting terrorist and/or violent extremist content.
Suggested approach	Reporting of suspected TOW by sharing of detailed dossier providing proof and with a clear request for action. Search engines should be engaged before hosting providers or as part of a joint approach. Should search engines not reply to the report it will be brought to hosting providers, a measure that search engines should be made aware of.
Recommended actions	• Deprioritise results for suspected TOWs • Remove all search results for suspected TOWs • Redirection from domain name to counternarrative and/or educational resources

Hosting providers: engagement strategy

Summary	
Threshold for engagement	Evidence of TOW and/or site storing terrorist content being hosted by the provider.
Threshold for recommending specific action	Strong evidence of the site being operated by a designated terrorist group.
Suggested approach	Reporting of suspected TOW by sharing of detailed dossier providing proof and with a clear request for action. Hosting providers should be engaged before DNS registrars or as part of a joint approach. Should hosting providers not reply to the report it will be brought to DNS registrars, a measure that hosting providers should be made aware of.
Recommended actions	• Warning (to be issued to site operator) • Blocking or disruption of service • Suspension of service

DNS registrars: engagement strategy

Summary	
Threshold for engagement	• Evidence of TOW and/or site storing terrorist content being hosted on a site that is registered to the registrar • Instances where hosting providers have failed to reply to requests
Threshold for recommending specific action	Strong evidence of the site being operated by a designated terrorist group.
Suggested approach	Reporting of suspected TOW by sharing of detailed dossier providing proof and with a clear request for action. DNS registrars should only be engaged following unsuccessful engagement with hosting providers. Should the registrar ignore the report the case will be brought to relevant registry. Recommended actions
Recommended actions	• Redirection from domain name to counternarrative and/or educational resources • Locking of domain name • Removal of website

Hosting providers: engagement strategy

Summary	
Threshold for engagement	• Evidence of TOW and/or site storing terrorist content being hosted on a site that is registered on a registrar within a registry's remit • Instances where hosting providers and DNS registrars have failed to reply to requests
Threshold for recommending specific action	Strong evidence of the site being operated by a designated terrorist group
Suggested approach	Reporting of suspected TOW by sharing of detailed dossier providing proof and with a clear request for action. DNS registries should only be engaged following unsuccessful engagement with hosting providers and DNS registrars.
Recommended actions	• Disciplinary action against member registrars