BACK TO THE FUTURE?

Twenty First Century Extremist and Terrorist Websites

Authored by Maura Conway and Seán Looney, Dublin City University, Swansea University, and VOX-Pol

Radicalisation Awareness Network
RAN Policy Support

Luxembourg: Publications Office of the European Union, 2021

INTRODUCTION

Online terrorism has been subject to significant change over the past twenty years. An appreciation of the roles of the Internet in terrorism was, like the Web itself, still nascent at the time of 9/11. An early focus on cyberterrorism was nevertheless, even then, giving way to a realisation that the Internet's affordances were already altering the extremism and terrorism landscape. Some of the earliest work in this area was on extremist and terrorist websites and their purposes.

Extremist and terrorist websites never really went away, they were just overlooked for a decade by researchers and others due to a not unwarranted narrowing of focus to social media platforms and, latterly, messaging applications and adjacent online spaces.

While there is less reliance on websites by extremists and terrorists than there once was, websites remain an important component of the contemporary online extremist and terrorist ecosystem(s) and could re-emerge more strongly with accelerated disruption of extremist and terrorist content and accounts by social media platforms and adjacent services unless providers further down 'the tech stack' take more concerted action.

This briefing seeks to restart research and discussion around the roles of websites in contemporary online extremism and terrorism.

The briefing opens by locating extremist and terrorist websites within an ecosystem framework. It follows-up by grappling with the question of what constitutes a 'terrorist website' and lays out a three-part categorisation that accounts for terrorist-operated websites, supporter sites, and ideologically adjacent sites.

This section includes description and discussion of eight websites from across the ideological spectrum chosen for analysis herein. These websites were the official sites of Hamas, the PKK, and the Taliban; three IS supporter sites, namely Elokab, I3lam, and Shine of Islam; and two ideologically adjacent sites: the Nordic Resistance Movement's official English language site and Daily Stormer.

The next section reviews the academic literature on extremist and terrorist sites.

The Analysis section, which takes-up the bulk of the report, addresses the content, purposes, and reach of our selected eight websites.

Also discussed in this section is the refusal of hosting or other crucial services, such as DDoS protection, by website providers, which has led to the disappearance—sometimes for a short period, sometimes more permanently—of some extremist and terrorist sites from the Web.

In the Conclusion, we sum-up our findings and point to the need for more research on the role of websites in contemporary extremist and terrorist online ecosystems and some of the directions this new work could take.

CONTEXT

THE UTILITY OF AN ECOSYSTEM APPROACH

Baele, Brace, and Coan (2020), in their conceptualisation of the far-right online ecosystem, point to how an ecosystem approach underlines the online far right's dynamism and multidimensionality.[1] Any given ecosystem, they say, is composed "of an ever-changing number of different components whose natures and interconnections are in constant evolution (as opposed to a static landscape made of a fixed number of well-defined objects)" (p.2).

Baele and colleagues go on to characterise the far-right ecosystem—but, in fact, this can apply to any extremist or terrorist online ecosystem—as comprising four key elements, each corresponding to a level of analysis: entities, communities, biotopes, and the whole network (p.3). The most important of these elements for our purposes here is the lowest level or most basic unit of analysis: 'entities.'

Entities are described Baele et al. (2020, 3) as "individual domains" and include what they refer to as "static websites," which are the focus of this report. Conceptualising these entities as part of an ecosystem requires exploration of their interdependencies too, however.

A focus on interdependencies brings us to Baele and colleagues' second level of analysis: 'communities' which, in line with network analysis, they understand as made-up of nodes connected together via links. Any extremist or terrorist online ecosystem can thus "be understood as a network made of a multitude of communities of linked entities" (p.4).

EXTREMIST AND TERRORIST WEBSITE TYPES

In a recent report for the industry-led Global Internet Forum to Counter Terrorism (GIFCT), Tech Against Terrorism (TaT) (2021) described terrorist-operated websites (TOWs) as "[w]ebsites that are run by terrorist groups or their supporters with the intended purpose of serving a terrorist group or network's interests." At the time of writing, in July 2021, TaT stated they were aware of 121 websites "suspected of being operated by terrorist actors" (p.15).

There are two components of 'terrorist websites,' the 'terrorist' part and the 'website' part. Agreement on the types of things that fall into either of these categories is not easily arrived at. Below, we begin by outlining our narrow conceptualisation of those entities known as 'websites' and follow-up by distinguishing between TOWs, supporter sites, and ideologically adjacent sites.

[1] Baele and colleagues are not the only extremism or terrorism researchers to have adopted an ecosystem approach in their work albeit their framework is the most well thought through. For more, see Awan, Hoskins, O'Loughlin, 2011; Clifford, 2018; Conway *et al*., 2020; Fisher, Prucha and Winterbotham, 2019; Macdonald *et al*., 2019.

What Constitutes a 'Website'?

The question of what types of online spaces generally fall into the category of 'website' is more complicated than it may first appear. Are social media platforms 'websites'? How about online discussion forums? Throughout the extremism and terrorism literature 'website' is used to refer to a wide range of types of online spaces, including not just forums, but also mainstream and fringe social media platforms, file sharing services, and video hosting services.

Baele et al. (2020) divide the entities level of their framework into two major categories: Web 1.0 and Web 2.0. Web 1.0 refers to the Internet prior to the development of social media platforms and other online spaces structured around the production and circulation of user generated content. On this analysis, Web 1.0 sites are run by an individual or team of administrators who dictate what content appears on a site.

Following from this, Web 1.0 sites include read-only sites but are not limited to them. Read-only static websites are becoming rare with an increasing number of Web 1.0 websites transforming into sophisticated multimedia hubs that embed various types of textual and audio-visual content (e.g., videos, podcasts). It is these Web 1.0 sites that this report examines.

A further way to distinguish Web 1.0 sites is by their levels of communication and interaction. While the just-described type websites are a means of communication for the extremists and terrorists in question, it is generally a largely one-way means of communication. The extent of user interaction may be the use of a 'contact us' section or an email address, which contrasts with highly interactive sites such as online discussion forums.

This report thus excludes forums, including generalised ones such as 'the chans' (e.g., 4chan, 8chan, etc.) (Zelenkauskaite *et al*., 2021; Crawford, Keen, and Suarez-Tangil, 2021), but also dedicated extreme right forums, such as Stormfront (Bowman-Grieve 2009; Gornishka, Rudinac, and Worring 2020; Hartzell, 2020; Kleinberg, van der Vegt, and Gill, 2021), Iron March and Fascist Forge (Benjamin and Knott, 2021; Scrivens, Wojciechowski, and Frank, 2021; Scrivens *et al*., 2021), and the range of jihadi forums (Zelin, 2013), all of which are covered elsewhere in the literature.

By contrast to Web 1.0, Web 2.0 is characterised by, among other things, platforms dedicated to online interaction and whose content is overwhelmingly multimedia and user generated. These include the major social media platforms (e.g., Facebook, Twitter, YouTube) where extremists and terrorists of all ideological leanings are subject to extensive takedown efforts, and more fringe social media (e.g., Bitchute, Gab, MeWe)—and messaging applications (e.g., Hoop, Telegram)—where extremists and terrorists have more freedom to act.

While these platforms may be used by extremist and terrorists, and some of the fringe platforms are owned and/or administered by extremists, these are not 'websites' as traditionally conceived but more accurately described as social media platforms or messaging applications. Thence they do not meet our definition of a website and are excluded from this report.

In this report therefore 'website' refers to a form of standalone, largely non-interactive, multimedia site. It thus excludes online discussions forums, social media platforms,

messaging applications, and the like. Neither are so-called 'Dark Web' (e.g., TOR) sites included but only those available on the surface Web.

Distinguishing Between Terrorist-operated Websites, Supporter Sites, and Ideologically Adjacent Sites

Terrorist-operated Websites (TOWs)

TOWs are sites that are expressly and officially affiliated with a terrorist group or movement. Older and more established terrorist groups are more likely to have official organisational websites than newer groups or movements.

TOWs are not limited to a specific ideology with left-wing ethno-nationalist groups like the Kurdistan Workers' Party (PKK), extreme-right groups like Blood and Honour, and violent Islamist groups like Hamas and Hizbollah all, at one time or another, maintaining official websites. In fact, some of these websites have been active for decades at this point.

Conway's (2005) chapter focused on the websites of groups appearing on the US State Department's list of Designated Foreign Terrorist Organisations; today a host of governments, including not just the US, but Canada, the UK, and others produce such lists, as do the EU and UN. Outside of the US, most have both a domestic and international focus. One way to establish whether a given site is a TOW or not is therefore to determine if it is run or officially claimed by a designated terrorist organisation.

There are two immediately apparent problems with this approach, however. First, terrorism designation lists have only recently begun to include extreme right groups. The first such proscription was of National Action by the UK government in December 2016 and a trickle of similar designations have been made since but are still relatively rare (see Table 1). None of the 21 organisations presently appearing on the EU list is extreme right in its orientation, for example.[2]

The second difficulty is that some such lists are highly political, including those of some democratic countries, and thus some designations have met with resistance within the international community. These include Russia's listing of 400 chapters of the Jehovah's Witnesses as terrorists (Friedlander, Albanese, and Castellum, 2021) and Israel's October 2021 designation of six Palestinian human rights and civil society groups (Krämer, 2021).

Reflecting these issues, the TOWs selected for description and analysis in this briefing were the official sites of Hamas, the PKK, and the Taliban. This broadly reflects the composition of a variety of terrorist group proscription lists, which are largely divided between violent Islamist, jihadi, and leftist organisations, with a cross-cutting ethnic-nationalist or nationalist separatist impetus also observable. These groups are all also designated as terrorist by more than one Western democratic country, along with either the EU or the UN.

[2] For the full EU listing, see *Council Implementing Regulation (EU) 2021/138 of 5 February, 2021 implementing Article 2(3) of Regulation (EC) No. 2580/2001* at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2021:043:FULL&from=en. See also, the Council of the EU's overview webpage 'EU Terrorist List' at https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist-list/#.

Table 1. Designation of Extreme Right Terrorist Groups by Democratic Countries and Supranational Organisations						
	UN	*EU*	*US*	*UK*	*Canada*	*Australia*
Blood and Honour	---	---	---	---	✓	---
National Action	---	---	---	✓	---	---
Combat 18	---	---	---	---	✓	---
Sonnenkrieg Division	---	---	---	✓	---	✓
Scottish Dawn	---	---	---	✓	---	---
National Socialist Anti-Capitalist Action	---	---	---	✓	---	---
System Resistance Network	---	---	---	✓	---	---
Feuerkrieg Division	---	---	---	✓	---	---
Atomwaffen Division	---	---	---	✓	✓	---
National Socialist Order	---	---	---	✓	✓	---
Russian Imperialist Movement	---	---	✓	---	✓	---
The Base	---	---	---	✓	✓	---
Proud Boys	---	---	---	---	✓	---
✓ = Designated terrorist group ✓ = Designated under synonym or umbrella group or by affiliation						
Source: Adapted from Terrorist Content Analytics Platform's (TCAP) 'Group Inclusion Policy' at https://www.terrorismanalytics.org/group-inclusion-policy.						

Founded in 1987, Hamas is designated a terrorist organisation by the EU and dozens of countries. It is also one of the Palestinian territories' two major political parties and governs more than two million people in the Gaza Strip, which is why some countries apply the terrorism label only to its military wing (i.e., Izz al-Din al-Qassam Brigades). Hamas has a lengthy online presence, with the now defunct hamasonline.com used to get their message out in the mid-2000s. It was Hamas' contemporary official English language website, **hamas.ps/en**, which was still operational in mid-October 2021, that was included for analysis here.

The Kurdistan Workers' Party (a.k.a. Kadek, Kongra-Gel), generally known by its Kurdish acronym PKK, is widely recognised as a terrorist organisation, including by the EU. The group was founded in 1978 on Marxist-Leninist ideology coupled with a separatist agenda. In its launch statement the PKK stated as its long-term objectives the liberation of Kurds scattered across Turkey, Syria, Iran, and Iraq and the formation of a "Greater Kurdistan." Conway included the PKK site kongra-gel.org, which is no longer operational, in her 2005 analysis. The site focused on here is **pkk-online.com**, which was still operational in mid-October 2021.

The United Nations (UN) designated the Taliban a terrorist organisation in 1999 due to their providing a haven for terrorists, including Osama Bin Laden. Surprisingly to many, the United States has never designated the Afghan Taliban as a foreign terrorist organisation nor do they appear on the EU designation list. The Taliban launched its original very basic website, www.taliban.com, in 1998. *Al-Emerah* (The Emirate), which came to be known as the official website of the Taliban, came online in 2005. It was made available in five languages: English, Arabic, Pashto, Dari, and Urdu. All five of the **Taliban websites went offline on 20 August, 2021**. The focus in this briefing is on **alemarahenglish.net**.[3]

[3] A cached copy of alemarahenglish.net from 16 August, 2021 can still be accessed via the Internet Archive's 'Wayback Machine,' which is at https://archive.org/web/.

Supporter Sites

Supporter sites are websites publicly claiming support for—and sometimes affiliation with—a terrorist group, but without being run directly by it.

It should be noted that, in some instances, it can be difficult to distinguish between official and supporter websites, especially when there is disagreement among a group's supporters as to a site's legitimacy and no official position taken by a group themselves on the matter.

Currently, the most prominent source of supporter websites are followers of so-called 'Islamic State' (IS). They represent attempts by IS supporters to establish online spaces, outside of social media and messaging applications, in which IS content can continue to be accessed.

These IS supporter sites can be difficult to substantively document as they are so often subject to takedown. Three of these sites are nonetheless presented here: **elokabe.de, i3lam.pm, and shineofislam.com**. At time of writing, all versions of the Elokab site, which cycled through numerous domain names and hosting companies, appeared unavailable. Using a Wayback Machine snapshot of elokabe.de dated 19 May, 2021 gives an insight as to its content, however. IS fan site i3lam.pm, which described itself as "specialized [*sic.*] in publishing everything released by the Islamic State in several languages," was also unavailable. Of the three IS fan sites referred to herein, Shine of Islam was the **only one of which that was still accessible in mid-October 2021**.

Ideologically Adjacent Sites

Ideologically adjacent or 'fellow traveller' websites are—sometimes expressly—unaffiliated with particular terrorist groups but are ideologically supportive of one or more such groups or movements and thus extremist in their orientation. In this report, discussion is restricted to ideologically adjacent sites that have shown explicit support for terrorism (i.e., Daily Stormer) or those of groups that have been assessed to have violent tendencies (i.e., NRM).

The number of websites falling into this ideologically adjacent category would increase exponentially were it to consider all websites with content having the possibility to inspire individuals to commit violent extremist or terrorist acts without explicit encouragement by the website.

Worth noting however is that increasing numbers of especially right-wing terrorist attackers have no group affiliation and, at most, can be described as active in the extreme right online movement or some-section(s) of it. Given this, restricting analysis of websites to the narrow categories of TOWs and supporter sites will ensure that influential extremist websites will be missed, which is why the category of ideologically adjacent websites is introduced herein.

The Nordic Resistance Movement (NRM) is a neo-Nazi organisation primarily based in Sweden but with branches in Norway, Finland, Denmark, and Iceland. Originally established as the Swedish Resistance Movement by a handful of activists in 1997, following the establishment of its associated divisions the organisation changed its name to NRM in 2016. Its declared goal is the formation of a white pan-Nordic state and it is an "organization that in principle embraces violent strategies, including terrorism, given the 'right' circumstances" (Bjørgo and Ravndal 2020, p.37). It is banned in Finland for activities "significantly contrary to law" (Associated Press, 2020).

The NRM maintains an extensive online presence, including two prominent websites, one in Swedish (www.nordfront.se) and another in English (**nordicresistancemovement.org**). The focus herein is on NRM's English language website, which acts as a central hub with outlinks at the top of the site to NRM's local branches' websites. It was **still live and accessible in mid-October 2021**.

Daily Stormer is a US-based Neo-Nazi website founded in 2013, which takes its name from the Nazi propaganda sheet *Der Sturmer*. The site is included here due to it having been **supportive of numerous acts of hate and terrorism**, including publishing an article mocking and abusing Heather Heyer, who was murdered by a right-wing extremist while protesting against the August 2017 'Unite the Right' rally in Charlottesville, Virginia, USA, and praising her killer. Unlike the other websites chosen for analysis in this briefing, Daily Stormer is not associated with or supportive of any particular group but encouraging of a variety of violent right-wing extremist ideas and causes. It is thus representative of an array of violent extreme right movement sites. Despite being knocked offline numerous times since 2017, Daily Stormer **remained live and accessible in mid-October 2021**.

Finally, for this section, it should be noted that the eight websites described and analysed in this briefing were chosen as **illustrative cases**. A much larger scale study is necessary in order to begin to make generalisations about the roles of different website types in contemporary online extremist and terrorist ecosystems.

PREVIOUS WORK

'HISTORICAL' AND NEW RESEARCH ON EXTREMIST AND TERRORIST WEBSITES

The bulk of available research on extremist and terrorist websites is from the mid-2000s and thus could be fairly described as 'historical' given the pace of change of the Internet. Having said this, static or traditional websites have many of the same basic frameworks today as they did ten to fifteen years ago, so it is **suggested that this 'old' work not be dismissed out of hand**. This older research includes work on a wide variety of extremist and terrorist groups' sites.

Conway's 2005 chapter examined the websites of groups from across the ideological spectrum appearing on the US State Department's listing of Designated Foreign Terrorist Organisations, including Aum Shinrikyo, FARC, the PKK, ETA, and the Shining Path. She found that the **TOWs she studied ran the gamut from "glitzy" and regularly updated to dull and outdated**. In the same year, Reid et al. (2005) published an article with a narrower focus on the content and linking activity of Jihadi websites.

Even earlier work by Weimann (2004), Tsfati and Weimann (2002), and Elison (2000) shares this predominant focus on violent jihadism. Seib and Janbek's later book, *Global Terrorism and the New Media: The Post-Al Qaeda Generation* (2011), also provides an overview of the content of terrorist websites, again largely violent jihadist groups as signalled in the title.

This is not to say that this earlier work ignored right-wing extremist sites. Caiani and Parenti did **extensive work on the European online extreme right**, including social network and content analysis of Italian extreme right websites, which found an extensive network of websites connecting extreme right political parties, street movements, and neo-Nazi groups (2009). They also produced a book-length comparative analysis of *European and American Extreme Right Groups and the Internet* (2013).

An almost decade-long lull in research on extremist and terrorist sites followed. It can be explained by the shift from Web 1.0 to Web 2.0 and a concomitant shift by extremists and terrorists to the newer online spaces characteristic of the latter, especially social media platforms. Worth mentioning here too is the 'real world' terrorist activity of first al-Qaeda and later so-called 'Islamic State' (IS) that together with their significant online presences—especially, as regards IS, their social media presence—caused a not inappropriate narrowing of many online terrorism researchers' focus to solely these.

An uptick in research on extremist and terrorist websites is again discernible, however. This renewed focus on websites stems at least partially from ecosystem studies that took as their starting points social media platforms, especially Twitter, and analysed outlinking to other online spaces by a variety of extremist and terrorist users and their supporters, which turned-up enough links to websites to be noteworthy.

Examples of such inductive studies include Conway *et al*.'s (2019) analysis of jihadi supporters' patterns of Twitter outlinking that showed official Taliban websites to be popular destinations (p.153) and follow-up research that found the overall Syrian jihadi online ecology "heavily **dominated by social media platforms, but with traditional websites playing a not insignificant role**" (Conway et al., 2021, p.9) and these being predominantly news sites, including those of major outlets (e.g., Al-Jazeera, BBC, RT, The Guardian) (Conway *et al*., 2021, pp's 11-12).

Methodologically similar studies, also with a geographical focus (i.e., mapping the online extremist ecosystem of a specific country), have had analogous results. For example, Comerford, Guhl, and Miller's 2021 report for ISD on the New Zealand extreme right's online ecosystem found that extremist activity was scattered across ten major platforms (i.e., Facebook, Twitter, Telegram, Reddit, YouTube, 4Chan, Gab, Parler, Discord, Bitchute), as well as a number of what they termed "standalone websites" that were left unidentified (p.10; see also p.6).

Other relevant work with a geographic concentration includes Froio's (2018) analysis of the official websites of French far-right organisations to determine how they framed Islam and France's Muslim population. The findings turned-up links to the websites of a range of non-French organisations, such as the English Defence League, *Casa Pound Italia*, and *Vlaams Belang*.

Bouchard et al. (2020) examined the social structure of extremist websites. Their work has a rare focus on more left-wing extremist and terrorist groups such as FARC and the PFLP, as well as eco-extremist groups such as Earth First! and the Animal Liberation Front (Bouchard et al., 2020). Earlier work by the same authors (Davies et al. 2015) had a similar emphasis on websites and was even more ideologically wide-ranging. It analysed the presence of recruitment content on not only left-wing and eco-extremist but also right-wing extremist sites, finding that the Earth First!, Animal Liberation Front, Aryan Nations, and KKK websites were **heavily oriented towards recruitment**.

Thomas' (2021) study for ISD of 100 far right, Neo-Nazi, and white nationalist sites also has a unique focus, in this case on the tools, technologies, and services that right-wing extremists are using to build and maintain their websites. Key findings were that Cloudflare was used by almost half (46) of the sites included in the data and Google Analytics by over a third (35), **pointing to the continued importance of mainstream providers in the extreme right online ecosystem**.

Extremist and terrorist **websites' reach** is an understudied issue. Guhl, Ebner, and Rau's (2020) report on Germany's far-right ecosystem, also for ISD, found that alternative media websites, which amplify and promote extreme far right messaging and propaganda, did not garner large audiences, with their reach being roughly 3% of the German population (p.42). Baele et al. (2020) found that some obscure right-wing extremist sites they analysed had only a handful of visitors (p.6).

On the other hand, a forthcoming report by Macdonald et al. (2021), for the Resolve Network, focusing on the Twitter outlinking activity of explicitly right-wing extremist followers of Germany's *Alternative fur Deutschland* (AfD) and France's *Rassemblement National* (RN) again found websites to be a core node that, when disaggregated, was **dominated by news sites**, both far-right alternative media sites and those of mainstream news outlets.[4]

A key difference between this new research and older work is that much of the older work focused on TOWs while newer work, reflecting changes in both Internet infrastructure and the workings of contemporary extremism and terrorism, surfaces a variety of website types, such as the foregoing alternative media sites.

[4] For additional recent work on far-right news websites see, for example, Heft *et al*., 2021 ; ISD, 2020.

ANALYSIS

Websites remain a core component of the contemporary Web. Every major actor, whether commercial, governmental, educational, civic, or otherwise, maintains a website that acts as its public face. Even social media companies have corporate websites.[5] As with these other organisations, extremists' and terrorists' websites are **effectively their public faces**.

This section supplies an overview of the workings of contemporary extremist and terrorist websites by focusing on the nature and purposes of the content appearing on them, the finance generation opportunities apparent on the sites, aspects of the websites' design, their audience reach, and the disappearance of some of them due to refusal of service, each of which is discussed separately below and illustrated with reference to our eight case study sites.

WEBSITE CONTENT AND PURPOSES

This section employs the framework devised by Davies et al (2015) to determine the levels of extremism of the selected websites and whether the sites were being used for recruitment.

Recruitment, on this analysis, refers to a broad range of actions encouraged by the websites, including promotion of group events and activities, recruitment to a list of group members or sympathisers, raising awareness of the group, and engaging broad support for its activities (Davies et al, 2015, p.105).

Determination of websites' extremism was on the basis of the levels of violence manifested in the posted content, including imagery or videos demonstrating acts of violence or text expressing violence towards or calling for violence against some group of people or the combination of these.

Davies et al's (2015) four-level website extremism scale is outlined in Table 2. It examines whether the websites actively encouraged visitors to join the cause. A website was considered 'active' if it explicitly sought to elicit participation or to motivate users to action. 'Passive' sites, on the other hand, were those which merely provided information on a group and/or cause, without engaging directly with visitors on what they could do to support it.

Table 2. Website Violence and Recruitment Scale		
	Violent	Non-Violent
Active	Level 4 Call-to-Violence	Level 2 Join-the-Cause
Passive	Level 3 Displays-of-Violence	Level 1 Fact-based

Level 1 websites were informational only, with this information avoiding clear presentation of violence and/or the use of hate speech. Level 2 websites also avoided presentation of violence but encouraged users to actively support the group and/or cause. Level 3 websites presented material of a violent nature without explicitly encouraging individuals to support the cause or take direct action. Level 4

[5] See, for example https://about.facebook.com/.

websites actively encouraged individuals to support the cause, including violent actions (Davies et al., 2015, p.116).

Table 3. Website Recruitment Scoring Scale	
Score	Recruitment Presence
0	None
1	Passive
2	Indirect Action
3	Active

Incorporated into this determination was a 0 to 3 scale utilised to score the degree to which the websites actively encouraged action on the part of users (see Table 3). A website which scored a 0 displayed no materials relevant to recruiting. A score of 1 on the scale pointed to the presence of efforts to pique the curiosity of site users, such as the provision of public discussion forums or opportunities to subscribe to newsletters or magazines. A score of 2 referred to the encouragement of 'indirect action,' such as donating to the group or cause. Finally, a score of 3 indicated active recruitment, including announcements and invitations to events up to overt calls to 'real world' violent action (Davies et al, 2015, p.117).

The application of this framework to the eight websites discussed herein resulted in the TOWs scoring lowest and the IS supporter sites highest. Table 4 supplies an overview of our findings, which are discussed further below, starting with the least extreme sites and going to the most extreme.

Table 4. Extremism, Recruitment, and Overall Scores for Selected Websites				
Website	*Website Type*	*Extremism Scale*	*Recruitment Scale*	*Overall Score*
Hamas	TOW	1	0	1
PKK	TOW	1 – 2	0	1 – 2
Taliban	TOW	1 – 2	0	1 – 2
Daily Stormer	Ideologically Adjacent	3	2	5
NRM	Ideologically Adjacent	3	3	6
IS	Supporter	4	4	8

The Hamas site was divided into eight sections: 'News,' 'Statements,' 'Palestine,' 'Occupation Crimes,' 'Opinion,' 'Gallery,' 'Hamas,' and 'Contact Us.' Hamas was the only one of our case study sites to have an extensive 'About Us' section (i.e., linked from 'Hamas' section). In it the group primarily defined itself as a Palestinian national movement rather than an Islamist group.

In terms of the website extremism scale the Hamas site was judged a Level 1 website (i.e., more passive than active). While the site was overall dedicated to the Israel-Palestine conflict, it did not explicitly encourage users to take action or support their cause.

For example, the 'Occupation Crimes' section of the Hamas site consisted of articles documenting the ongoing situation in Gaza. Examples included 'UNICEF: "Israel" Killed 9 Children, Wounded 556 Others in Two Months,' 'Rights Groups: Israeli Occupation Detained 471 Palestinian Children in May,' and "Hamas: Israeli Colonists are Accomplices in Killing Palestinian Civilians in the West Bank.'

This was not new for Hamas whose previous website(s) also contained text, images, and video detailing similar events. These examples also draw attention the utilisation of reporting by named (e.g., UNICEF) and unnamed (e.g., "Rights Groups") organisations by Hamas to verify their assertions.

While this was undoubtedly a one-sided depiction of the conflict, the articles contained within this section and others did not call for acts of violence, protest, or any type of support in response. The Hamas site also didn't feature depictions of violence such as

images or videos of violence supporting their cause or examples of speech encouraging violence against a specific group or groups.

Similarly, in terms of the recruitment scale the Hamas website had no recruiting presence. There were links to Hamas' social media accounts and a 'Contact Us' page, but no means to donate and no newsletters, magazines, or embedded discussion forums, placing the site somewhere between 0 and 1 on the scale.

Images of the group's imprisoned leader, Abdullah Öcalan (b.1949), featured prominently on the PKK site, including in a banner at the top of its homepage (see Figure 1). PKK 'martyrs' were also memorialised on the site with photographs, including of females. There was also a tab labelled 'Women' in each language version of the site. Albeit this was only populated with content in the Kurdish and Turkish versions, it is reflective of broad leftist ideology and values around gender equality.

Figure 1 - Screenshot of Landing Page of English-language Version of PKK Website

Similarly to the Hamas website, the PKK site was more passive than active in terms of the website extremism scale. Overall, the site was assessed to be between Levels 1 and 2 on the scale. It was focused on emphasising the democratic and people-centred character of the PKK and the "murderous" and "fascist" nature of the Turkish government.

While 'martyrs' were celebrated on the site there was no explicit encouragement for users to martyr themselves. There was more violent content appearing on the PKK site than on the Hamas site although this was limited to 'Gallery' images of guerrilla fighters aiming and posing with rifles rather than actual depictions of violence.

In terms of violence-supporting text, this was generalised and directed at the "fascist Turkish state." For example, an article titled 'To the Patriotic People of Kurdistan and the Demokratic [sic.] Public' signed by the PKK Solidarity Committee with the Families of Martyrs, which stated: "We will avenge all our martyrs of the revolution."

In terms of the recruitment scale the PKK scored a 0, as there was even less of a presence of recruiting activity than on the Hamas site. The PKK site showed no means of donating to their cause, no means of contacting the group, no newsletters to subscribe to, and no social media outlinks.

The trend among the TOWs to downplay their own violence, which was overwhelmingly framed as retaliatory, and instead showcase what they viewed as the crimes of their enemies extended also to the Taliban website.

The alemarahenglish.net site consistently highlighted actions of the US military such as drone strikes and bombings. In an article describing a 27 July 2021 drone strike the US is described as a terrorist and the Afghanistan government its puppet. The site also had a monthly feature detailing 'War Crimes' by the US and the Afghan government with each day detailing a different "crime." The nature of this content would place the website between Levels 1 and 2 on the extremism scale.

Another purpose of the Taliban site was to present themselves, even before their August 2021 takeover of the country, as the legitimate government of Afghanistan. Reflecting this, the site highlighted Commissions pertaining to issues such as 'Agriculture, Livestock, Ushr, and Zakat,' 'Power Distribution,' 'Affairs of the Indigent, Orphans and Disabled,' and 'Prevention of Civilian Casualties and Complaints.' Information on most of these Commissions was accompanied by a phone number and email address.

In terms of the website extremism scale therefore, the Taliban site was 'active' in the sense that it encouraged users to contact them, but with the express aim of presenting themselves as rightfully governing and contactable for those purposes. The Taliban site, like those of Hamas and the PKK, was not aimed at recruiting users into the group or encouraging material—including financial—support, giving the site a 0 on the recruitment scale.

Daily Stormer's homepage was divided in a similar fashion to the news websites it apes, with sub-sections labelled 'US,' 'World,' 'Society,' and 'Insight.' The 'news' purveyed was overwhelmingly anti people of colour, Muslims, Jews, immigrants, refugees, women, and the LGBTQI+ community. Its content was virulently anti-Semitic and racist, with prominent sections on the 'Jewish Problem' and 'Race War.' Very high levels of misogyny and hatred towards transgender people were also displayed. This places the site on Level 3 of the website extremism scale.

In terms of recruitment the Daily Stormer site scored a 2. At time of writing, the site sought to present itself as non-violent and most explicitly encouraged action in the form of pushing users to donate to the site's upkeep. In the past however, it unambiguously stimulated direct personal 'real world' action. Not only did the site's founder Andrew Anglin post articles on the site mocking and abusing Heather Heyer, the woman murdered at the 'Unite the Right' event, but he followed these up with articles calling for the harassment of mourners at Ms. Heyer's funeral.

This goes some way to explaining the disclaimer appearing at the bottom of the Daily Stormer homepage:

"We here at the Daily Stormer are opposed to violence. We seek revolution through the education of the masses. When the information is available to the people, systemic change will be inevitable

and unavoidable. Anyone suggesting or promoting violence in the comments section will be immediately banned permanently."

The above was probably added for at least two reasons. First, it may have been necessary to source a website hosting company post-Charlottesville and, second, at around the time the text first appeared on the site in 2017, Anglin was also embroiled in a court case that hinged on various calls to action he made on the site in 2016. The Jewish woman who, along with her family, was the victim of the 2016 'troll storm' has since won a $14 million judgement against Anglin.

In a 2018 episode of the Nordic Resistance Movement's podcast 'More than Words,' the NRM member host stated that he wanted "to be the friendly face of National Socialism. I want to be part of normalising this ideology so that we can all show our faces in the streets without those fucking idiots throwing rocks at us. That is my main goal" (Askanius, 2021, p.17).

In keeping with its overall goal to sanitise Nazism (Bjørgo and Ravndal, 2020), the NRM website's 'Activism' page detailed its presence at peaceful protests, engagement in awareness campaigns, and propaganda offensives (i.e., postering, stickering) rather than detailing any violent action. In addition, its 'Social Activity' page predominantly featured group outdoor activities, including hiking, mountain climbing, abseiling, canoeing, and camping rather than more explicitly training activities.

While the NRM website avoided explicitly violent imagery, it did contain text expressing violent ideas. An example was the item titled 'Simon Lindberg's Thoughts on the Mosque Shootings,' in which the NRM leader, Lindberg, justified the 2019 Christchurch terrorist attack by reference to falling white birth rates and violent jihadist terrorism, even though Lindberg described the shooting itself as "counter-productive." Endorsements of hate and terrorism such as these caused the NRM website to be scored as 3 on the extremism scale.

At its core, the NRM website was dedicated to encouraging users to join its cause and was thus more active than passive in terms of the website recruitment scale. Five tabs, 'Resistance News,' 'Radio,' 'Media,' 'Ideology,' and 'International Comrades,' were prominently displayed across the top of the Nordic Resistance website homepage (see Figure 2). The 'Resistance News' section of the site was subdivided into the already-described 'Activism,' and 'Social Activity,' along with 'Events' and 'Written Interviews.' The International Comrades section contained news about interactions with and the activities of ideologically commensurate groups Europe-wide, including Greece's Golden Dawn, Germany's Der Dritte Weg, and Italy's CasaPound.

'Ideology' featured not just the NRM manifesto 'Our Path: New Politics for a New Time,' but a series of articles encouraging readers to join the extreme right movement by using rhetoric such as "Structural anti-Whiteness has claimed another victim. Have you had enough yet, White man?" and "the time to take your rightful place in the struggle is now, and not a moment later."

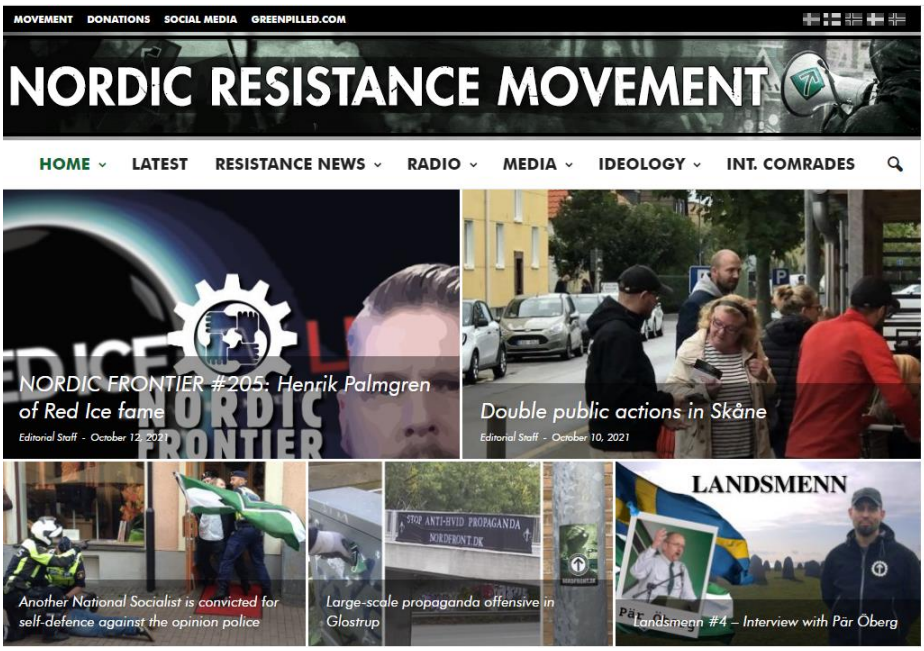

Figure 2 - Screenshot of Homepage of NRM Website

In addition, the site contained direct invitations for readers to join upcoming demonstrations and other events, as well as social activities. The site also encouraged readers to donate and otherwise support the movement financially, submit articles for posting on the website, and to organise themselves. The site catered to those who were outside of the Nordic region too, by offering to put readers in contact with "nationalistic organisations around the world." Together, these caused the NRM site to score 3 on the recruitment scale.

Unlike the ideologically adjacent type sites, the analysed supporter sites made no effort to shy away from violence. For example, the Arabic-language only Elokab site had a header image displaying IS forces invading the US and the IS flag superimposed on the North American landmass. The bulk of the Ekolabe.de homepage was dedicated to showcasing a variety of types of IS content, including videos, magazines, and posters that, per Conway's 2005 analysis had a heavy emphasis on "delivering threats, and disseminating horrific images" (p.190).

Prior to its takedown, shineofislam.com was very similar in design to the various iterations of the Elokab site although it presented itself as a scientific and educational advocacy site. To this end, the site featured a section labelled 'Jihad Scholars,' which consisted of a series of sermons, an education section with content about Sharia jurisprudence for men and women, 'Muslim Belief,' 'Arabic Lessons,' and 'Geography.'

Nonetheless, the Shine of Islam site also featured audio files of popular IS nashid and speeches by IS leaders and shared issues of IS's weekly al-Naba newsletter, but not issues of IS's Dabiq or Rumiyah magazines.

I3lam published and shared IS materials in Arabic, English, French, Indonesian, Persian, Urdu, Russian, Turkish, Pashto, Kurdish, Hindi, Bengali, Dhivehi, Amharic, Swahili, Somali, and Uzbek, but with some languages plainly having more content than others.

For example, the English portion of the I3lam site was broken down into categories such as 'Khilafa News,' 'Naba Newspaper,' 'Translated Videos,' 'Al-Hayat Media Center,' 'Dabiq Magazine,' 'Rumiyah Magazine,' and 'Ansar Production.' The Arabic, French, Indonesian, Persian, Urdu, Russian, and Turkish sections were similarly categorised.

The primary purpose of the IS supporter sites examined was the collation and easy provision of access to official IS propaganda content. The hyper violent nature of this content and the direct calls to violent action against specified groups peppered throughout ensured that these websites scored 4 on both the extremism and recruitment scales.

Overall, many of the same types of content as identified by Conway in her 2005 analysis were observable on the contemporary TOWs for largely the same purposes: portrayal of the group as the legitimate representatives of the people against a vicious enemy, generally a state or its representatives, and any violence on the part of the group as necessary and proportionate counter violence. Explicit violence, whether in text or images, was shied away from and recruitment activity was non-existent.

The ideologically adjacent sites sampled here were both extreme-right in their orientation and both sought to present themselves as non-violent. With its array of ideological content, including presentation of its manifesto, the NRM shared some similarities with the TOWs. The Daily Stormer, on the other hand, presented itself as more of an alternative news site, including via its structuring. The NRM site was judged to be more active in its recruitment activity than the Daily Stormer, which is probably explainable by its being a membership organisation rather than what might be termed a 'movement website' like Daily Stormer.

Similar to the ideologically adjacent website cases, the supporter websites described and discussed in this briefing were associated with, in this a case, a single group, IS. These sites therefore had a high level of resemblance, including hosting large amounts of extraordinarily violent content and having recruitment as a core purpose.

ONLINE FINANCING AND PAYMENTS

Efforts by extremists and terrorists to raise funds for their activities via the Internet are longstanding. **Five of the eight websites we studied had a financing or payments aspect.** These took two main forms: **requests for financial contributions and sale of merchandise.**

No financing, fundraising, or payment links of any kind were present on the Taliban, Hamas, or PKK websites.

Earlier studies of terrorist websites found some soliciting financial contributions, but none providing online donation facilities, such as a credit card payment facility (Conway 2005). **Changes in online payment options** means that this is no longer the case however, with extremists and terrorists moving toward the use of cryptocurrency for online fundraising.

The Nordic Resistance website's 'Donation' page lists cash, electronic transfer, and an **extensive list of crypto currencies** the group can accept, including Bitcoin, Ethereum,

Litecoin, and Monero. At least one reason that NRM accepts cryptocurrency donations is, as pointed out on the same page, that the Nordic countries have terminated their bank accounts (see also Europol 2021).

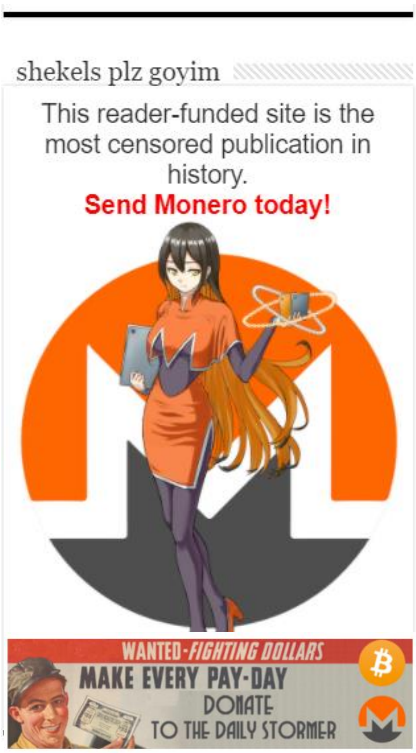

Figure 3 - Daily Stormer Adverts Soliciting Cryptocurrency Contributions

Immediately apparent on the Daily Stormer home page were requests for users to donate to the site's upkeep via donations of Bitcoin and Monero. One such request shows the Bitcoin symbol and text reading "Wanted – Fighting Dollars – Make Every Pay-Day – Donate to the Daily Stormer," another shows the Monero symbol with a cartoon/anime girl and text reading "shekels plz goyim [sic.]. This reader-funded site is the most censored publication in history – Send Monero today!" (see Figure 3).

Both the Elokab.de and Shine of Islam site included broken links calling for **contributions to support the continued publication of the websites** too.

The bottom of the i3lam.pm contained a 'Donate' link with the Bitcoin logo showing. Clicking on the link led to a page stating "[t]o provide financial support to the I'lam Foundation (Munasir Foundation), contact the following account on the Telegram app," followed by a link to a Telegram channel. This channel did not require an invitation to join and the user was last online within a day, but there were no posts in it.

The online sale of merchandise is another way to raise money, but of the eight sites we reviewed, only the NRM site had this option. More accurately, the tab bar at the top of the NRM site had a link to Greenpilled.com, which appeared to be based in Sweden, and described itself as "a webshop selling products related to the national struggle in the nordic [*sic*.] countries, but also to the entire rest of the world." These products included Scandinavian-language e-books, clothing, posters, banners, and coffee mugs.

The predominance of Bitcoin and other cryptocurrency points to a change in the online ecosystem(s) rather than innovation by the extremists and terrorists operating these websites. As Internet users generally become more accustomed to crypto currency payment, it was to be expected that extremists and terrorists would as well. Some crypto currencies, such as **Monero, which prides itself on its total privacy**, provide excellent means for extremists and terrorists of all ideological leanings to fundraise.

WEB DESIGN AND SOPHISTICATION

In her 2005 TOW study, Conway discussed not just the examined websites' content and purposes but also categorised them in terms of their sophistication, which she divided into six basic components: presentation and appearance, accessibility, navigability, freshness, and visibility. In this section, we rank our eight case study sites using the same criteria.

Presentation and appearance are divided into two sub-categories: flashiness (graphics emphasis) and dynamism (multimedia properties). The second component is accessibility; **high levels of flashiness and dynamism will be undermined if a site is offline**, takes a long time to load, and various features and/or pages are inaccessible.

Third, navigability is an important component of any site. A site that is easy to move around and makes it simple to locate particular information communicates its message more effectively. Fourth, freshness is considered key to effective content delivery. Sites that are regularly updated will create more interest than those that are not. Finally, visibility refers to how easy a site is to locate, as **a site that is not visible on the Web is failing to deliver its contents**.

Taking this approach, **Nordic Resistance had the most sophisticated website of the eight sampled here** (see Figure 2). In terms of appearance and presentation, the site was a modern multimedia website, including videos and podcasts, divided into broad sections with modern graphics, and large easy to read text overlay on images. The site had not been banned or blocked and was thus easily accessible and was simple to navigate, including having a working search function.

In terms of freshness, the NRM site was updated on a near daily basis. As regards visibility, the site could be found via Google search using the group's name. The 'Radio' section of the site linked various NRM-produced podcasts, including *Mer an Ord* (More Than Words), which focused on the daily activism of the group's 'foot soldiers' and *Ledarperspektiv*, which was dedicated to one-way, top-down distribution to listeners of NRM's leaders' perspectives.

NRM's English language podcast, Nordic Frontier, reached its 198th episode in August 2021. The content of these podcasts was sanitised to dodge allegations of illegal hate speech and carefully edited to avoid being removed. For example, expressions such as 'heiling' (i.e., Nazi-saluting) were removed in post-production using beeps (Askanius 2019, p.29). The 'Media' section of the site provided excerpts from the podcasts in video form, usually in the form of an embedded Odysee video.

Conway (2005) assessed the Hamas site to be the "flashiest" of the websites she studied, due to its heavy reliance on graphics; it also received a high "Multimedia/Dynamism" rating (p.196). Given Conway's (2005) findings, it is perhaps unsurprising to find that Hamas' contemporary English language website, hamas.ps/en/, was similarly sophisticated, with a multimedia site structure, large easy to scan images and articles, a search function, and new articles uploaded daily. It too was locatable via Google search.

The Hamas website was the only one of the eight sites introduced here with a Contact Us page. The page itself was a standard form with fields for 'Name,' 'Email,' 'Subject, 'and 'Text.' There was also an effort at social media outreach. One of the larger banners on the Hamas website was for the official Hamas Telegram channel, including a QR code linking directly to it (see Figure 4).

Six buttons for Facebook, Twitter, Instagram, YouTube, WhatsApp, and Telegram appeared on the side of the Hamas homepage (see Figure 4). However, the Facebook, Twitter, and YouTube buttons redirected to the same homepage likely owing to the accounts having been removed from the respective platforms.

Somewhat surprisingly, the Hamas Instagram page (i.e., hamasmovement) was active at time of writing, although with only 19 posts and 14 followers, which suggests that it was short-lived. The WhatsApp and Telegram links both led to a joining page, neither of which appeared to require invitations to join.

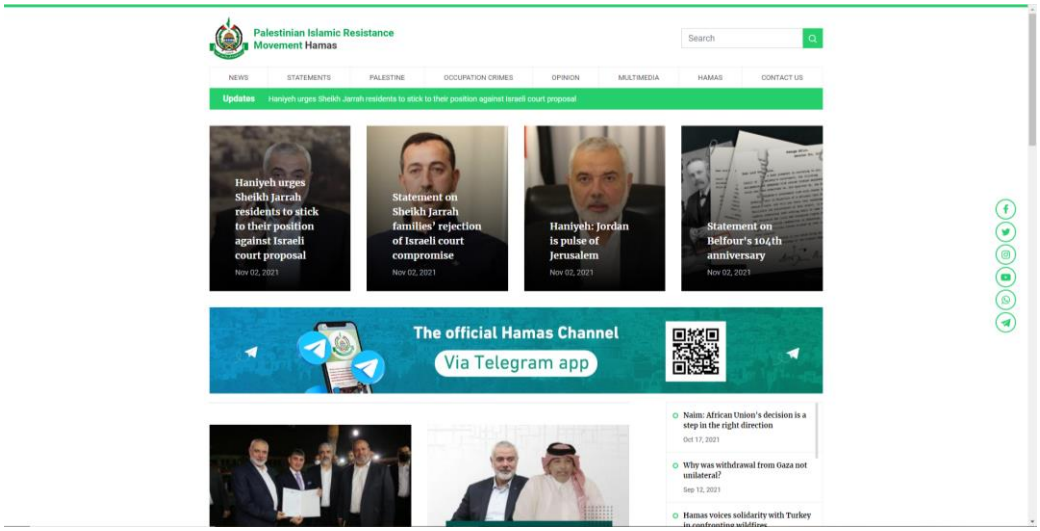

Figure 4 - Screenshot of Homepage of Hamas' English-language Website

Prior to its takedown, the Taliban website was of a similar level of sophistication to the Hamas site. Although its graphics were of a slightly lower quality, this was compensated for through the featuring of video content reporting on the military actions of the Taliban and its enemies.

Prominent on the Taliban site too were the Twitter account handles of three spokespeople for the group: Zabehulah Mujahid (@Zabehulah_M33; 403.9K followers), Qari Yousef Ahmadi (@QyAhmadi21; 81K followers), and Dr. Muhammed Naeem (@IeaOffice; 253.1K followers).

Unlike Facebook and a variety of other social media companies, Twitter took the decision to allow Taliban accounts and content to remain on their platform unless they explicitly contravened the company's ToS. All three mentioned accounts were still active on Twitter in mid-October 2021.

Worth noting here too is the difficulty in accurately determining levels of Internet access and use in Afghanistan. The World Bank's most recent data from 2017 determined only 11.4% of the population were Internet users (Thorbecke, 2021), but the Asia Foundation stated that in 2018 c.40 percent of Afghan households had access to the Internet (Brooking 2021). Regardless, given the low level of even local language literacy levels in Afghanistan, the target audience of the Taliban's English-language—and also Arabic-language—site was largely outside of the country.

Daily Stormer' web design was rudimentary. Like the many low-quality news and opinion sites of the 2010s that it was copying, it consisted of lists of articles with accompanying images. It was **predominantly text-based**, with multimedia content consisting of embeds from social media platforms such as Twitter.

In terms of accessibility the site was available at time of writing but has a history of takedowns. The site was simple to navigate, being divided into 'World,' 'US,' 'Society,'

and 'Insight,' but there was no means of searching the site for a specific article. The site was nonetheless updated almost daily and could be found with a simple Google search.

The top-right corner of the Daily Stormer homepage contained links to **social media profiles on Gab, Russia's VK, and Sina Weibo**, the Chinese microblogging site. While the VK and Weibo accounts were named 'Daily Stormer,' the Gab account was attributed to Anglin personally (@AndrewAnglin). The latter had the most reach, with 18.6k followers, compared to 2,366 on VK and the Weibo profile's 18. The choice of these social media platforms is reflective of Anglin and Daily Stormer's banishment by major mainstream companies.

All three profiles featured posts informing users of the Daily Stormer's current domain name, although the information on the Weibo account was from 2018 and thus out of date. The Gab and VK profiles also featured instructions on how to access **Daily Stormer's Dark Web version** via the TOR browser. The VK profile was the most recently updated, in September 2021, whereas the Gab profile hadn't posted or commented since January 2021 and the Weibo profile since March 2018.

Two of the ISIS sites, ekolabe.de and shineofislam, used the same web design tools and **may even have been established by the same individual(s)**, as reflected in the sites' near identical layouts and design. In terms of presentation and appearance, both homepages were very lengthy and filled with image-based links to a variety of types of IS content, most prominently video and audio (see Figure 5). As already mentioned, neither site was accessible at time of writing due to takedown efforts and they were already **difficult to find via search, outside of having a direct link**.

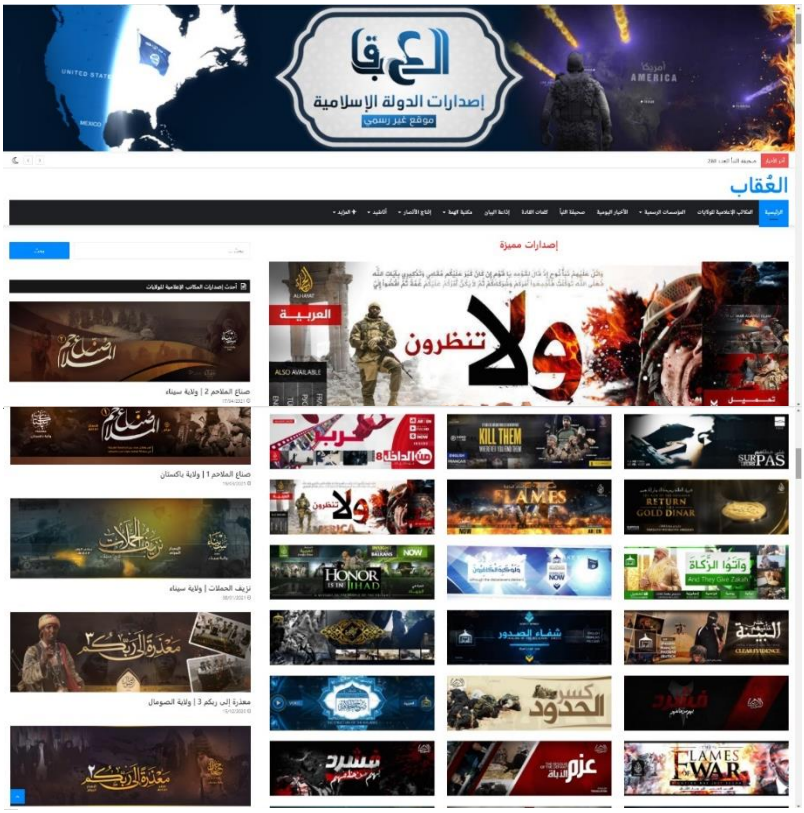

Figure 5 - Screenshots of Homepage of IS Support Website Elokab

Furthermore, although the Kurdish, Turkish, and English versions of the site had up-to date content, the others did not. Having said this, the English language content was largely composed of clumsily translated articles from one of the other language versions of the site. Nor was an email address or other means of contacting the PKK via the website provided.

Not addressed by Conway (2005) were the tools used to design the sites she studied. Thomas' (2021) research on far-right websites found that rather than being custom-built by professional developers or web designers, the majority were built using open-source technologies. Specifically, 63 of the 100 sites in her dataset were built using WordPress. In terms **of the eight websites surveyed here, only two of the eight did not use WordPress**; these were the Hamas and PKK sites.

Both our figures and Thomas' (2021) for the use of open-source website development tools and software by extremists and terrorists are out of line with general use of open-source technologies to build websites. Approximately 34% of all websites today use WordPress' content management system; our figure of 75%—admittedly based on a very small sample—and Thomas' of 63% hover around double this.

Due to the open-source and community-based structure of WordPress, it is difficult to devise means of preventing extremists and terrorists from utilising this software (Thomas 2021, pp.'s 8-9). This is almost certainly part of the explanation for why there is such a heavy reliance by extremists and terrorists on WordPress. Other website design and development tools and services are proprietary and oftentimes require payment—this includes the paid version of WordPress—and thus open users up to much greater scrutiny and therefore potential takedown.

In summary, applying Conway's (2005) methodology reveals the **wide disparity in sophistication between the case study websites**, ranging from the most sophisticated, Nordic Resistance, to the least, PKK, which is broadly similar to the findings of her original TOW study, which revealed similar disparities.

A focus on website design and sophistication draws useful attention, via a focus on the presence or absence of social media outlinks, to the **embedding of the sites—or not—within broader extremist and terrorist ecosystems** comprised of a multiplicity of types of online spaces, including social media platforms and messaging applications.

Furthermore, a focus on accessibility emphasises how websites being easy or difficult to find via search or accessible or inaccessible (e.g., due to takedown) points to how websites that are not easily found or are otherwise inaccessible are severely disadvantaged. **Regardless of the high recruitment score of the IS supporter sites in the previous section, for example, the obstacles to locating them via search and the subsequent takedown of two of them seriously impacts their utility to users**.

WEBSITE REACH

In this sub-section we discuss extremist and terrorist websites' reach or popularity using data drawn from the Amazon-owned web traffic analysis site Alexa.com. There are two primary ways to measure the popularity of a given website, its Alexa site ranking, which is based on traffic and engagement metrics of 30+ million sites, and the numbers of in-links to a site.

Table 5 ranks each of our case study websites from highest to lowest based on their Alexa.com global ranking, which is calculated using a combination of average daily visitors to a site and pageviews on a site over the preceding 90 days.

Table 5. Case Study Websites' Alexa.com Global Rankings: Highest to Lowest				
	Affiliation	*URL*	*Type of Site*	*Global Ranking*
1.	Daily Stormer	Dailystormer.su	Ideologically Adjacent	112,810
2.	Hamas	Hamas.ps	TOW	333,197
3.	Taliban	alemarahenglish.net	TOW	589,758
4.	Nordic Resistance	Nordicresistance.org	Ideologically Adjacent	2,013,388
5.	PKK	pkk-online.com	TOW	2,278,538
6.	IS	i3lam.pm	Fan Site	3,710,210
7.	IS	shineofislam.com	Fan Site	5,394,794
8.	IS	Elokabe.de	Fan Site	Not ranked

For comparison, in mid-October 2021, facebook.com was ranked no.7 globally by Alexa.com, The New York Times website appeared at no.115, the European Commission site at no.686, and spiegel.de at 1,112. Given that there are in the region of 1.88 billion websites in existence, Table 1's **top three websites were relatively highly ranked, with all those sites for which data was available ranking in the top 1% of all websites.**

An alternate measure of website popularity is via analysis of the number of links to a given website from other sites, which can be done through Alexa.com's in-linking tool. Going to Baele et al's second level of analysis (2020, p.4), the nature of the sites in-linking to a given extremist or terrorist site can also be illustrative of the community or communities within which the website is embedded.

While Daily Stormer was the most popular site in terms of Alexa.com's global rankings, **Hamas' website was the case study with the most in-links at 164**. This appeared to be due to news media websites linking to the site in articles. Such linking was undertaken by news websites in a range of countries (e.g., timesofisrael.com, farsnews.ir, thejournal.ie) and with a variety of ideological leanings (e.g., breitbart.com, sputniknews.com, telegraph.co.uk, npr.org, progressive.org).

Daily Stormer had the second highest number of in-links of the examined websites at 147. Most of the sites linking to Daily Stormer were either outright white supremacist sites (e.g., white-power.org, cjcc-aryan-nations.com, whitenationalist.org) or sites dedicated to the conspiracy theory known as 'the Great Replacement' or 'White Genocide' (e.g., age-of-treason.com, politicallyincorrect.info).

News media sites also linked to Daily Stormer although far fewer than linked to the Hamas site. Daily Stormer was therefore the site with the most in-links from fringe and extremist sites. In terms of audience demographics, according to Alexa.com's estimate, 94% of Daily Stormer's audience is US-based.

Using a snapshot of the site prior to its takedown, it was also possible to determine alemarahenglish.net was linked to from 58 domains. Again, **a large number of these were links from news media organisations** in articles covering the 2021 withdrawal of US armed forces from Afghanistan, which was ongoing at time of writing. Once more too, these included links from an ideologically diverse array of news sites, including npr.org, sputniknews.com, and theglobeandmail.com.

When compared to the other case study websites that ranked highly in Alexa.com's global rankings, nordicresistance.org had few in-links (30). Of these, just two overlapped with Daily Stormer in-links (i.e., age-of-treason.com and politicallyincorrect.info). In-linking to the NRM site too were a number of podcast hosting sites such as lybsyn.com, which hosts the white nationalist podcast Full Haus, and spreaker.com, which hosts a number of Nordic Resistance's own podcasts.

The PKK website was the TOW with the least in-links at just three, all from news sites. The IS supporter sites attracted even fewer in-links; Shineofislam.com had just one, from ghostsecuritygroup.com, which maintains a list of extremist and terrorist websites.

Taken together, these results point to the **disparity between sites in terms of reach and popularity.** The Daily Stormer, Hamas, and Taliban websites had far greater reach and were far more popular than the Nordic Resistance, PKK, and IS supporter sites.

The Taliban's 2021 takeover of Afghanistan may account for some of their site's popularity, especially the number of in-links from news media websites. Hamas' in-links were similarly populated by news media sites. On the other hand, the Daily Stormer and Nordic Resistance's in-links ran the gamut from fringe conservative to neo-Nazi websites.

To sum-up, it is clear the IS supporter sites' reach and popularity were negatively affected by their being subject to disruption and takedown and therefore short-lived while the longevity of both the Hamas group and its website advantaged it as did the notoriety and, again, longevity of the Daily Stormer site.

REFUSAL OF SERVICE

Considerable attention has been paid by researchers to social media platforms, especially the 'big companies,' and increasingly also messaging applications, and how effectively they moderate extremist and terrorist content on their services. Much less attention has yet been paid to if and how infrastructure and service providers, further down 'the tech stack,' deal with extremism and terrorism.

Of the eight websites in our sample, half were no longer available. These were the Taliban site and the three IS supporter sites. At least one additional site, the Daily Stomer, has been subject to intermittent takedown, but was accessible on the surface Web at time of writing.

Discussed in this section is refusal of service by companies composing the tech stack, intense discussion about which the Daily Stormer prompted post-Charlottesville and which the Taliban's websites were assumed to have been subject to in mid-August 2021.

A 'tech stack' is the combination of tools and technologies, generally some combination of programming languages, frameworks, libraries, servers, software, and similar, used by individuals or organisations to build a web or mobile application.

'*The* tech stack,' on the other hand, is the layers of actors and entities that account for the continued working of the Internet itself. This includes everything from cloud service providers to governments and telecoms (see Table 6).

Table 6. Content Moderation in the Internet Tech Stack			
Level	*Description*	*Actors*	*Content Moderation?*
1.	Open Web	Websites, Forums, Blogs, etc.	✓
2.	Platforms, Search Engines, and Apps	Facebook, Google, Twitter, YouTube, Telegram, etc.	✓
3.	Cloud Services	AWS (Amazon web Services), Microsoft Azure, Google Cloud, etc.	?
4.	Content Delivery Networks	Cloudflare, Microsoft Azure, etc.	?
5.	Domain Registrars	GoDaddy, Network Solutions, Tucows, etc.	?
6.	Internet Service Providers	Deutsche Telekom, Orange, Vodafone, etc.	?
7.	Government/Telecom Infrastructure	Eircom, Comcast, Huawei	?
Source: Modified from Donovan 2019			

As regards content moderation, the higher in the stack an actor is the higher the expectation that content moderation practices and policies, including around extremism and terrorism, are in place. For this reason, most of the research and discussion around content moderation is around individual websites' policies (Level 1) and major platforms' Terms of Service (ToS) (Level 2) (Donovan 2019).

But what about if a website is an extremist or terrorist site? Suffice it to say, extremist and terrorist websites don't generally have policies against the sharing of extremist and terrorist content albeit the Daily Stormer nods in this direction. This is where the roles and responsibilities of actors and entities in Layers 3 to 7 of 'the tech stack' come in.

Thomas (2021) found that Cloudflare hosted 46 of the 100 extreme right websites that she studied (p.6). Cloudflare currently hosts or has hosted the majority of the websites discussed herein too, including alemarahenglish.net, nordicresistance.org, pkk-online, shineofislam.com, i3lam.pm, and the original Daily Stormer.

Cloudflare is a core node in the Internet tech stack and the bulk of our discussion on service refusal below thus focuses on it, but much of the commentary is relevant to a range of actors in especially Layers 3 to 6 of Table 6.

Cloudflare is a San Francisco-based Content Delivery Network (CDN) and website security provider. It is particularly well known for its Distributed Denial of Service (DDoS) mitigation services, which protect websites from attack. In terms of its CDN, in 2021 Cloudflare claimed to support over 25 million websites (Cloudflare 2021a).

Cloudflare provided its services to all-comers, including a swathe of extreme right and terrorist websites, on a wholly content neutral basis up until the 2017 Charlottesville's 'Unite the Right' rally. One of the websites Cloudflare had been providing service to was The Daily Stormer.

After Andrew Anglin's post praising Heather Heyer's killer, Cloudflare's CEO, Matthew Prince, terminated The Daily Stormer's Cloudflare account. In a post on Cloudflare's official blog on 16 August, 2017 Prince said "The tipping point for us making this decision was that the team behind Daily Stormer made the claim that we were secretly supporters of their ideology… We could not remain neutral after these claims of secret support by Cloudflare" (Prince, 2017).

The bulk of the post, entitled 'Why We Terminated Daily Stormer,' was taken up with "why it's so dangerous." In particular, Prince pointed out that sites requiring security protections such as those supplied by Cloudflare oftentimes will be knocked offline by the frequency and intensity of attacks without them.

Prince also argued that soon it is likely that there will only be a small number of companies capable of providing content hosting services, which will essentially hand them the power of determining what can and cannot appear online.

Prince underlined that, for him, this was not a free speech issue, but an issue of due process:

"The issue of who can and cannot be online has often been associated with Freedom of Speech. We think the more important principle is Due Process. I, personally, believe in strong Freedom of Speech protections, but I also acknowledge that it is a very American idea that is not shared globally. On the other hand, the concept of Due Process is close to universal. At its most basic, Due Process means that you should be able to know the rules a system will follow if you participate in that system" (Prince, 2017).

An Electronic Frontier Foundation (EFF) spokesperson made similar observations, noting that **already only a few hundred companies globally offer domain hosting services.** This means that if a site was blacklisted by most or all of these (i.e., cannot find a host), there's the possibility that it ceases to exist, certainly on the open web.

"The issue is not 'we won't let this person into our home,'" the EFF spokesperson said; "[i]t's more 'we won't offer you electricity or plumbing,' the things that run your house in the first place" (Hayden, 2017). This is essentially what happened to the Daily Stormer in the wake of Charlottesville. When major web-hosting companies (e.g., GoDaddy, Google, Tucows, Zoho) began refusing to host the site, and with Cloudflare refusing security services, it could not remain on the open Internet and retreated for some time to the Dark Web.

Today, Cloudflare warns that it reserves the right to suspend or terminate websites or access to their other services "at any time, with or without notice for any reason or no reason at all." The service also prohibits the use of websites supported by them or using their online services in a way that violates any applicable US federal, US state, local, or international law or regulation (Cloudflare 2021b).

Notably, there is no explicit mention of extremist content or the use of Cloudflare's services by terrorist or proscribed groups in 'Cloudflare Website and Online Services Terms of Use' (Cloudflare 2021b). Having said this, these are essentially covered by the above prohibition on using Cloudflare's service in ways which violate US or international law, while still allowing the company a measure of discretion as to how they deal with extremist and terrorist-related activity.

Five websites operated by the Taliban went offline on 20 August, 2021 amid a larger push by tech companies to limit the group's digital reach following their takeover of Afghanistan. It remains unclear who or what was actually responsible for the shutdown. While it is widely assumed that Cloudflare had a hand in it (i.e., removed their DDoS protections), the company did not respond to journalists' requests for comment nor did they publish an official Blog post on the matter. These were TOWs on the basis of, for example, the UN's designation of the Taliban, however.

Cloudflare and/or other service providers are plainly refusing service to IS supporter sites too. This is indicated by the cycling of these sites through multiple and increasingly obscure domains and the relatively short online existence of many. For example, the Elokab IS supporter site cycled through numerous country code top-level (ccTLD) and more general Internet top-level domains (TLD). Minor changes in spelling, reflected in

the shift in the domain name from 'elokab' to 'elokabe,' are also utilised for purposes of avoiding takedown, but still being findable by knowledgeable users.

ccTLDs are two-letter Internet top-level domains used by or reserved for specific countries or sovereign or dependent territories. Administration and control of these is devolved by the Internet Assigned Numbers Authority (IANA) to an entity, generally within the country designated by the two-letter code. These designees are responsible for the policies and operation of the domain,[6] which may include requirements for a local presence (e.g., citizenship, domicile, etc.). Some ccTLDs are, for profit and other motives, freely open for registration, however.

The Elokab IS supporter site cycled through numerous ccTLDs, including elokab.pm, elokab.in, elokab.pw, elokab.nl, elokabe.de, and elokab.eu. Some of these were ccTLDs for large and prominent countries such as India ('.in'), Germany ('.de'), and the Netherlands ('.nl') whereas others were for obscure locations such as the French territory of Saint-Pierre and Miquelon ('.pm') and Palau ('.pw'), a 500-island archipelago in the Western Pacific Ocean. The '.eu' ccTLD, which is theoretically restricted to persons and entities in EU member states, was also utilised.

Some more general Internet top-level domains (TLD) were relied upon by the Elokab site too. These included the '.icu' TLD, which is generally targeted at businesses and '.fun,' which is described by name.com as being available to "[a]musement parks, arcades, and other facilities geared towards entertainment." Regardless of their registration requirements, all of these ccTLD and TLDs initially allowed access to the Elokab site, but all also eventually revoked the IS supporter site's access though we cannot determine why or after what lengths of time.

Daily Stormer engaged in a similar process of domain cycling post-Charlottesville. Following failed attempts to utilise '.al' (Albania), '.is' (Iceland), '.ru' (Russia), and '.hk' (Hong Kong), the site re-emerged on the surface Web using a '.name' suffix. It is currently utilising the throwback '.su' (Soviet Union) ccTLD.

While the Daily Stormer is once again on the surface Web, notable is that in April 2017, just five months prior to the Charlottesville rally, the site ranked no.13,137 globally and at no.5,597 within the United States, according to Alexa.com (SPLC, n.d.). As already mentioned, its September 2021 global ranking was no.112,810 and its local US ranking 17,804. One explanation for these reduced rankings may be the increased level of difficulty associated with finding the Daily Stormer site post-Charlotteville when it cycled through numerous providers and domain names.

Websites more likely to be subject to takedown efforts often include means of how to find them when they obtain a new hosting service. In our sample, these were the IS fan sites; a page on the I3lam website titled 'Find Us' read: "If the I'lam website gets deleted, you will find the new link on this website," followed by a link to a html page available in English and Arabic with the 'Foundation's' logo in the centre. That page advised users to use a VPN or TOR Browser for secure browsing and, along with a Tor link featured, a 'public link' that directed back to the original site homepage. The page also contained links to download TOR on Android, IOS, and PC.

[6] IANA's full list of ccTLDs and accompanying designees is at https://www.iana.org/domains/root/db.

At time of writing, Shineofislam.com too consisted of just a landing page promising the site would be back soon, apologising for the inconvenience, and instructing users to contact them on their Telegram channel to get the TOR site link. (The Telegram channel, in turn, was innocuously named TheSunshineDay, most likely an attempt to avoid being taken down by Telegram).

Similarly, and as already mentioned, Andrew Anglin's Gab account and the Daily Stormer's VK profile featured instructions on how to access Daily Stormer's Dark Web version via the TOR browser.

We know that, since Charlottesville, the Daily Stormer has been subject to semi-regular takedown. Some have put Cloudflare's initial decision and Daily Stormer takedowns by other companies subsequently down largely to "significant negative media attention" (Thomas, 2021, p.4).

The takedown of the official websites of designated terrorist organisation and websites that openly support those organisations would seem more straightforward and, in some instances, required. It is unclear in the main the processes via which this is occurring, however.

Are service providers engaging in some form of content review and refusing service on this basis? Some services, like Cloudflare, have an abuse reporting facility, so are users reporting sites via these types of mechanisms? Another possibility is that law enforcement units specifically tasked in this area, such as the EU's Internet Referral Unit (EUIRU) and the UK's Counter-terrorism Internet Referral Unit (CTIRU), are reporting TOWs and supporter sites to their hosting companies and other service providers for ToS violations. Persistent high-level hacking attacks may also account for the disappearance of some sites. Some combination of all of these is also a feasible explanation for site takedowns.

The widespread disruption by a raft of major and minor social media platforms, messaging applications, and similar, of extremist and terrorist content may grow websites' attractiveness to extremist and terrorists and their supporters because of the lack of clarity around content review at the infrastructural levels underpinning those sites.

This is especially the case if it becomes apparent that takedown of even IS-affiliated sites is a (much?) lengthier process than on major platforms and that, like on the latter, differential disruption is in effect with regard to websites (i.e., IS-related websites are disrupted much more swiftly and thoroughly than those belonging to other groups and movements, including other jihadis) (Conway et al., 2019; Conway et al., 2021).

Cloudflare's Prince's and others' concerns around due process remain. International human rights standards emphasise that limits to freedom of expression should be the preserve of an independent judiciary and not delegated to private companies.

CONCLUSION

The structures of the Internet change over time. It is unsurprising therefore that the types of online spaces utilised by extremists and terrorists change too, generally in tandem with changes in the Internet's overall infrastructure.

Research by Kenyon, Binder, and Baker-Beall (2021), showed that among convicted UK terrorists who primarily radicalised online, along with those who radicalised through both online and offline influences, there was:

"a reduction in the number of individuals using specific extremist websites from 2005 onwards (60 and 83-percentage point decrease respectively from 2005 to 2017). Across the same period, there was an increase in the number of individuals using open social media platforms (36 and 57-percentage point increase respectively)" (pp.'s 11-12).

Having said this, websites are a perennial feature of the online ecosystem and are being reverted to by, in particular, IS supporters due to their content and accounts having high rates of deletion by social media platforms and messaging apps.

Websites are especially attractive online spaces for these IS supporters for several reasons, including the websites acting as archives of content increasingly unavailable via social media and messaging apps and, for those who establish them, the setting-up of the sites being a form of 'media jihad.'

Other appealing features of websites for extremists and terrorists across the ideological spectrum are that:

- Unlike most social media and messaging apps, website content is often indexed by search engines;
- Extremists and terrorists retain much greater control over the content on their websites, which are not subject to content moderation;
- Extremist and terrorist websites can be removed, but this is generally a much lengthier process due to a plethora of issues, including the multi-jurisdictional nature of online domains, than for content or accounts that egregiously violate social media companies' ToS (TaT 2021, p.15).

Other groups and movements that begin to come under the same pressure as IS on social media platforms, messaging apps, and in other online spaces may therefore be expected to increase their reliance on traditional websites also. Already, at least one terrorist attacker, the Hanau, Germany, shooter who killed nine people in February 2020, had established his own personal website, where he published files, some in English, that indicated a racist motivation for the attacks (Europol, 2021, p.78).

While there is new research emerging on extremist and terrorist websites, such little attention has been paid to them in the last decade and more that there are many research gaps to fill. Some recommendations for this future work are as follows:

- A clear statement of the types of sites that fall into the category 'website,' and why or why not, is warranted;
- The pros and cons of narrowing the research—and policy—focus to TOWs and supporter websites only needs to be systematically thought through;
- A large scale comparative study of, at a minimum, TOW and supporter websites, but we suggest also adjacent sites, from across the ideological spectrum should be conducted;
- Little research has yet been produced on content policies and processes—if any—in Layers 4 – 6 of the tech stack, which needs to change;
- A raft of recent and forthcoming legislation globally will impact websites, including their takedown. A study collating and interrogating these laws for their applicability with respect to extremist and terrorist websites is required;
- The role of 'news' websites in contemporary extremist and terrorist ecosystems also needs further investigation. This includes the roles of mainstream and alternative news sites, including media outlets run by terrorist supporters (e.g., Al-Qaeda-related Thabat News Agency).

CITATIONS

- Askanius, Tina. 2021. "'I Just Want to be the Friendly Face of National Socialism": The Turn to Civility in the Cultural Expressions of Neo-Nazism in Sweden.' *Nordicom Review* 42(s1).
- Associated Press. 'Finnish Top Court Bans Finland's Main Neo-Nazi Group.' *Associated Press*, 22 September 2020: https://apnews.com/article/finland-archive-courts-959402562fc46f29ac4a7fbf21fa6615.
- Awan, Akil, Andrew Hoskins, and Ben O'Loughlin. 2011. *Radicalisation and the Media: Connectivity and Terrorism in the New Media Ecology*. London and New York: Routledge, 2011.
- Baele, Stephane J., Lewys Brace, and Travis G. Coan. 2020. 'Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda.' *Studies in Conflict & Terrorism* [Online First].
- Barton-Hronešová, Jessie and Sanela Hodžić. 2021. 'Portrayals of Women on Ethno-Nationalist and Radical Islamic Websites in Bosnia and Herzegovina.' *Nationalism and Ethnic Politics* 27(2).
- Bjørgo, Tore and Jacob Aasland Ravndal. 2020. 'Why the Nordic Resistance Movement Restrains Its Use of Violence.' *Perspectives on Terrorism* 14(6): https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2020/issue-6/bjorgo-and-ravndal.pdf.
- Bouchard, Martin, Garth Davies, Richard Frank, Edith Wu and Kila Joffres. 2020. 'The Social Structure of Extremist Websites.' In Jez Littlewood, Lorne Dawson and Sara K. Thompson (Ed.s), *Terrorism and Counterterrorism in Canada*. Toronto: University of Toronto Press.
- Bowman-Grieve, Lorraine. 2009. 'Exploring "Stormfront": A Virtual Community of the Radical Right.' *Studies in Conflict & Terrorism* 32(11).
- Caiani, Manuela and Linda Parenti. 2013. European and American Extreme Right Groups and the Internet. Surrey: Ashgate.
- Caiani, Manuela and Linda Parenti. 2009. 'The Dark Side of the Web: Italian Right-Wing Extremist Groups and the Internet.' *South European Society and Politics* 14(3).
- Clifford, Bennett. 2018. "'Trucks, Knives, Bombs, Whatever": Exploring Pro-Islamic State Instructional Material on Telegram.' *CTC Sentinel* 11(5): 23–29.
- Cloudflare. 2021a. 'So What *is* Cloudflare?': https://www.cloudflare.com/learning/what-is-cloudflare/.
- Cloudflare. 2021b. 'Cloudflare Website and Online Services Terms of Use': https://www.cloudflare.com/website-terms/ (Effective from 16 August 2021).
- Comerford, Milo, Jakob Guhl, and Carl Miller. 2021. Understanding the New Zealand Online Extremist Ecosystem. London: Institute for Strategic Dialogue: https://www.isdglobal.org/wp-content/uploads/2021/06/NZ-Online-Extremism-Findings-Report.pdf.

- Conway, Maura, Moign Khawaja, Suraj Lakhani, and Jeremy Reffin. 2021. 'A Snapshot of the Syrian Jihadi Online Ecology: Differential Disruption, Community Strength, and Preferred Other Platforms.' *Studies in Conflict & Terrorism* [Online First].

- Conway, Maura, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson, and David Weir. 2019. 'Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts.' *Studies in Conflict & Terrorism* 42(1/2).

- Conway, Maura. 2005. 'Terrorist Web Sites: Their Contents, Functioning and Effectiveness.' In Philip Seib (Ed.), *Media and Conflict in the Twenty-first Century*. London: Palgrave Macmillan.

- Crawford, Blyth, Florence Keen, and Guillermo Suarez-Tangil. 2021. 'Memes, Radicalisation, and the Promotion of Violence on Chan Sites.' In *Proceedings of the International AAAI Conference on Web and Social Media (ICWSM)* : https://ojs.aaai.org/index.php/ICWSM/article/view/18121.

- Davies, Garth, Martin Bouchard, Edith Wu, Kila Joffres, and Richard Frank. (2015). 'Terrorist Organizations' Use of the Internet for Recruitment.' In Martin Bouchard (Ed.), *Social Network, Terrorism and Counter-Terrorism: Radical and Connected*. New York, NY: Routledge.

- Donovan, Joan. 2019. 'Navigating the Tech Stack: When, Where and How Should We Moderate Content?' *CIGI Online*, 28 October: https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content/.

- Elison, William. 2000. 'Netwar: Studying Rebels on the Internet.' *The Social Studies* 91(3).

- Europol. 2021. *EU Terrorism Situation and Trend Report 2021 (Te-Sat)*. The Hague: Europol: https://www.europol.europa.eu/sites/default/files/documents/tesat_2021_0.pdf.

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

- Friedlander, Julia, Michael Albanese and Al Castellum. 'Global Sanctions Dashboard: April.' *Atlantic Council*, 14 May 2021: https://www.atlanticcouncil.org/blogs/econographics/global-sanctions-dashboard-april/.

- Froio, Caterina. 2018. 'Race, Religion, or Culture? Framing Islam Between Racism and Neo-Racism in the Online Network of the French Far Right.' *Perspectives on Politics* 16(3).

- Gornishka, Iva, Stevan Rudinac, and Marcel Worring. 2020. 'Interactive Search and Exploration in Discussion Forums Using Multimodal Embeddings.' In Ro Y. *et al.* (Ed.s), *Lecture Notes in Computer Science, Vol. 11962.*

- Guhl, Jakob, Julia Ebner, and Jan Rau. 2020. *The Online Ecosystem of the German Far-Right*. London: Institute for Strategic Dialogue: https://www.isdglobal.org/isd-publications/the-online-ecosystem-of-the-german-far-right/.

- Hartzell, Stephanie L. 2020. 'Whiteness Feels Good Here: Interrogating White Nationalist Rhetoric on Stormfront.' *Communication and Critical/Cultural Studies* 17(2).

- Heft, Annett, Curd Knüpfer, Susanne Reinhardt, and Eva Mayerhöffer. 2021. 'Toward a Transnational Information Ecology on the Right? Hyperlink Networking among Right-Wing Digital News Sites in Europe and the United States.' *The International Journal of Press/Politics* 26(2).

- Institute for Strategic Dialogue (ISD). 2020. *Trans-Atlantic Journeys of Far-Right Narratives Through Online-Media Ecosystems*. London : ISD: https://www.isdglobal.org/wp-content/uploads/2020/12/TransAtlanticJourneysofFar-RightNarratives_v4.pdf.

- Kenyon, Jonathan, Jens Binder, and Christopher Baker-Beall. 2021. *Exploring the Role of the Internet in Radicalisation and Offending of Convicted Extremists*. London: HM Prison and Probation Service: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017413/exploring-role-internet-radicalisation.pdf.

- Kleinberg, Bennett, Isabelle van der Vegt, and Paul Gill. 2021. 'The Temporal Evolution of a Far-Right Forum.' *Journal of Computational Social Science* 4(1).

- Krämer, Tania. 'Critics Seek Proof After Israel Designates Palestinian Rights Groups as Terrorists.' *Deutsche Welle*, 26 October 2021: https://www.dw.com/en/critics-seek-proof-after-israel-designates-palestinian-rights-groups-as-terrorists/a-59623937.

- Lee, Benjamin and Kim Knott. 2021. 'Fascist Aspirants: Fascist Forge and Ideological Learning in the Extreme-Right Online Milieu.' *Behavioral Sciences of Terrorism and Political Aggression* [Online First].

- Stuart Macdonald, Kamil Yilmaz, Chamin Herath, JM Berger, Suraj Lakhani, Lella Nouri, and Maura Conway. Forthcoming. *A Snapshot of Europe's Far-Right Online Ecosystem*. Washington DC: RESOLVE Network.

- Macdonald, Stuart, Daniel Grinnell, Anina Kinzel, and Nuria Lorenzo-Dus. 2019. 'Daesh, Twitter and the Social Media Ecosystem: A Study of Outlinks Contained in Tweets Mentioning *Rumiyah*.' *RUSI Journal* 164(4): 60–72.

- Matthew Prince. 'Why We Terminated Daily Stormer.' *Cloudflare Blog*, 16 August, 2017: https://blog.cloudflare.com/why-we-terminated-daily-stormer/.

- Reid, Edna, Jialun Qin, Yilu Zhou, Guanpi Lai, Marc Sageman, Gabriel Weimann, and Hsinchun Chen. 2005. 'Collecting and Analyzing the Presence of Terrorists on the Web: A Case Study of Jihad Websites.' In *International Conference on Intelligence and Security Informatics*. Berlin and Heidelberg: Springer.

- Scrivens, Ryan, Amanda Isabel Osuna, Steven M. Chermak, Michael A. Whitney, and Richard Frank. 2021. 'Examining Online Indicators of Extremism in Violent Right-Wing Extremist Forums.' *Studies in Conflict & Terrorism* [Online First].

- Scrivens, Ryan, Thomas W. Wojciechowski, and Richard Frank. 2020. 'Examining the Developmental Pathways of Online Posting Behavior in Violent Right-Wing Extremist Forums.' *Terrorism and Political Violence* [Online First].

- Seib, Philip and Dana Janbek. 2011. *Global Terrorism and the New Media: The Post-Al Qaeda Generation*. Abingdon: Routledge.

- Southern Poverty Law Center. n.d. 'Andrew Anglin': https://www.splcenter.org/fighting-hate/extremist-files/individual/andrew-anglin.

- Tech Against Terrorism. 2021. *GIFCT Technical Approaches Working Group: Gap Analysis and Recommendations for Deploying Technical Solutions to Tackle the Terrorist Use of the Internet*. https://gifct.org/wp-content/uploads/2021/07/GIFCT-TAWG-2021.pdf.

- Thomas, Elise. 2021. *Open Source, Self Defence: Tackling the Challenge of Extremist Websites and Open Source Tech*. London: Institute for Strategic Dialogue: https://www.isdglobal.org/wp-content/uploads/2021/08/Open-Source-Self-Defence_v2.pdf.

- Thorbecke, Catherine. 'How the Taliban Uses Social Media to Seek Legitimacy in the West, Sow Chaos at Home.' *ABC News*, 19 August 2021: https://abcnews.go.com/Technology/taliban-social-media-seek-legitimacy-west-sow-chaos/story?id=79500632.

- Tsfati, Yariv and Gabriel Weimann. 2002. 'www.terrorism.com: Terror on the Internet.' *Studies in Conflict & Terrorism* 25(5).

- Weimann, Gabriel. 2004. *www.terrorism.net: How Modern Terrorism Uses the Internet*. Washington DC: US Institute of Peace: https://www.usip.org/sites/default/files/sr116.pdf.

- Zelenkauskaite, Asta, Pihla Toivanen, Jukka Huhtamäki, and Katja Valaskivi. 2021. 'Shades of Hatred Online: 4chan Duplicate Circulation Surge During Hybrid Media Events.' *First Monday* 26(1): https://firstmonday.org/ojs/index.php/fm/article/view/11075.

- Zelin, Aaron. 2013. *The State of Global Jihad Online*. Washington DC: Washington Institute for Near East Policy: https://www.washingtoninstitute.org/policy-analysis/state-global-jihad-online.