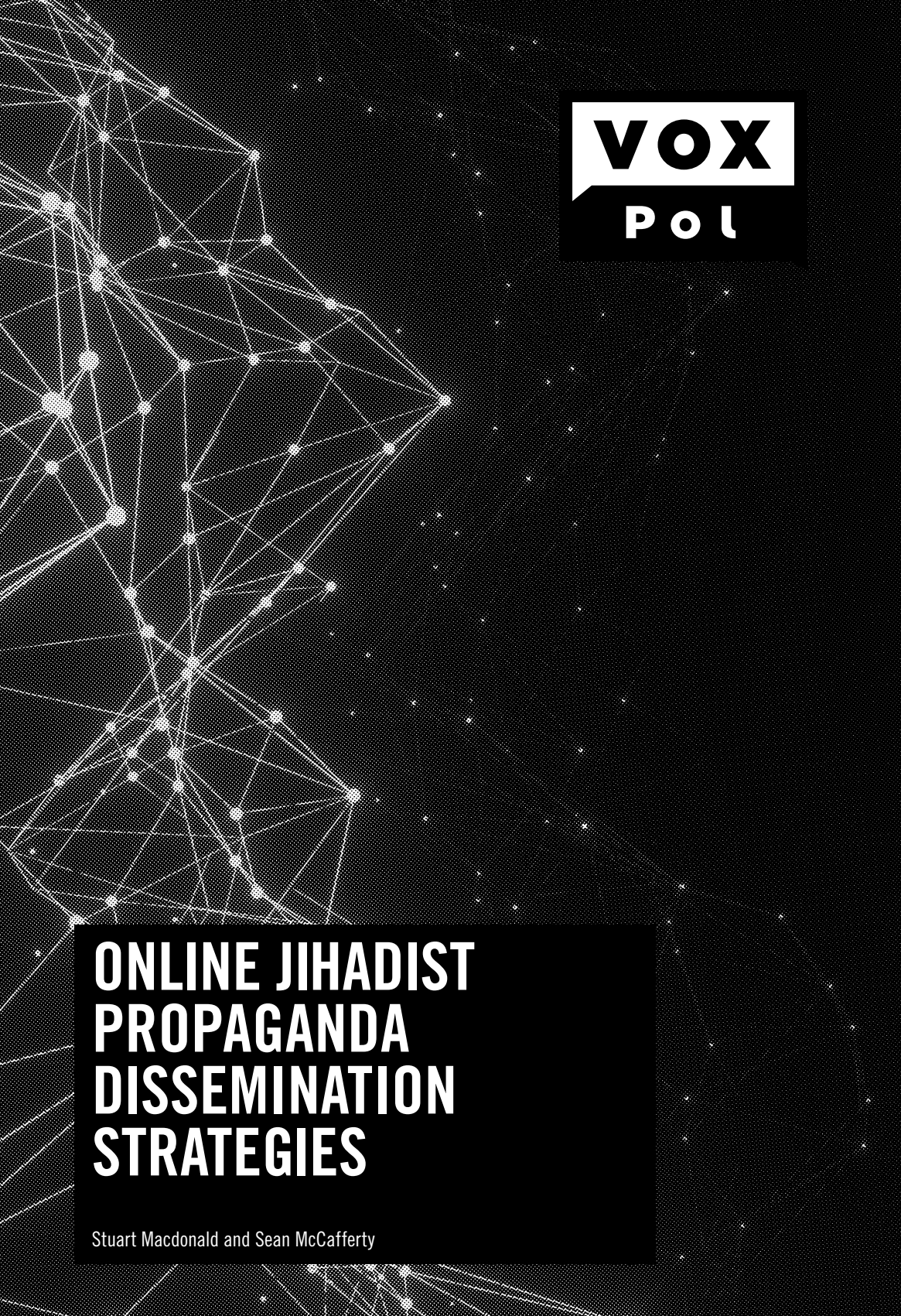


VOX Pol

ONLINE JIHADIST PROPAGANDA DISSEMINATION STRATEGIES

Stuart Macdonald and Sean McCafferty

ONLINE JIHADIST PROPAGANDA DISSEMINATION STRATEGIES

About the authors

Stuart Macdonald is Professor of Law at the Hillary Rodham Clinton School of Law, Swansea University, UK. He is Co-Director of the University's Cyber Threats Research Centre (CYTREC) and Coordinator of the VOX-Pol Network. Stuart's research focuses on terrorist's use of the internet. Most recently, he has examined jihadist narratives, the strategies used to disseminate terrorist propaganda online, and regulatory responses. He has received research funding from the British Academy, Welsh Government, US Government, NATO and the EU, among others. Stuart is the lead organiser of the biennial Terrorism and Social Media (TASM) conference, a member of Europol's Advisory Network on terrorism and propaganda and a Senior Fellow at Hedayah. In 2016/17 he was also the holder of a Fulbright Cyber Security Award.

Sean McCafferty is a Research Assistant at Dublin City University, Ireland. His research focuses on open-source intelligence, terrorism, propaganda, and technology. Sean holds an Erasmus Mundus International Master's in Security, Intelligence and Strategic Studies from Glasgow University, Dublin City University and Charles University.

Acknowledgements

The authors are grateful for the support received for this research from Tech Against Terrorism and Swansea University's Legal Innovation Lab Wales (which is part-funded by the European Regional Development Fund through the Welsh Government). They would also like to thank Archie Macfarlane and the anonymous reviewers for feedback on an earlier draft.

ISBN: 978-1-911669-66-1

Designed and typeset by Soapbox, www.designbysoapbox.com

Cover photo: Conny Schneider/Unsplash

TABLE OF CONTENTS

EXECUTIVE SUMMARY

IT IS WELL established that jihadist groups and their supporters post URLs on online platforms to outlink to items of propaganda stored on other platforms. Industry initiatives – such as the Global Internet Forum to Counter Terrorism's inclusion of URLs in its hash-sharing database, and Tech Against Terrorism's Terrorist Content Analytics Platform – have sought to counter this practice. These measures, together with new regulatory regimes (e.g. the EU's Terrorist Content Online Regulation) and the growing use of decentralised services, raise the question whether jihadist groups' propaganda dissemination strategies are perhaps being forced to evolve. This study considers whether there is evidence of such an evolution, by examining the means that three jihadist groups (Islamic State (IS), Al-Qaeda (AQ) and Al-Shabaab) used to disseminate their propaganda during a two-month period in early 2023.

The study focuses on 12 channels across four platforms: one archiving platform that has featured prominently in other studies of jihadist propaganda dissemination, one Europe-based decentralised messaging service, and two decentralised chat apps on the Rocketchat server. In total, we collected 4,164 posts that between them shared 796 distinct items of propaganda. A large majority of these items (682; 85.68%) were either attached to, or embedded in, in-channel posts – making this by far the most common method of sharing content. The use of URLs to outlink to content stored on other platforms was far less frequent, with 162 items (20.35%) shared in this way. Meanwhile, the use of inlinking to share content was rare (33 items; 4.15%).

The vast majority of the propaganda was produced by or in support of IS (715 items; 89.82%). This spanned a diverse range of formats: text (including bulletins, magazines and newsletters); images and photosets; videos; nasheeds, speeches and other audio content; banners and infographics; and instructional materials. As well as outlinks and posts in one-way channels, there was also widespread use of posts in interactive channels to share items in support of IS.

This reflects the fact that, while most of the IS items were official content (500; 69.93%), there was also a significant quantity of unofficial content (142 items; 19.86%).[1]

The volume of AQ and Al-Shabaab content was more limited. There were 54 items of AQ content. These encompassed bulletins, magazines and other written publications, images and photosets, videos and promotional banners – and were almost exclusively official content. All 27 of the Al-Shabaab items were official content: mainly videos produced by the Al-Kataib foundation and banners promoting them. The dissemination strategy of each of these groups was unidirectional and hierarchical, focusing on posts in one-way channels and outlinking.

The differences between the three groups – in terms of both content type and dissemination strategy – show the importance of tailored regulatory strategies. While outlinking was rarely used to share bulletins, banners or photosets, it was used regularly to share videos, magazines, infographics and instructional material. It seemed that outlinks were often used to provide supporters with shareable links to content, and to ensure stable access to back-up copies of propaganda items. These objectives were frequently frustrated: one week after the end of our data collection period, 67.61% of the outlinks had been deactivated. While this demonstrates that there remains room for improvement, it compares favourably with the enforcement rates for in-channel posts (4.67%) and inlinks (0.51%).

Although the use of inlinking was rare within our dataset, there are reasons why it should be regarded as a cause for concern (in addition to the low enforcement rate). First, where instances of inlinking were found, the inlinks often appeared in posts beneath another item of content – providing the user with a catalogue of content similar to the item they had just viewed. The effect was thus to create a filter bubble manually. Secondly, since our study focused on the sharing of content, it excluded links to other terrorist channels on the same platform. Our anecdotal impression was that inlinks

1 It was unclear whether the remaining 73 items were official or unofficial.

were more often used to direct users to other channels on the same platform, as opposed to other items of content. This requires further testing in future work but, if correct, would exacerbate concerns about inlinks being used to create a filter bubble effect.

Even though a large majority of the items of content in our dataset were shared in in-channel posts, this method of propaganda dissemination faced relatively little disruption. Not only was the enforcement rate only 4.67%, but all 12 of the channels that we monitored remained live from the start of data collection to at least one week after its completion – providing users with a steady flow of propaganda. While opinions may differ on the usefulness of seeking to shut down channels on lesser-known platforms, what is clear is that there are limits, both to the scope of existing regulatory regimes (for example, they may apply only to providers offering certain types of service, to service providers with a certain number of users and/or to those that disseminate content to the public) and to these regimes' practical implementation (especially given the large number of platforms that are exploited, and the resource constraints faced by enforcement agencies). The stable presence of these channels hosting a steady flow of jihadist propaganda may suggest that the disruptive efforts and subsequent adversarial shifts of recent years are beginning to reach an equilibrium.

1. INTRODUCTION

TERRORIST GROUPS AND their supporters use a wide variety of online platforms and services. This has been demonstrated by a number of studies of online extremist and terrorist 'ecosystems' (e.g., Macdonald et al. 2019b; Conway et al. 2020; Droogan et al. 2022; Macdonald et al. 2022a). One of the contributions of these studies has been to advance our understanding of how jihadist propaganda is disseminated online. In particular, they have drawn attention to the sharing of content by outlinking – that is, posting on one platform URLs that link to content stored on a different platform. This focus on outlinking reflects these studies' objective: to analyse the variety of online services being utilised and the connections between them.

There have been concerted efforts, at both the policy and practice levels, to disrupt the use of outlinks in disseminating jihadist propaganda. The Terrorist Content Analytics Platform (TCAP), established by Tech Against Terrorism, alerts companies to the presence of terrorist content on their platforms so that they can remove it speedily. From November 2020 to January 2023, 22,615 alerts were sent to a total of 95 different tech companies. The vast majority of these alerts related to jihadist content on file-sharing platforms, with a high enforcement rate (Tech Against Terrorism 2023a). In 2022, the Global Internet Forum to Counter Terrorism (GIFCT) operationalised the inclusion of URL hashes within its hash-sharing database (GIFCT 2023), as a first step towards alerting member companies when their platforms were being used to outlink to terrorist content. Alongside – and possibly as a result of – these efforts to disrupt outlinking, there has been an increase in the number and use of terrorist-operated websites (Conway and Looney 2021; Tech Against Terrorism 2022a), and of decentralised services (Trauthig and Bodo, 2022). The comparatively low levels of enforcement on these other types of service raise the possibility of alternative/additional strategies being employed by jihadist groups and their supporters to disseminate their propaganda online. Indeed, there is some evidence of such an adversarial shift – towards the end of 2022 there was a discernible reduction in jihadist submissions to the TCAP, apparently as a result of the decline in outlinking via large banks of URLs (Tech Against Terrorism 2023a).

Accordingly, this report seeks to answer the question: what propaganda dissemination strategies are currently being employed by jihadist groups? To this end, it examines the items of jihadist propaganda that were shared within 12 channels across four different online platforms during a two-month period in early 2023. The findings reveal that, while outlinking continues to play a significant role – especially for certain groups and particular types of content – by far the most common dissemination method is to attach content to, or embed it in, in-channel posts. Moreover, the channels examined in this study maintain a stable presence with low enforcement levels – in terms of both the removal of individual items of content and the shutdown of the channels themselves. Given the decentralised nature of some of these platforms, the apparent unwillingness of the others to moderate effectively the jihadist content they host, and the limits on the scope of existing regulatory regimes that might be employed to induce compliance, the report highlights the need for a strategy to disrupt the dissemination of jihadist content within these online spaces.

2. CONTEXT

IN RECENT YEARS, a number of studies have conceptualised the variety of online services and platforms utilised by extremist and terrorist actors as an ecosystem. In their examination of the far-right online landscape, Baele, Brace and Coan (2020) identify four components of an online ecosystem: entities (individual domains, such as a Facebook group page, a thematic forum or a blog); communities (entities are that connected, e.g., by the use of hyperlinks, movements in the user base or the flow of content); biotopes (groupings of communities that share a common ideological, thematic or cultural sub-identity); and whole networks (the composite of all these entities, communities and biotopes, which may overlap with other networks/ecosystems) (see also Hutchinson et al. 2022). One important benefit of this framework, the authors state, is to make plain the "*vast, dynamic, multidimensional, and heterogeneous* (in terms of ideology and practices) nature of the far-right online ecosystem" (3, emphasis original).

Other studies have also adopted an ecosystems-based approach in order to highlight the range of different online services – or entities – used by far-right extremists. Droogan et al. (2022) collected URLs from Twitter and Gab to map the platforms and content shared by Australian far-right violent extremists. They found that the majority of the sites that were linked to were social media platforms and news-related sites, and they highlighted the "interconnectedness of a social media ecosystem consisting of multiple platforms that were identified as having different purposes and functions" (4). In a similar vein, the Twitter outlink analysis conducted by Macdonald et al. (2022a) identified a total of 11 different service types that were used by members of far-right networks in France and Germany. As well as websites, video sharing and social networking, these services included follower tracking, URL shortening and social media marketing and posting.

An ecosystems approach has also been employed in studies of the online activities of jihadist groups and their supporters. Conway et al.'s (2019) study of pro-IS users on Twitter found significant levels of disruption, leading them to conclude that "pro-IS Twitter activity has largely been reduced to tactical use of throwaway accounts

for distributing links to pro-IS content on other platforms, rather than as a space for public IS support and influencing activity" (152). Other studies have reached a similar conclusion (e.g., Macdonald et al. 2019b). By comparison, Conway et al. found that other jihadist groups faced far lower levels of enforcement activity on Twitter. This "differential disruption" was examined further in their follow-on study (Conway et al. 2020, 14), in which they emphasised the value of an ecological approach, including in order to understand how enforcement activity on one platform can impact the use of other platforms by a group's supporters.

These knock-on effects of disruption include the movement of *users* between platforms – variously described as migration (Amarasingam et al. 2021; Hutchinson et al. 2022), displacement (Macdonald et al. 2019a) and as akin to whack-a-mole (Berger and Morgan 2015). A focus on the whole ecosystem has also proven valuable in understanding the dissemination of *content*, including the strategies employed to try and circumvent takedowns and account suspensions. For example, Weirman and Alexander (2020) examined a total of 240,158 URLs that were shared among English-language IS sympathisers on Twitter. Aside from intra-platform links, the most common service types outlinked to were news sources, file-sharing and social networking. The prevalence of file-sharing services, the authors explain, reflects the ability of such sites to "inoculate extremist networks against takedowns by separating the content producers, disseminators, and consumers from the material itself" (247). This strategy has been likened to a digital form of dead drop (Weimann and Vellante 2021). According to Fisher et al. (2019), "content stores" (9) such as file-sharing sites are used in conjunction with other services that function as "aggregators" (20) (where collections of links to a single piece of content are gathered and shared), and as "beacons" (22) (which signpost other users to where jihadist materials can be located). This strategy is designed to achieve the greatest possible reach while maintaining resilience. Subsequent analysis of data collected from public-facing Telegram channels (Macdonald et al. 2022b) showed that the URLs shared via these aggregator services are regarded as throwaway items that are rarely

reused. The emphasis is placed on volume – generating large batches of URLs that lead to copies of the same item of content on multiple file-sharing sites, with multiple URLs for each individual site – and on speed, with evidence of the use of automation to enable the dissemination of potentially thousands of distinct URLs in one day.

This report is also concerned with the dissemination of content within jihadist online ecosystems. It builds upon existing scholarship in three ways. First, the data for many of the existing studies were collected from Twitter and, more recently, Telegram. In contrast, the data for this report were collected from other platforms that have received little attention but are nonetheless important entities in jihadist online ecosystems. Second, the emphasis in much of the previous work has been on mapping the platforms that comprise these ecosystems (e.g., documenting the service types of the most shared domain names within a dataset) and the content that is shared within them (e.g., content analyses of the most shared URLs within a dataset). This report instead seeks to contribute to the smaller subset of ecosystems research which aims to understand strategies for disseminating content. Third, previous work on dissemination strategies (as well as ecosystems research more generally) has had a strong focus on the use of URLs, particularly outlinks. This report aims to contextualise the use of outlinking as a strategy for propaganda dissemination, by comparing its use with other methods of sharing content. To do this, it takes discreet items of propaganda as its units of analysis and examines the different ways in which each individual item was shared. This approach offers not only insights into the prevalence of outlinking as a dissemination strategy relative to other methods of sharing, but also the chance to explore correlations between how content is shared and different content types and formats.

3. METHODOLOGY

FOR THE PURPOSES of this study, one of the researchers was embedded in the Open-Source Intelligence team at Tech Against Terrorism. They were provided with the necessary induction and training, together with wellbeing support. Data collection took place over a two-month period, from 21 January to 21 March 2023, using manual open-source techniques. At the beginning of the collection period, data were collected from a total of six channels across four platforms. Our selection of these platforms was purposive and guided by the industry experience of Tech Against Terrorism – who advised that these platforms were key nodes in the online jihadist propaganda dissemination ecosystem. The platforms were: an archiving platform that had previously featured prominently in similar studies,[2] a Europe-based decentralised messaging service, and two decentralised chat apps on the Rocketchat server.[3]

Our identification of channels on these platforms also benefited from the experience of Tech Against Terrorism, who shared details of the channels they were monitoring. Beyond this, we sought to identify additional channels using keyword searches. The search terms employed were the names of each group's official media outlets, the names of each group's publications and the names of all known videos produced by each group. Whether a channel was identified by Tech Against Terrorism or via a keyword search, it was included in the study only if it was demonstrably pro-jihadist and met at least one of the following four criteria:

- The channel posted official content from a jihadist group (such as claims of attacks, video/photo propaganda or nasheeds);
- The channel published unofficial content that praised a jihadist group and its efforts and/or promoted its ideology;
- The channel administrator had published official content from a jihadist group or content in support of a jihadist group on another platform; or
- The channel had been promoted by a network affiliated with a jihadist group, or the group's supporters, on other platforms.

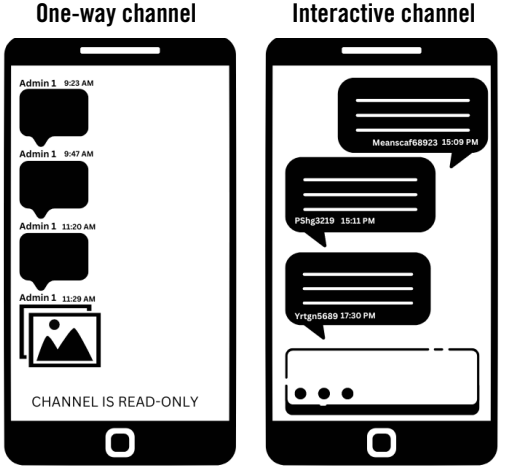
2 E.g., Grinnell et al. (2018), Conway et al. (2019), Macdonald et al. (2019b).

3 In accordance with Tech Against Terrorism's policy, these platforms are not named here. Readers who would like to know the names of the platforms are welcome to contact the authors.

Data were collected from these channels daily. By tracking the activity on them, it was possible to find links to new ones during the data collection period, and these newly identified channels were added to the study if they met the above conditions. To ensure consistency across the dataset, when a channel was added, posts were collected back to the date on which data collection had started.

By the end of the collection period, data had been collected from a total of 12 channels across the four platforms (see Table 1). Eight of these were one-way channels (i.e., ones in which only the channel administrator could post). The other four were interactive (meaning that all users in the channel could post). Figure 1 illustrates the difference between these two types of channel.

Figure 1: One-way and interactive channels



Our data collection focused on posts that shared content, so posts that consisted solely of text, with no accompanying content, were excluded from the study. Content encompassed both official and unofficial content but was limited to items produced by or in support of Islamic State, Al-Qaeda or Al-Shabaab.[4] The data were stored in a secure cloud-based service and formatted in an Excel workbook for analysis.

4 While some Jama'at Nasr Al-Islam wal Muslimin (JNIM) content was collected, it was deemed to be too limited for inclusion in the study.

Table 1: Channels from which data were collected

CHANNEL NO.	PLATFORM TYPE	COMMUNICATION	NO. OF CONTENT-SHARING POSTS	NO. OF POSTS SHARING CONTENT BY INLINK	NO. OF POSTS SHARING CONTENT BY OUTLINK	NO. OF POSTS WITH CONTENT EMBEDDED OR ATTACHED	STATUS OF CHANNEL (AS OF 28/03/2023)	NO. OF POSTS WITH CONTENT STILL AVAILABLE (AS OF 28/03/2023)
1	Archiving site	One-way	253	50	34	169	Live	221 (87.35%)
2	Archiving site	One-way	291	95	43	153	Live	246 (84.54%)
3	Archiving site	One-way	7	0	0	7	Live	7 (100%)
4	Decentralised chat	Interactive	397	58	82	257	Live	366 (92.19%)
5	Decentralised chat	Interactive	167	7	0	160	Live	167 (100%)
6	Messaging service	Interactive	225	1	88	136	Live	156 (69.33%)
7	Messaging service	Interactive	284	8	154	122	Live	167 (58.80%)
8	Messaging service	One-way	515	0	363	152	Live	303 (58.83%)
9	Decentralised chat	One-way	319	36	246	37	Live	220 (68.97%)
10	Decentralised chat	One-way	381	16	352	13	Live	78 (20.47%)
11	Decentralised chat	One-way	390	12	368	10	Live	89 (22.82%)
12	Decentralised chat	One-way	935	111	582	242	Live	584 (62.46%)
Total		**8 one-way, 4 interactive**	**4,164**	**394**	**2,312**	**1,458**		**2,604 (62.54%)**

Data analysis focused on individual *items* of propaganda that had been shared by the posts within the dataset. Each of the 796 pieces of content was coded using the following categories, which were generated inductively through examination of the dataset:

- Group [IS/AQ/Al-Shabaab];
- Content status [official/unofficial/unclear];
- Shared via outlink [Yes/No];
- Shared via inlink [Yes/No];
- Shared via post in a one-way channel [Yes/No];
- Shared via post in an interactive channel [Yes/No];
- Format [.jpg/.mp4/.pdf/.epub/.mp3/.png/.html/.docx/.m4a]; and,
- Content type [app package/audio/banner/bulletin/image/infographic/instructional material/list of websites/magazine/nasheed/newsletter/photoset/video/written publication].

To ensure consistency of approach, all coding was completed by one researcher, and then reviewed by the other researcher.

Prior to its commencement, the project received ethical approval from Swansea University. Ethics arrangements included: (1) access was limited to public channels and private channels with publicly available joinlinks (where no engagement with the channel administrator was necessary to join); and (2) any content that fell within the scope of the Terrorist Content Analytics Platform was added to it. The effect of this was to alert companies to the presence of terrorist content on their platform.

4. FINDINGS

AN OVERVIEW OF THE DATASET

During the two-month data-collection period, a total of 4,164 posts were collected (an average of 70.57 posts per day). Of them, 2,312 (55.52%) shared the content via an outlink,[5] compared with 394 (9.46%) which shared the content via an inlink.[6] The remaining 1,458 (35.01%) posts were collected from one-way or interactive channels, with the content attached to or embedded in the post.

To calculate an enforcement rate, one week after the completion of data collection each of the 4,164 posts was checked to see whether the content it shared was still available. For 2,604 of the posts, the content was still available – which means that, as of 28 March 2023, the enforcement rate was 37.47%. However, this overall figure obscures a considerable difference between the various methods for sharing content. For outlinking posts, the enforcement rate was 67.61%,[7] compared with a rate of 4.67% for in-channel posts and 0.51% for inlinks.

Table 2: An overview of the dataset

No. of platforms from which posts were collected	4
No. of posts	4,164
No. of outlinking posts	2,312
No. of inlinking posts	394
No. of posts with content embedded or attached	1,458
No. of distinct items of propaganda shared	796
Enforcement Rate	37.46%
- Outlinks	67.61%
- Inlinks	0.51%
- In-channel posts	4.67%

5 A URL leading to content hosted on a different platform.

6 A URL leading to content hosted on the same platform.

7 This rate may in part be a result of the fact that any content that fell within the scope of the Terrorist Content Analytics Platform (TCAP) was added to it, thereby notifying the host platform of its presence. At the same time, however, unofficial content fell outside the scope of the TCAP and it is not always possible to send companies a TCAP alert (e.g., if their platform provides no referral mechanism or other contact details).

The 4,164 posts shared a total of 796 distinct items of propaganda. For the purposes of this count, items that had been created to promote another publication were regarded as being distinct from the item they were promoting. So, a banner promoting a new issue of a newsletter was counted as one item and the newsletter itself was counted as a separate item. Similarly, a trailer promoting a propaganda video was counted separately from the video, as were infographics summarising a publication or video. The dataset also contained some photosets and videos that compiled a number of still images. Each photoset and compilation video was counted as one item, with the individual images counted as distinct items only if there were posts in the dataset that shared the image in its own right. By contrast, where a publication (such as a newsletter) was shared using a series of images/screenshots of individual pages, this was counted as a single item (a newsletter).

Table 3 shows the breakdown of the propaganda items by group. For the purposes of this study, distinct branches of Islamic State and Al-Qaeda were grouped together. This reflects the desire to identify broad patterns and trends in propaganda dissemination, and should not be taken as diminishing the significance of the differences between various factions. Following this approach, the Islamic State (IS) umbrella encompassed a total of ten branches and affiliates,[8] while the Al-Qaeda (AQ) umbrella covered four.[9] All content gathered relating to Al-Shabaab originated from its central group and sole official media outlet.

8 Islamic State Khorasan Province, Islamic State Pakistan Province, Islamic State East Asia, Islamic State Yemen, Islamic State Central Africa Province, Islamic State West Africa Province, Islamic State Somalia, Islamic State Al-Sham, Islamic State Mozambique, and Islamic State Sahel.

9 Al-Qaeda in the Arabian Peninsula, Al-Qaeda Islamic Maghreb, Al-Qaeda in the Indian Subcontinent and Al-Qaeda central.

Table 3: Items of propaganda by group

Islamic State	715
Al-Qaeda	54
Al-Shabaab	27
Total	**796**

Of the 796 items of propaganda, the vast majority (715; 89.82%) were created by or in support of IS. The remainder were created by or in support of AQ (54; 6.78%) and Al-Shabaab (27; 3.39%).

Table 4 shows the proportions of items that were official and unofficial content. Here, items were classed as official if they were branded with the logo or symbol of a known media entity belonging to the group in question. Items were classed as unofficial if they were supporter-generated. The majority of them were official content (577; 72.49%), while 143 (17.96%) were unofficial. For 76 items (9.55%), it was not possible to determine whether the content was official or unofficial.

Table 4: Items of propaganda by official/unofficial

Official	577
Unofficial	143
Unclear	76
Total	**796**

All of the AQ and Al-Shabaab propaganda items were official content. All of the unofficial content was produced in support of IS.

DISSEMINATION STRATEGY

Different methods were employed to share the propaganda items. Outlinks and inlinks were used, and content was also shared by either attaching it to a post or embedding it in one.[10] The dataset was examined to determine how each individual item of propaganda was shared, with a distinction drawn between posts in a one-way channel and posts in an interactive channel. The results are shown in Table 5.

Table 5: Items of propaganda by dissemination strategy

SINGLE STRATEGY		MULTIPLE STRATEGIES	
Outlinking only	85	Outlinking & post in one-way channel	55
Inlinking only	29	Outlinking & post in interactive channel	6
Post in one-way channel only	275	Inlinking & post in one-way channel	1
Post in interactive channel only	277	Post in one-way channel & post in interactive channel	52
		Outlinking, post in one-way channel & post in interactive channel	13
		All strategies	3
Total	**666**	**Total**	**130**

The first point to note from Table 5 is that the majority of the items (666; 83.67%) were shared using a single method. Of the items that were shared via a single strategy, by far the most common methods were posts in one-way channels (275 items; 34.55%) and posts in interactive channels (277 items; 34.80%). Inlinking was infrequent, and less than a quarter of the items in the dataset were shared by

10 A URL is not employed in the process of creating a post with content attached/embedded. It should be noted, however, that it is possible to extract a URL from such a post. This URL could then be shared with other users to signpost them to the post/content. For example, it would be possible to extract a link to an image embedded in a post in a messaging channel, which could then be shared as an outlink or inlink.

outlink.[11] The large proportion of posts in the dataset that contained an outlink (see Table 2) does not, therefore, indicate that this is the most common method used to share terrorist content: rather, it reflects the fact that, when outlinking *is* used to share an item, large batches of URLs are often generated and disseminated for individual items of content (Macdonald et al. (2022b)). Consistently with the findings of previous studies, when outlinking was used the most common domains were file-sharing, archiving and messaging services – although it is worth noting that this study also found outlinks being posted to direct users to terrorist-operated websites.[12]

A relatively small proportion of items (130; 16.33%) were shared using a combination of the dissemination strategies. Within this, only 13 items were shared using three strategies, and just three items were shared using all four strategies. When a combination of strategies was used, it was normally in a post in a one-way channel accompanied by one of the other dissemination methods (124 items; 95.38% of the items that were shared using multiple strategies). When content was shared using an in-channel post and an inlink/outlink, the content was almost invariably shared either by in-channel post first or by in-channel post and inlink/outlink simultaneously (with simultaneous here meaning posted by the same user, in the same channel, within the space of three minutes).[13] In these instances, it would seem that in-channel posts are intended for immediate

11 Including the use of multiple dissemination strategies, a total of 162 items were shared by outlink (20.35% of the dataset).

12 The top 30 most shared URLs included seven outlinks to terrorist-operated websites, while two terrorist-operated websites appeared in the top 30 most outlinked to domains. On the apparent recent increase in the use of terrorist-operated websites, see Conway and Looney (2021) and Tech Against Terrorism (2022a).

13 Seventy-eight items were shared using a combination of in-channel post and inlink/outlink. For 55 (70.51%) of them, an in-channel post and outlink were posted simultaneously. The in-channel post appeared before the inlink/outlink for 20 (25.64%) of the remaining items – it was rare to see content shared first by inlink/outlink, and then later by in-channel post. Of the 130 items shared using multiple dissemination strategies, just three (2.31%) were shared first by outlink. None were shared first by inlink.

consumption, with inlinks/outlinks serving two other purposes: first, to provide a convenient means of sharing the item on other platforms; and second, to ensure stable future access to copies of the content stored elsewhere.

CONTENT TYPE AND FORMAT

Table 6 breaks down the propaganda items by file format. By far the most common format was .jpg (549 items), followed by .mp4 (145 items), .pdf (67 items), .epub (54 items) and .mp3 (38 items). There was also one app package, which consisted of four android application packages, one SQL database file and two .xml files. For operational security, these were not accessed. It was not possible to discern the nature of the apps/files from the information that was available.

Table 6: Items of propaganda by dissemination strategy

.jpg	549
.mp4	145
.pdf	67
.epub	54
.mp3	38
.png	24
.html	7
.docx	3
.m4a	2
App package	1
Total	**890**

A total of 67 of the items of propaganda were shared in multiple formats. For example, an English translation of the editorial in issue 377 of IS's *Al-Naba* newsletter was shared in four file formats (.pdf, .epub, .png and .jpg), while the 8th edition of as-Sahab media's

One Nation magazine was shared as both a .pdf and a .docx file. For this reason, the total shown in Table 6 (890) is greater than the number of individual propaganda items (796).

Table 7 breaks down the propaganda items by content type.

Table 7: Items of propaganda by content type

	AL-SHABAAB	AQ	IS	TOTAL
App package	-	-	1	1
Audio	-	-	19	19
Banner	8	7	42	57
Bulletin	-	13	240	253
Image	-	3	71	74
Infographic	-	-	51	51
Instructional material	-	-	7	7
List of IS websites	-	-	1	1
Magazine/newsletter	-	2	31	33
Nasheed	-	-	19	19
Photoset	-	4	56	60
Video	18	14	113	145
Written publication	1	11	35	47
Composite items				
Banner and infographic	-	-	2	2
Bulletin and infographic	-	-	5	5
Bulletin and photoset	-	-	21	21
Photoset and infographic	-	-	1	1
Total	**27**	**54**	**715**	**796**

In broad terms, there were five types of content: textual, visual, video, audio and promotional. In addition, there were three types of miscellaneous item and 29 composite items.

Textual content

Bulletins were the most common type of propaganda item in the dataset. They consisted of short statements outlining the group's recent activity – most commonly, attack claims. There were 253 bulletins in the dataset. Thirteen of these were AQ content, of which 11 were official content, while the status of two was unclear. The AQ bulletins were all in the same format (.jpg) and all disseminated by post in a one-way channel. The other 240 bulletins were IS content. The IS bulletins were mostly official content (212 items; 88.33%),[14] they were shared almost exclusively by in-channel posts,[15] and 237 of them were shared as .jpg files only.[16]

The dataset included a total of 33 issues of magazines and newsletters. Two of these were issues of the AQ magazine *One Ummah*. The other 31 were issues of the IS magazines *Voice of Khorasan, Serat Ul Haq* and *The Last Front of Baghuz*, and the *Al-Naba* newsletter.

Nineteen of the magazines were available in both .pdf and .epub formats, with a further ten available both in these formats and also as a .jpg file.[17] Compared with the dataset as a whole, it was relatively

14 Twenty-five (10.42%) were unofficial. The status of the remaining three (1.25%) was unclear.

15 One hundred and twenty-five (52.08%) were shared only by post in a one-way channel, 82 (34.17%) were shared only by post in an interactive channel, and 20 (8.33%) were shared by posts in both types of channel. Eleven bulletins (4.59%) were shared by simultaneous post in a one-way channel and outlink. Just two (0.83%) of the IS bulletins were shared by outlink only, and none was shared by inlink.

16 One of the other three was shared in .jpg, .pdf and .epub formats. Of the remaining two, one was shared in .pdf and .epub formats, and one as a .png file.

17 Of the remaining four, two were available only as .jpg files, one was available only as a .pdf file, and one was available in .docx and .html formats.

common for magazines to be disseminated using multiple strategies. Less than half of the magazines (14 items; 42.42%) were shared using a single method, compared with more than three-quarters of the dataset as a whole (666 items; 83.67%). Only three items in the whole dataset were shared using all four dissemination methods; two of these were magazines. Post in a one-way channel (27 items) and outlinking (18 items) were the most commonly used methods, followed by post in an interactive channel (11 items) and inlinking (four items). The most common combination of dissemination strategies was outlinking and post in a one-way channel (nine items).

The remaining textual items were classed under the heading 'written publications'. There were 47 items in this category, which included such things as editorials, translations of other items of propaganda, transcripts of speeches, statements and biographies. The different groups' publications generally followed one particular dissemination strategy.[18] AQ publications were shared only by outlink, by post in a one-way channel, or by a combination of the two.[19] By contrast, the most common dissemination method for IS publications was post in an interactive channel.[20]

Visual content

Seventy-four items in the dataset were classed as images. Three of them were AQ content.[21] Each featured a 'martyr', was a .jpg file and was shared by post in a one-way channel. The other 71 were all IS images. These included: photos (e.g., of IS 'martyrs', IS soldiers, IS attacks, prisoners and weapons), stills from IS videos

18 The one Al-Shabaab item was shared by outlink only.

19 Of the 11 AQ publications, four were shared by outlink only, four were shared by post in a one-way channel only, and three were shared by outlink and post in a one-way channel.

20 Of the 35 IS publications, 22 (62.86%) were shared by post in an interactive channel. The other 13 publications were shared by outlink only (four items), outlink and post in a one-way channel (four items), post in a one-way channel (three items), outlink and post in both types of channel (one item) and inlink (one item).

21 One official, one unofficial and one whose status was unclear.

and motivational-type quotes against a background image. Some of the images had superimposed usernames or emojis. Sixteen of these images were official IS content, while 38 were unofficial; the status of the remaining 17 was unclear. All but two of the IS images were .jpg files; one of the others was a .png file and the remaining one was shared in both .pdf and .epub formats. The IS images were mostly shared by post in an interactive channel (50 items), with the remainder shared by post in a one-way channel (18 items) and by inlink (three items).

The other type of visual content was photosets, of which there were 60 in the dataset. Four of these were official AQ content: they were .jpg files and were shared by post in a one-way channel. Of the other 56 photosets, 55 were official IS content, with one further unofficial photoset produced in support of IS. All were available as .jpg files. The IS photosets were disseminated primarily by post in a one-way channel.[22]

Video content

There were 145 videos in the dataset, all of which were shared as .mp4 files. The majority (113) were IS videos, with the remainder consisting of 14 AQ videos and 18 Al-Shabaab videos. All of the Al-Shabaab videos were official content produced by the Al-Kataib foundation. The AQ videos were also all official content, produced mainly by as-Sahab media and the Al-Malahem foundation, while an additional one was a video compilation of content from one of their magazines. By contrast, just over half of the IS videos (58; 51.33%) were official content, compared with 32 (28.32%) that were unofficial.[23]

22 Thirty-one (55.36%) were shared only in this way, with a further 13 (23.21%) shared via posts in both types of channel and two (3.57%) shared by post in a one-way channel and outlink. The remaining ten (17.86%) IS photosets were shared via post in an interactive channel only. None of the photosets were shared by inlink.

23 It was unclear whether the remaining 23 (20.35%) IS videos were official content or not.

All 14 of the AQ videos were shared in the same way: solely by outlinking. The Al-Shabaab videos were disseminated in a similar manner: 14 exclusively by outlinking and four by a combination of simultaneously outlinking and posting in a one-way channel. These groups' pattern of dissemination may be contrasted with that of IS: outlinking did play a significant role in the dissemination of IS propaganda videos, 34 (30.09%) of which were shared by outlink (22 of these were shared *only* by outlink),[24] but the group's most prevalent form of dissemination was by post in an interactive channel, with 79 (69.91%) of its videos shared in this way (69 of these were shared *only* by post in an interactive channel).[25] Of the IS videos posted in interactive channels, 40 were official videos, 21 were unofficial and the status of the remaining 18 was unclear.

Audio content

There were 38 items of audio content in the dataset, comprising 19 nasheeds and 19 other items. All were produced by or in support of IS. For the majority of items, it was unclear whether the content was official or not.[26] All 19 nasheeds were shared in the .mp3 format. Of the other 19 audio items, 17 were shared only as .mp3 files, while the other two were shared in both .mp3 and .m4A formats. These other audio items mainly consisted of speeches (including by

24 The other 12 were shared by: outlink and post in an interactive channel (five items); outlink and post in both types of channel (four items); outlink and post in a one-way channel (two items); all four modes of dissemination (one item).

25 The other ten were shared by: post in an interactive channel and outlink (five items); post in both types of channel and outlink (four items); all four modes of dissemination (one item).

26 Thirteen of the 19 nasheeds were classified as unclear, as were 12 of the other 19 audio items.

Abu Omar Al-Baghdadi, Abu Muhammad Al-Adnani, Abu Hamza Al-Qurashi, Abu Musab Al-Zarqawi and Abu Al-Hasan Al-Muhajir),[27] songs and audio versions of written publications.

The dissemination pattern for audio content differed markedly from that of other content types. Of the 796 items of propaganda in the whole dataset, a total of just 33 (4.15%) were shared by inlink.[28] By contrast, 17 (44.74%) of the 38 audio items were shared by inlink.[29] As explained in Section 5, this reflected the use of inlinks to produce catalogues of audio content.[30]

Promotional material

There was a total of 57 banners in the dataset, of which 56 were .jpg files.[31] Banners typically took the form of an elongated rectangular image that promoted an item of propaganda. They generally appeared alongside a post that shared the item being publicised, or in anticipation of the release of a video or magazine in the coming days, as a visual way of encouraging users to engage with the content. Eight of the banners in the dataset were posted by Al-Shabaab, all of them promoting videos produced by the Al-Kataib foundation. The seven banners posted by AQ promoted mostly videos, but also a biography,

27 There were also speeches by Anwar Al-Awlaki. These were posted in pro-IS channels and so were classified as IS content, notwithstanding his AQ affiliation. Content featuring Al-Awlaki is known to be popular among IS supporters.

28 Of which, 29 were shared only by inlink.

29 Eight of the nasheeds were shared by inlink only. Nine of the other audio items were shared by inlink only.

30 The other most common dissemination method for audio content was by post in an interactive channel, with nine nasheeds and six other audio items shared in this way. The other two nasheeds were shared by outlink (one item) and by post in a one-way channel (one item). The other four audio items were shared by outlink only (one item), by outlink and post in an interactive channel (one item), and by outlink and post in a one-way channel (two items).

31 The other was available in .pdf and .epub formats.

and an obituary. The IS banners also promoted videos, as well as photosets and regular publications including the *Al-Naba* newsletter and *Voice of Khorasan* magazine.

Banners were almost exclusively found embedded in posts, so that they were immediately visible to users. This reflects their purpose: to publicise other items and generate engagement. Twenty-nine (50.88%) of the banners were shared in posts in one-way channels, 18 (31.58%) in posts in interactive channels, and eight (14.04%) in posts in both one-way and interactive channels. Two items (3.51%) were shared via inlinks. None were shared by outlink.

Infographics were also used to promote content. There were 51 infographics in the dataset, all of which were produced by or in support of IS. By far the most common file type was .jpg, with 46 (90.20%) of the infographics available in this format (and 36 of these available only in this format). The next most common format was .png, with 12 (23.53%) (and five of the infographics available only in this format).[32] They often accompanied new issues of *Al-Naba* (15 items),[33] offering summaries and translations of the newsletter's content. Infographics such as *Al-Naba*'s regular 'Harvest of the soldiers' detail attack claims by IS and the supposed numbers of casualties inflicted. Other infographics relate to advice on adherence to group norms, or give visual summaries of weekly or monthly propaganda bulletins.

As with banners, the primary method for disseminating infographics was to embed them in posts. Twenty-nine (56.86%) of the infographics were shared only by post in a one-way channel (15 items), interactive channel (six items) or both types of channel (eight items). The other 22 infographics were shared by outlink.[34]

32 Forty-one of the infographics were shared in a single file format, with seven shared in two formats and three in three formats. The other file formats used were .pdf (three items) and .epub (the same three items).

33 The dataset contained a total of 12 editions of *Al-Naba*.

34 Of these 22, ten were shared only by outlink, with the remainder also shared by post in a one-way channel (eight items) and post in both types of channel (four items).

This perhaps indicates that some infographics are regarded as having a wider significance than just as a means of signposting users towards other items of content. As well as this promotional function, they also have some intrinsic value as standalone items that the groups' supporters can appreciate, irrespective of whether these users go on to view the propaganda items on which the infographics are based.

Miscellaneous

The dataset also included seven items of unofficial IS content that provided instruction. This instructional material tended to offer IT advice, covering subjects such as the use of encrypted services and anti-virus software, and how to code, although there was also one item that explained how to create a firing circuit from a cell phone as a potential component of an IED. This instructional material was all shared by outlink.[35]

There were two other miscellaneous items. One was the app package mentioned above; the other was a list of IS websites. It was unclear whether this list was official content or not.[36]

Composite items

Composite items combined two distinct pieces of content in a single file. There were four types of composite item in the dataset. The most common type combined a bulletin with a photoset (21 items). All were in .jpg format. Eighteen of these (85.71%) were official IS content. They were disseminated by outlink (three items), by post in a one-way channel (nine items), or both (six items). The other three bulletin/photoset amalgams were unofficial IS content and were disseminated only by post in an interactive channel.

35 One of the items was also shared by post in a one-way channel.

36 The list was shared by inlink and by a post in a one-way channel, in .pdf and .epub formats.

The other types of composite combined an infographic with either a bulletin (five items), a banner (two items) or a photoset (one item). All of these were official IS content and were available in .jpg format only. All eight were shared by post in a one-way channel, with three simultaneously shared by outlink as well.

5. DISCUSSION

DIFFERENCES BETWEEN GROUPS

This dataset focused on content produced by or in support of three terrorist entities: IS, AQ and Al-Shabaab. The stark difference between AQ and Al-Shabaab, on the one hand, and IS, on the other, illustrates the importance of tailored regulatory strategies. A one-size-fits-all approach is not possible. The Al-Shabaab items were all official content, with an almost exclusive focus on videos produced by the Al-Kataib foundation and banners promoting them. The format of the AQ content was more diverse, encompassing bulletins, magazines and other written publications, images and photosets, as well as videos and promotional banners – but again the items were almost exclusively official content and the volume was limited. This emphasis on official content is consistent with the two groups' dissemination strategies, which focused entirely on the use of outlinks and posts in one-way channels. In other words, the mode of communication was unidirectional and hierarchical, and it relied on branded official content – a practice that has been shown to lend itself more readily to moderation strategies that employ image or logo recognition (Thorley and Saltman 2023).

This may be contrasted with IS. As well having a far greater volume of content, the IS items encompassed both official and unofficial output and utilised a more diverse range of formats. The sharing of nasheeds and other audio items, infographics and instructional material was unique to IS, while the number of other types of item such as bulletins, images, photosets, videos, magazines and newsletters was far greater for IS than for the other two groups. This finding is wholly consistent with previous scholarship on IS's media strategy, and reflects the much larger, more diverse and more globally networked structure associated with IS (e.g., Whiteside, Winter and Ingram 2020). In terms of dissemination, while IS made use of outlinking and posts in one-way channels, it also made extensive use of posts in interactive channels. This is in keeping with contemporary uses of social media and the emergence of "prosumers"

(i.e., those who produce content as well as consuming it: Conway 2017, 86), and also with IS's more diffuse approach to membership (Winter 2017).

OUTLINKING

Previous studies have highlighted the use of outlinks to circumvent platforms' content moderation efforts and to enable resilient content storage and dissemination. This report has further advanced this understanding of outlinking, by examining its use on four hitherto under-researched platforms and placing it in a wider context by comparing it with other methods of sharing content. While a majority (55.52%) of the posts in the dataset contained outlinks, this is in large part due to the distribution of large batches of outlinks for single pieces of content, and it obscures the fact that outlinking as a method for sharing content was used for less than a quarter (162 items; 20.35%) of the items of propaganda. For some types of content – in particular bulletins, banners and photosets – outlinks were rarely employed.

Nonetheless, there are some important respects in which outlinking continues to play a significant role. For Al-Shabaab, outlinking was the predominant method of content dissemination.[37] It was also used regularly to share AQ content,[38] and was the only method used to disseminate the 14 official AQ videos in the dataset. Outlinking was also used widely in the dissemination of IS videos, as well as IS magazines and infographics. All of the IS instructional material was also shared using outlinks. And outlinks were frequently posted simultaneously with in-channel posts that shared the same item of content, apparently as a way of providing followers with a shareable link to the content that had just been posted and to ensure secure access to a back-up copy for the future. Collaborative efforts

37 Of the 27 Al-Shabaab items in the dataset, 19 (70.37%) were shared by outlink and eight (29.63%) were not.

38 Of the 54 AQ items in the dataset, 23 (42.59%) were shared by outlink and 31 (57.41%) were not.

to deactivate URLs sharing terrorist content thus remain important, especially for certain groups and content types. The inclusion of URLs within GIFCT's hash-sharing database is therefore welcome.

The ongoing use of URLs to share terrorist content raises the question why the enforcement rate for the outlinks in this study was not higher than 67.61%, given that all URLs were shared with Tech Against Terrorism for inclusion in the TCAP – which alerts the company in question to the presence of the content on its platform. There are several contributory factors. At the time of this study, the TCAP was limited to official content only, so URLs leading to unofficial content would have been deemed to be out-of-scope.[39] Even for official content, in some instances it is not in fact possible to alert a platform; there may be no referral mechanism and no contact details or identifying information on the company's site.[40] Even when an alert is sent, companies may lack the capacity or the willingness to act upon it. Resource constraints may also lead to delays in removing content, which is relevant here given that we calculated the enforcement rate one week after the end of our data collection period. Some of the content that was still available then may not be so now. What is clear, however, is that there is potential to increase the enforcement rate significantly, which demonstrates the importance of upscaling the TCAP and Tech Against Terrorism's outreach, mentoring and capacity-building work more generally.

39 In July 2023 it was announced that the TCAP inclusion criteria would be expanded to include unofficial content. For further information, see Tech Against Terrorism (2023b).

40 It is striking that, from November 2020 to January 2023, Tech Against Terrorism identified 39,964 URLs hosting terrorist content, yet it sent only 22,615 alerts (a rate of 57%) (Tech Against Terrorism 2023a). This seems in large part to be due to the difficulty of identifying a point of contact at content-hosting platforms.

INLINKING

Of the content-sharing methods examined in this report, inlinking was by far the least frequent. Across the four platforms from which data were collected, content-sharing inlinks were found in just 394 (9.46%) of the 4,164 posts collected. Of the 796 items of propaganda that were shared within the dataset, just 33 (4.15%) were shared by inlink. Importantly, the enforcement rate for inlinking was extremely low, at just 0.51%. In other words, of the 394 inlinks in the dataset, the content was still available for 392 of these (as of 28 March 2023, one week after the end of our data collection period). This is a lower level of enforcement activity than for the other methods of content dissemination.

Of the 394 inlinks in the dataset, 145 (36.80%) were posted on the same archiving platform. The fact that this company received TCAP alerts informing it of the presence of this content on its platform raises important questions regarding its content moderation efforts. The company's Terms of Use stipulate that, by using the service, users agree not to act in a way that "might" give rise to criminal liability. Of course, criminal laws vary in different national jurisdictions, and users may make use of a VPN or other technology to conceal their location. But the company's Terms of Use do not require proof that a terrorism offence *has* been committed, only that a criminal offence *might* have been. In many countries it is a criminal offence to provide support for a terrorist organisation and/or to encourage the commission of acts of terrorism.[41] It is difficult, therefore, to reconcile the company's Terms of Use, on the one hand, with, on the other, its apparent willingness to allow channels to maintain a stable presence on the platform notwithstanding their overt support for groups that have been internationally designated as terrorist organisations.

41 At the international level, Article 5 of the Council of Europe Convention on the Prevention of Terrorism requires member states to criminalise "public provocation to commit a terrorist offence".

A further concern about the use of inlinking is its potential to create a filter bubble effect. Many of the inlinks collected for this report, including those described in the previous paragraph, were included in posts beneath another item of content – so that after viewing one item users could then choose to view another, similar item on the same platform. In fact, some of these posts provided catalogues of similar content. This was the case, for example, with the nasheeds contained within the dataset. Inlinking was thus used to generate a filter bubble effect. At a time when much concern is being expressed about the potential for algorithmic recommender systems to create echo chambers and take users down the 'rabbit hole' (O'Callaghan et al. 2015; Ledwich and Zaitsev 2019; Whittaker et al. 2021), it is important that manual efforts to use inlinks to do something similar are not overlooked.

This leads to an important caveat about the relatively low numbers of inlinks within the dataset for this report. To be included in the study, a post must have shared *content*. For this reason, a number of posts containing inlinks were filtered out because they linked, not to content, but to other channels on the same platform. This observation is consistent with the use of inlinking noted by Weirman and Alexander (2020) in their study of Twitter. The number of inlinks in our dataset may therefore not reflect the true prevalence of inlinking, because our focus on the sharing of content does not capture the purpose for which inlinking is most commonly used: to direct users to other channels. If this hypothesis is correct, it would significantly increase concerns about a filter bubble effect. This is an area that requires further, dedicated research.

IN-CHANNEL POSTS

Roughly one third of the posts in the dataset had terrorist content attached or embedded.[42] This seemingly small proportion should not overshadow the fact that in-channel posts were the most significant

42 The total number of posts with content attached or embedded was 1,458, which constituted 35.01% of the dataset (see Table 2).

content-sharing method. Of the 796 items of propaganda in the dataset, just 114 (14.32%) were not shared using in-channel posts. Bulletins, banners and images were almost exclusively shared in this way, while it was the primary means of dissemination for IS videos, IS written publications, photosets, infographics and composite items. This is even more significant given that not only were these content types the most numerous within the dataset, but they also promote other content and present information in an easily accessible and digestible manner well suited to contemporary social media.

In spite of this steady flow of posts with terrorist content attached/embedded,[43] as of 28 March 2023 (one week after the end of data collection) all 12 of the channels from which data had been collected remained live. Moreover, the enforcement rate for posts with terrorist content attached/embedded was only 4.67% – i.e., the content from 1,390 of the 1,458 posts remained available. So users within these channels had stable access to the latest news, updates and propaganda releases, without having to click on outlinks that would take them to other platforms.

The existence of channels like these has some utility for security agencies and law enforcement. They offer an opportunity to gain information on the terrorist groups and their supporters – especially as many overestimate the level of anonymity they enjoy online (Benson 2014). Indeed, recent studies have found that groups that engaged in an online network were far less likely to succeed in their plot than those that did not (Kenyon, Binder and Baker-Beall 2022; Whittaker 2021). Moreover, deplatforming can have unintended consequences, such as driving these users to more clandestine areas of the internet and spurring greater technological innovation and sophistication (Whittaker and Craanen, under review). On the other hand, there are dangers inherent in allowing such channels to function without disruption. As one recent empirical study of individuals convicted of extremism offences in the UK found,

43 Eight of the 12 channels from which data were collected averaged at least two posts with content attached/embedded per day throughout the data collection period.

the internet is playing an increasingly prominent role in radicalisation processes, and radicalisation now takes place primarily online (Kenyon, Binder and Baker-Beall 2022). And to allow these channels to operate without disruption would send a mixed moral message.

However, even if the aim is to shut down channels such as these, there remains the question how to do this. As stated above, the archiving site that hosted three of the channels examined in this study (channels 1–3 in Table 1) appears unwilling to remove the vast majority of the content on its platform that supports IS, or to close the channels that host this content.[44] The provider of the messaging service that hosted three of the other channels (nos 6–8 in Table 1) – a European start-up company – appears to be similarly unwilling, and the remaining two platforms from which data were collected were hosted on a decentralised server. In recent years, legislation at both the national level (e.g., Germany's Netz DG law and the UK's Online Safety Act) and the transnational level (e.g., the EU's Terrorist Content Online Regulation) have been enacted, in order to provide strong powers of enforcement against companies that fail to moderate terrorist content on their platforms adequately. While in most cases strong enforcement powers are likely to induce compliance (Watkin 2023), it is also the case that not all content-sharing platforms will fall within the scope of these regulatory regimes. Some regimes apply only to services with a minimum number of users, which may place smaller platforms out of scope.[45] Most also apply only to services that disseminate content to the public.[46] This raises the important question whether content posted in channels that may be ostensibly labelled as private, and which are difficult and time-consuming to locate, but which can be accessed using openly available joinlinks

44 All of the content shared in channels 1–3 was posted by or in support of IS.

45 For example, Germany's NetzDG law applies only to platforms with over two million users.

46 The EU Terrorist Content Online Regulation is targeted at the dissemination of terrorist content to the public (Article 1(1)). Terrorism Content Notices under the UK's Online Safety Act apply only to public communications (section 207). And Germany's NetzDG law applies to platforms that make content available to the public (section 1).

and without any engagement with the channel administrator, are properly regarded as public (Macdonald and Hall forthcoming). If not, it may be that the disruption efforts and subsequent adversarial shifts of recent years are beginning to reach an equilibrium.

6. CONCLUSION

ANALYSES OF ONLINE extremist ecosystems have drawn attention to the use of outlinking to disseminate terrorist content. Collaborative initiatives have been developed in an effort to buck this trend, most notably the TCAP, with GIFCT also operationalising the hashing of URLs from the TCAP so that member companies are alerted to URLs that lead to terrorist content. This is important work that must be maintained, especially as outlinking continues to be used widely for some types of content and remains the primary means of dissemination for some groups. In fact, the enforcement rate found in this study indicates that there is scope to improve the disruption of outlinking to jihadist propaganda further, in three respects. First, upscaling existing initiatives such as the TCAP will make it possible to monitor a greater number of channels and identify a greater number of URLs. Second, it is often impossible to alert companies to the presence of terrorist content on their platforms because of the lack of a referral mechanism, contact details or identifying information. In this respect, it is welcome that the EU's Digital Services Act requires providers of intermediary services to designate a point of contact and to make their contact details publicly available.[47] The extent to which this requirement is enforced in practice remains to be seen. Third, even where an alert is sent, the platform in question may lack the capacity and/or the willingness to act upon it. As well as stipulating norms and prohibitions, regulatory strategies must make provision for capacity building and for incentivising recalcitrant platforms (Watkin 2023), and must respond to the unique challenges posed by terrorist-operated websites (Tech Against Terrorism 2022b).

While maintaining efforts to disrupt the use of outlinks to share jihadist propaganda, it is also important to respond to emergent dissemination strategies. By examining the methods that were used to disseminate 796 items of Al-Shabaab, AQ and IS content, this report has provided an empirically grounded assessment of the prevalence of outlinking relative to inlinking and attaching content to, or embedding it in, in-channel posts. It has highlighted

47 Regulation (EU) 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Article 12.

the use of inlinks to create filter bubbles manually and has urged the need for further work on this phenomenon, in two respects. First, further research is needed to assess the full extent of the use of inlinks to create filter bubbles. This would consider the use of inlinks to direct users to other channels, as well as to other content. Secondly, at the policy level, it is necessary to understand and address the unwillingness of some platforms to enforce their own stated Terms of Use.

Finally, this report has also shown that in-channel posts are the predominant method for sharing content, with some content types disseminated almost exclusively in this way. The fact that neither inlinking nor in-channel posting requires the user to navigate to a different platform, coupled with the low enforcement rates observed in these channels, has allowed spaces to develop in which users can engage with – and, in some cases, contribute – content with little disruption. The desirability of disrupting these channels, where users have stable access to a steady flow of propaganda, is a question on which opinions may differ. After all, as ecosystems research has consistently shown, disrupting the dissemination of propaganda inevitably has knock-on effects – including displacement to harder-to-regulate platforms. More fundamentally, questions of desirability presuppose that disruption is feasible. For some online spaces, such as decentralised chat apps on the Rocketchat server, this may simply not be the case. For such spaces, strategies should instead focus on gaining access and maximising the utility of such access for security agencies, law enforcement and other relevant actors.

References

Amarnath Amarasingam, Shiraz Maher and Charlie Winter (2021), *How Telegram Disruption Impacts Jihadist Platform Migration* (Centre for Research and Evidence on Security Threats), https://crestresearch.ac.uk/download/3520/21-002-01.pdf.

Stephane J. Baele, Lewys Brace and Travis G. Coan (2020), "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda", *Studies in Conflict & Terrorism*, https://doi.org/10.1080/1057610X.2020.1862895.

David C. Benson (2014) "Why the Internet is Not Increasing Terrorism", *Security Studies* 23, no.2: 293–328.

J.M. Berger and Jonathon Morgan (2015), *The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter* (The Brookings Institution), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

Maura Conway (2017), "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research", *Studies in Conflict & Terrorism* 40, no. 1: 77–98, http://dx.doi.org/10.1080/1057610X.2016.1157408.

Maura Conway, 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, nos 1-2: 141–160, https://doi.org/10.1080/1057610X.2018.1513984.

Maura Conway, Moign Khawaja, Suraj Lakhani and Jeremy Reffin (2020), "A Snapshot of the Syrian Jihadi Online Ecology: Differential Disruption, Community Strength, and Preferred Other Platforms", *Studies in Conflict and Terrorism*, https://doi.org/10.1080/1057610X.2020.1866736.

Maura Conway and Seán Looney (2021), *Back to the Future? Twenty First Century Extremist and Terrorist Websites* (Radicalisation Awareness Network), https://home-affairs.ec.europa.eu/system/files/2022-03/Terrorist%20Operated%20Websites%20Workshop-paper.pdf.

Julian Droogan, Lise Waldek, Brian Ballsun-Stanton and Jade Hutchinson (2022), *Mapping a Social Media Ecosystem Outlinking on Gab & Twitter Amongst the Australian Far-right Milieu* (Resolve Network), https://www.resolvenet.org/research/mapping-social-media-ecosystem-outlinking-gab-twitter-amongst-australian-far-right-milieu.

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

GIFCT (2023), *2022 GIFCT Annual Report,* https://gifct.org/wp-content/uploads/2022/12/GIFCT-Annual-Report-2022.pdf.

Daniel Grinnell, Stuart Macdonald, David Mair and Nuria Lorenzo-Dus (2018), *Who disseminates* Rumiyah*? Examining the relative influence of sympathiser and non-sympathiser Twitter users* (European Counter Terrorism Centre), https://www.europol.europa.eu/publications-events/publications/who-disseminates-rumiyah-examining-relative-influence-of-sympathiser-and-non-sympathiser-twitter-users.

Jade Hutchinson, Julian Droogan, Lise Waldek and Brian Ballsun-Stanton (2022), *Violent Extremist & REMVE Online Ecosystems: Ecological Characteristics for Future Research & Conceptualization* (Resolve Network), https://resolvenet.org/system/files/2022-08/RSVE_REMVE_ViolentExtremistandREMVEOnlineEcosystems_Hutchinson%20et%20al.%20August2022.pdf.

Jonathan Keynon, Jens Binder and Christopher Baker-Beall (2022), *The internet and radicalisation pathways: technological advances, relevance of mental health and role of attackers* (HM Prison & Probation Service), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1121985/internet-radicalisation-report.pdf.

Mark Ledwich and Anna Zaitsev (2019), "Algorithmic Extremism: Examining YouTube's Rabbit Hole of Radicalization", https://doi.org/10.48550/arXiv.1912.11211.

Stuart Macdonald, Sara Giro Correia and Amy-Louise Watkin (2019a) "Regulating terrorist content on social media: automation and the rule of law," *International Journal of Law in Context*, 15, no. 2: 183–197.

Stuart Macdonald, Daniel Grinnell, Anina Kinzel and Nuria Lorenzo-Dus (2019b), "Daesh, Twitter and the Social Media Ecosystem: A Study of Outlinks Contained in Tweets Mentioning Rumiyah", *The RUSI Journal* 164, no. 4: 60–72, https://doi.org/10.1080/03071847.2019.1644775.

Stuart Macdonald and Jonathan Hall KC (forthcoming), "Publicising Terrorism in Private: Criminal Law, Online Safety and the Meaning of 'Public Communications'".

Stuart Macdonald, Kamil Yilmaz, Chamin Herath, J.M. Berger, Suraj Lakhani, Lella Nouri and Maura Conway (2022a), *The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German & French Far-Right Online Ecosystems* (Resolve Network), https://www.resolvenet.org/research/european-far-right-online-exploratory-twitter-outlink-analysis-german-french-far-right.

Stuart Macdonald, Connor Rees and Joost S. (2022b), *Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms* (Resolve Network), https://www.resolvenet.org/research/remove-impede-disrupt-redirect-understanding-combating-pro-islamic-state-use-file-sharing.

Derek O'Callaghan, Derek Greene, Maura Conway, Joe Carthy and Pádraig Cunningham (2015), "Down the (White) Rabbit Hole: The Extreme Right and Online Recommender Systems," *Social Science Computer Review* 33, no. 4: 459–478.

Tech Against Terrorism (2022a), *The Threat of Terrorist and Violent Extremist-Operated Websites* (London: Tech Against Terrorism), https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf.

Tech Against Terrorism (2022b), *Responding to Terrorist Operated Websites* (London: Tech Against Terrorism), https://www.techagainstterrorism.org/wp-content/uploads/2022/07/TAT-TOW-Mitigation-Strategy-July-2022.pdf.

Tech Against Terrorism (2023a), *Patterns of Online Terrorist Exploitation,* https://26492205.fs1.hubspotusercontent-eu1.net/hubfs/26492205/260423%20TCAP%20INSIGHTS%20-%20FINAL.pdf.

Tech Against Terrorism (2023b), "Launching the Terrorist Content Analytics Platform's (TCAP) Tiered Alert System", Terrorist Contents Analytics Platform, https://terrorismanalytics.org/project-news/TCAP-Tiered-Alert-Launch.

Tom G. Thorley and Erin Saltman (2023), "GIFCT Tech Trials: Combining Behavioural Signals to Surface Terrorist and Violent Extremist Content Online" *Studies in Conflict & Terrorism,* https://doi.org/10.1080/1057610X.2023.2222901.

Inga Trauthig and Lorand Bodo (2022), "Emergent Technologies and Extremists: The Dweb as a New Internet Reality?", Global Network on Extremism and Technology, https://gnet-research.org/2022/08/01/emergent-technologies-and-extremists-the-dweb-as-a-new-internet-reality/.

Amy-Louise Watkin (2023), "Developing a Responsive Regulatory Approach to Online Terrorist Content on Tech Platforms", *Studies in Conflict & Terrorism*, https://doi.org/10.1080/1057610X.2023.2222891.

Gabriel Weimann and Asia Vellante (2021), "The Dead Drops of Online Terrorism: How Jihadists Use Anonymous Online Platforms", *Perspectives on Terrorism* 12, no. 1: 81–99.

Samantha Weirman and Audrey Alexander (2020), "Hyperlinked Sympathizers: URLs and the Islamic State", *Studies in Conflict & Terrorism* 43, no. 3: 239–257, https://doi.org/10.1080/1057610X.2018.1457204.

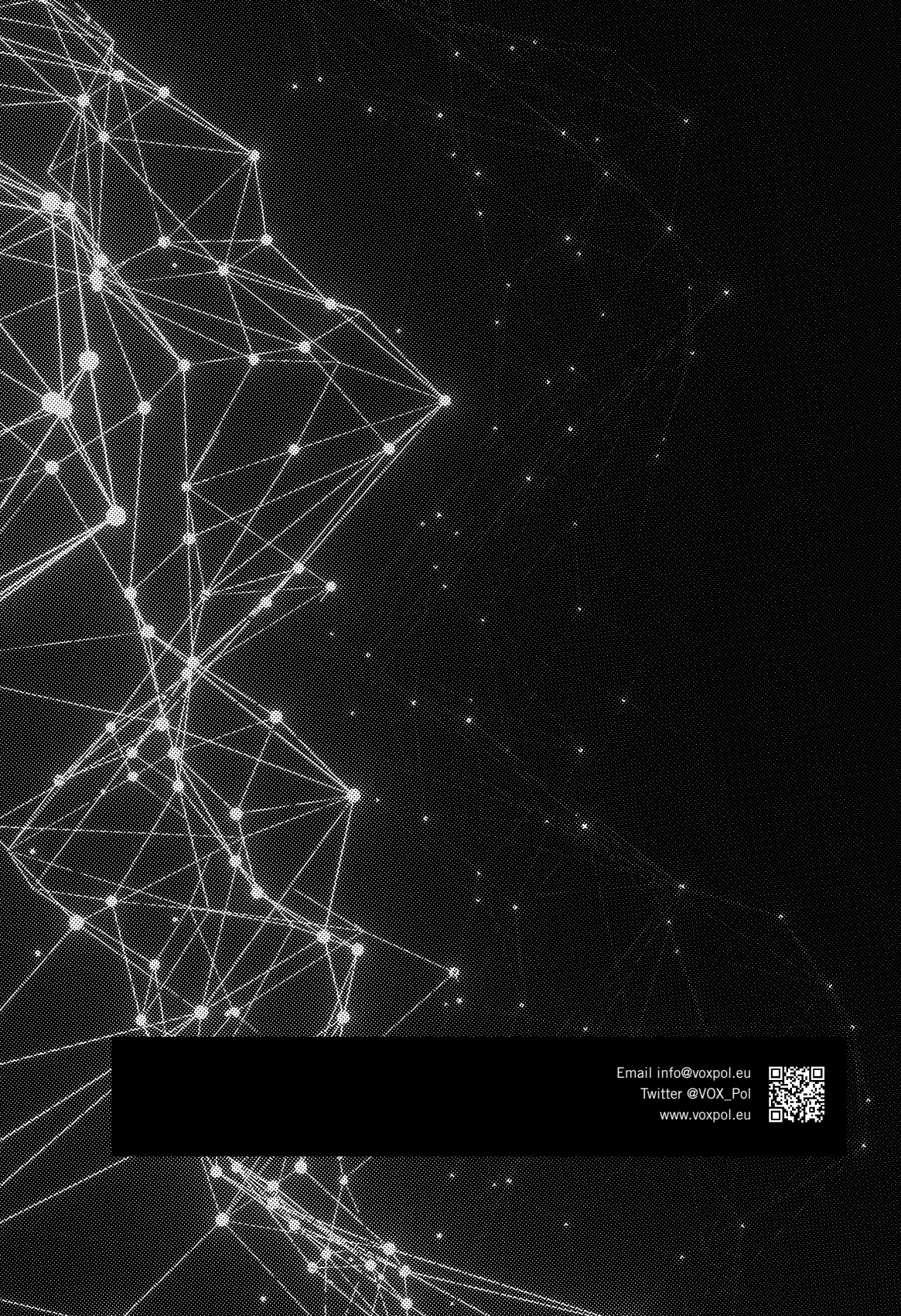
Craig Whiteside, Charlie Winter and Haroro J. Ingram (2020), *The ISIS Reader: Milestone Texts of the Islamic State Movement* (New York, NY: OUP).

Joe Whittaker (2021), "The online behaviors of Islamic state terrorists in the United States", *Criminology & Public Policy* 20, no. 1: 177–203.

Joe Whittaker and Anne Craanen (under review), "The Unintended Consequences of Content Removal, Marginalisation, and the Case of BitChute".

Joe Whittaker, Seán Looney, Alastair Reed and Fabio Votta (2021), "Recommender systems and the amplification of extremist content", *Internet Policy Review* 10, no. 2: https://doi.org/10.14763/2021.2.1565 (accessed 23 July 2023).

Charlie Winter (2017), *Media Jihad: The Islamic State's Doctrine for Information Warfare*, (London: International Centre for the Study of Radicalisation and Political Violence).



Email info@voxpol.eu
Twitter @VOX_Pol
www.voxpol.eu