RESOLVE NETWORK

# Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms

Stuart Macdonald, Connor Rees, & Joost S.

Research Report | April 2022

CYTREC
CYBER THREATS RESEARCH CENTRE

tech against terrorism

# ACKNOWLEDGEMENTS

This research was conducted through a secondment scheme hosted at the Cyber Threats Research Centre (CYTREC) at Swansea University. The scheme aimed to create space to form a multi-stakeholder team tasked with looking at the ways terrorist groups exploit the internet and uncover how to respond in a way that respects human rights. The data used to meet this aim came from the Government of Canada-funded, Tech Against Terrorism-created Terrorist Content Analytics Platform (TCAP).

The authors would like to thank HEFCW for funding the secondment scheme via the Research Wales Innovation Fund. The authors also gratefully acknowledge the support received from Tech Against Terrorism, the United Nations Counter-Terrorism Executive Directorate, Moonshot and Swansea University's Legal Innovation Lab Wales (which is part-funded by the European Regional Development Fund through the Welsh Government).

*The views expressed in this publication are those of the author. They do not necessarily reflect the views of the RESOLVE Network, acknowledged partners contributing to the production of this publication, the U.S. Institute of Peace, or any entity of the U.S. government.*

https://doi.org/10.37805/remve2022.2

# ABSTRACT

**In the face of content takedown and account suspensions on the biggest social media** platforms, terrorist groups and their supporters have resorted to the use of file-sharing sites to ensure stable access to their propaganda. Amongst those to have employed this strategy are supporters of the so-called Islamic State (IS). Yet, while studies have repeatedly highlighted the key role that file-sharing platforms play in the dissemination of IS propaganda, there has been little investigation of the strategic considerations that may influence the choice of file-sharing sites from the many available. To address this, this report uses data gathered from 13 public IS Telegram channels over a 45-day period in July - September 2021 to assess three possible strategic considerations: the features offered by different file-sharing sites (such as data storage capacity, maximum upload size, and password file protection); a platform's enforcement activity; and the ability to generate large banks of URLs quickly and conveniently. Based on these findings, the report proposes a four-pronged strategy to combat the exploitation of file-sharing sites by supporters of IS and other terrorist groups: remove terrorist content at the point of upload; impede the automated generation and dissemination of banks of URLs; disrupt the posting of these URLs on other platforms; and redirect users to other content and support services.

# INTRODUCTION

Studies of online jihadist ecosystems have consistently shown that terrorists utilize a wide variety of platforms and online services. In addition to social media, these online services include websites (including both news sites and terrorist-operated websites), messaging, video-sharing, content-hosting and URL shortening platforms.[1] An important node in the so-called Islamic State's (IS) online ecosystem is the messaging service Telegram. Following IS's "Golden Age" on Twitter in 2013 and 2014,[2] the group experienced significant levels of disruption.[3] As Twitter became a more hostile environment, IS's community-building activities were driven to other platforms, particularly Telegram.[4] Importantly, Clifford and Powell's study of IS activity on Telegram found that, while the platform was used for the purposes of interaction and communication, by far the most common purpose for which it was being used by IS sympathizers was the distribution of core IS media and other pro-IS materials. These materials were disseminated not only using Telegram's file-sharing features, but also by using "external file-sharing sites to ensure IS content remains on the internet and resilient to takedowns."[5] These findings resonated with studies of IS's outlinking practices, or use of URLs directing users on one platform to another, on Twitter, which also highlighted the central role of file-sharing platforms within the IS online ecosystem.[6]

IS has long used online platforms to share files and host a variety of content (including video, Web, text, image, and audio[7]), as have its predecessors and competitors.[8] Initially, jihadist forums and websites were used for this purpose.[9] This was followed by "the rapid adoption of other Web 2.0 tools that fostered

[1] Maura Conway et al, "A Snapshot of the Syrian Jihadi Online Ecology: Differential Disruption, Community Strength, and Preferred Other Platforms," *Studies in Conflict and Terrorism* (2020), https://doi.org/10.1080/1057610X.2020.1866736; Ali Fisher, Nico Prucha, and Emily Winterbotham, *Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability*, (London: Royal United Services Institute, 2019), https://static.rusi.org/20190716_grntt_paper_06.pdf; Stuart Macdonald et al, "Daesh, Twitter and the Social Media Ecosystem: A Study of Outlinks Contained in Tweets Mentioning Rumiyah," *The RUSI Journal* 164, no. 4 (2019): 60-72, https://doi.org/10.1080/03071847.2019.1644775.

[2] Maura Conway et al, "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts," *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 150, https://doi.org/10.1080/1057610X.2018.1513984.

[3] JM Berger and Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters* (Washington, DC: George Washington University Program on Extremism, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf.

[4] Nico Prucha, "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram," *Perspectives on Terrorism* 10, no. 6 (2016): 48–58; Audrey Alexander, *Digital Decay? Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*, (Washington, DC: George Washington University Program on Extremism, 2017), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.

[5] Bennett Clifford and Helen Powell, *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram* (Washington DC: George Washington University Program on Extremism, 2019), 24, https://scholarspace.library.gwu.edu/work/9s161692z.

[6] Conway et al, "A Snapshot of the Syrian Jihadi Online Ecology"; Macdonald et al, "Daesh, Twitter and the Social Media Ecosystem".

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

[8] Moustafa Ayad, Amarnath Amarasingam, and Audrey Alexander, *The Cloud Caliphate: Archiving the Islamic State in Real-Time* (West Point, NY: Combating Terrorism Center, 2021), https://ctc.usma.edu/wp-content/uploads/2021/05/Cloud-Caliphate.pdf.

[9] Craig Whiteside, *Lighting the Path: the Evolution of the Islamic State Media Enterprise* (2003-2016), (The Hague: International Centre for Counter-Terrorism, 2016), https://icct.nl/app/uploads/2016/11/ICCT-Whiteside-Lighting-the-Path-the-Evolution-of-the-Islamic-State-Media-Enterprise-2003-2016-Nov2016.pdf.

more genuine collaboration and participation, including file-sharing portals, podcasts, personal spaces, social networking sites, virtual worlds and the blogosphere."[10] The media department of IS "embraced the popularity of social media and other methods of reaching new audiences," creating "almost a dozen central media organs with diverse purposes, mediums, and target audiences," including al-I'tisam, who "jumped into the social media domain and began disseminating Islamic State of Iraq products on Twitter and other social media platforms in 2012."[11] As jihadist forums faced increased levels of disruption, and the biggest social media platforms ramped-up their enforcement activity, pro-IS users also began to disseminate jihadist content through uncensored file-sharing portals.[12] Conway et al. explain that file-sharing sites "act as back-up "drives" that can be resorted to when content is deleted from higher profile online spaces."[13] While a number of jihadist groups have used file-sharing sites in this way, it is a tactic that has been most heavily used by supporters of IS, in large part because of the greater disruption pro-IS users face on platforms such as Twitter.[14] The far-right has also used file-sharing platforms to circumvent disruption faced on major platforms including, most notably, the Christchurch attacker, who before his attack uploaded his manifesto to a range of smaller file-sharing sites (including ones previously used by IS and al-Qaeda).[15]

Tackling the exploitation of file-sharing sites is thus a key part of a holistic approach to disrupting the dissemination of terrorist propaganda. Yet, while existing studies have highlighted IS supporters' use of file-sharing services, research to date has largely treated these platforms as a homogeneous entity. There has been little consideration of whether there are strategic reasons for IS supporters' use of particular file-sharing platforms. Some studies have highlighted the exploitation of smaller and micro platforms,[16] but, given the plethora of such services, the question remains why some smaller platforms are used and not others. This report seeks to address this question. Drawing on previous studies of the dissemination of IS propaganda, it hypothesizes three possible strategic considerations that might motivate IS supporters' use of specific file-sharing platforms. Using data from public IS Telegram channels, the report then provides an empirically grounded examination of each of these strategic considerations in turn.

The first possible strategic consideration is the features of different file-sharing sites. Past studies have consistently found the repeated use of certain platforms, such as justpaste.it and mediafire.com.[17] This raises the question of whether there are particular features, such as data storage capacity, maximum

[10] Akil N. Awan and Mina Al-Lami, "Al-Qa'ida's Virtual Crisis," *The RUSI Journal 154*, no. 1 (2009): 59, https://doi.org/10.1080/03071840902818605.

[11] Whiteside, *Lighting the Pat*h, 18.

[12] Awan and Al-Lami, "Al-Qa'ida's Virtual Crisis," 61.

[13] Conway et al, "A Snapshot of the Syrian Jihadi Online Ecology," 12.

[14] Conway et al, "A Snapshot of the Syrian Jihadi Online Ecology," 12. See also Joe Whittaker, "The online behaviors of Islamic State terrorists in the United States," *Criminology & Public Policy* 20, no. 1 (2021): 177-203, https://doi.org/10.1111/1745-9133.12537.

[15] "Analysis: New Zealand attack and the terrorist use of the internet," Tech Against Terrorism, accessed March 7, 2022, https://www.techagainstterrorism.org/2019/03/26/analysis-new-zealand-attack-and-the-terrorist-use-of-the-internet/; Graham Macklin, "The Christchurch Attacks: Livestream Terror in the Viral Video Age," *CTC Sentinel* 12, no.6 (2019): 18-29, https://ctc.usma.edu/wp-content/uploads/2019/07/CTC-SENTINEL-062019.pdf.

[16] Stuart Macdonald, Sara Giro Correia, and Amy-Louise Watkin, "Regulating terrorist content on social media: automation and the rule of law," *International Journal of Law in Context* 15, no. 2 (2019): 183-197, https://doi.org/10.1017/s1744552319000119.

[17] Conway *et a*l, "A Snapshot of the Syrian Jihadi Online Ecology"; Fisher *et al*, *Mapping the Jihadist Information Ecosystem*; Macdonald et al, "Daesh, Twitter and the Social Media Ecosystem"; Weirman and Alexander, "Hyperlinked Sympathizers".

upload size, password file protection, or the availability of encryption or monetization, that influence IS supporters' decision to share content via specific platforms. Understanding the features of the file-sharing platforms that are most frequently utilized by IS supporters (or the absence of such features) has the potential to shed further light on their dissemination strategy. It may also enable an assessment of the vulnerability of specific platforms, helping the tech sector to know where to prioritize its capacity-building efforts and enabling file-sharing platforms to conduct risk assessments and take steps to increase their resilience before their services are exploited.

A second possible strategic consideration is the platform's enforcement activity. Do IS supporters target specific platforms because experience has taught them that content is likely to remain available on that site for a long period of time? Previous studies have found that pro-IS users face high levels of disruption, which seems to point in the opposite direction.[18] This report therefore examines the extent to which a company's enforcement activity and the longevity of URLs are a strategic consideration for pro-IS users. When IS supporters outlink to file-sharing platforms, do they do so in the expectation that the links will be deactivated, in much the same way that IS supporters utilize throwaway accounts on Twitter to disseminate links to pro-IS content on other platforms?[19]

A third possible strategic consideration is the ability of a user to generate large banks of URLs quickly and conveniently. There is evidence that pro-IS users create multiple URLs for individual items of propaganda to increase resilience against content moderation.[20] This is connected to URLs' longevity. If IS supporters do share outlinks to file-sharing platforms expecting them to be deactivated—so that they are regarded as single-use, throwaway URLs—then the ability to create repeated swathes of URLs swiftly and efficiently is likely to be a priority. Automated methods for generating and disseminating URLs, in particular, are likely to be valued.

This report uses data obtained from 13 public Telegram channels over a 45-day period in July - September 2021 to assess the salience of each of these possible strategic considerations. It begins with a review of relevant literature and a description of the study's methodology. To justify its focus on file-sharing platforms, the report then provides an overview of the dataset. This reveals both the frequency of outlinking within public IS Telegram channels and the overwhelming prevalence of file-sharing platforms within these outlinks. The subsequent analysis examines the features of the file-sharing sites that IS supporters most frequently outlink to, then tests the availability of the content that was shared via these outlinks. Finally, it highlights the important role that automation plays in pro-IS users' generation and dissemination of URLs. The report concludes by outlining a four-pronged strategy—remove, impede, disrupt, redirect (RIDR)—for combating IS supporters' propaganda dissemination strategy.

[18] Conway *et al*, "A Snapshot of the Syrian Jihadi Online Ecology"; Macdonald et al, "Daesh, Twitter and the Social Media Ecosystem".

[19] Conway *et al*, "Disrupting Daesh".

[20] Laurence Bindner and Raphael Gluck, "Trends in Islamic State's Online Propaganda: Shorter Longevity, Wider Dissemination of Content," accessed March 2, 2022, https://icct.nl/publication/trends-in-islamic-states-online-propaganda-shorter-longevity-wider-dissemination-of-content/.

# CONTEXT

Based on interview data gathered from eastern Syria in 2018, Almohammad and Winter found “a high degree of systemic standardization” in IS’s production of propaganda.[21] Similarly, in his examination of instructions from IS’s central media organization to those coordinating the group’s media efforts in Afghanistan, Milton highlighted “the group’s desire to control the creation of the message as much as possible.”[22] Milton further observed that “This stands in contrast to the group’s treatment of the propaganda dissemination process.”[23] Official IS propaganda is posted in secretive Telegram channels.[24] Following this, “the process then becomes rapidly decentralized.”[25] Pro-IS media activists and sympathizers obtain the content and seek to disseminate it.[26] Such activity has been championed by IS “as a form of worship”[27] that is “tantamount to fighting in the caliphate’s army or conducting terrorism in its name.”[28] Indeed, in his study of jihadi online culture, Ramsay identifies it as one form of jihadi online practice.[29]

As noted above, IS’s media department embraced the popularity of social media, as did other jihadist groups.[30] According to one study, as recently as late 2014, there were between 46,000 and 90,000 overt IS supporter accounts on Twitter, posting an average of 7.3 tweets per day.[31] Since then, the biggest social media companies have significantly stepped up their efforts to block and remove terrorist content from their platforms, as well as establishing the Global Internet Forum to Counter Terrorism (GIFCT).[32] Increased content moderation efforts by the major social media platforms led to an evolution in jihadist propaganda dissemination, as networks sought to maintain a persistent online presence. Writing in 2015, Fisher explained that, in the decentralized process that follows the production and release of new content, “it is often the distributing network of media mujahideen, rather than the original producer, that ensures continuing content availability.”[33] As disseminators of jihadist propaganda seek to ensure such continuing availability, their interactions aggregate into “collective behaviors which facilitate the persistent sharing of material.”[34] For the resultant networks of disseminators, three attributes are key:

[21] Asaad Almohammad and Charlie Winter, *From Battlefront to Cyberspace: Demystifying the Islamic State’s Propaganda Machine* (West Point, NY: Combating Terrorism Center, 2019), https://ctc.usma.edu/wp-content/uploads/2019/05/Battlefront-to-Cyberspace.pdf, 24.

[22] Daniel Milton, *Pulling Back the Curtain: An Inside Look at the Islamic State’s Media Organization*, (West Point, NY: Combating Terrorism Center, 2018), https://ctc.usma.edu/wp-content/uploads/2018/08/Pulling-Back-the-Curtain.pdf, 10.

[23] Milton, *Pulling Back the Curtain*, 10.

[24] Almohammad and Winter, *From Battlefront to Cyberspace*; Laurence Bindner and Raphael Gluck, “Assessing Europol’s Operation Against ISIS’ Propaganda: Approach and Impact,” accessed March 9, 2022, https://icct.nl/publication/assessing-europols-operation-against-isis-propaganda-approach-and-impact/.

[25] Milton, *Pulling Back the Curtain*, 10.

[26] Bindner and Gluck, “Assessing Europol’s Operation Against ISIS’ Propaganda”.

[27] Charlie Winter, *Media Jihad: The Islamic State’s Doctrine for Information Warfare*, (London: ICSR, 2017), https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf, 11.

[28] Winter, *Media Jihad*, 13.

[29] Gilbert Ramsay, *Jihadi Culture on the World Wide Web*, (New York, NY: Bloomsbury, 2013).

[30] Awan and Al-Lami, “Al-Qa’ida’s Virtual Crisis”; Md Sazzad Hossain, “Social media and terrorism: Threats and challenges to the modern era,” *South Asian Survey* 22, no. 2 (2015): 136-155, https://doi.org/10.1177%2F0971523117753280.

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

[32] Conway *et al*, “Disrupting Daesh”.

[33] Ali Fisher, “Swarmcast: How jihadist networks maintain a persistent online presence,” *Perspectives on Terrorism* 9, no. 3 (2015): 4.

[34] Fisher, “Swarmcast,” 4.

speed (the ability to share content to a wide network of individuals rapidly); resilience (a high level of interconnection minimizing the impact of account takedowns); and, agility (the ability to move between different platforms and use different technologies for periods of time).[35]

Given the use of different platforms by the "media mujahedeen"[36]—one study estimated that jihadist groups use more than 700 platforms to distribute their content[37]—more recent research has examined online jihadist ecosystems.[38] Fisher et al. describe the platforms within these ecosystems as performing three different roles: content stores (repositories where jihadist materials are uploaded for users to access via a link), aggregators (where collections of links to a single piece of content are gathered and shared), and beacons (which signpost other users to where jihadist materials can be located).[39] This framework is useful in explaining the consistent finding that one of jihadist groups' most outlinked to online spaces on Twitter is file-sharing platforms.[40] Outlinking is the use of URLs to take users from one online platform to another, often because the destination platform has fewer protective measures against terrorist material.[41] Jihadist groups seek to use Twitter, a social media platform with a wide reach, primarily as a beacon, posting outlinks in order to signpost users to file-sharing platforms where jihadist materials are stored.[42]

File-sharing platforms thus form a crucial part of online jihadist ecosystems, used to maintain the resilience and agility of the dissemination networks of IS supporters. A single piece of pro-IS propaganda may be stored on multiple file-sharing platforms. The focus of this report is whether there are strategic considerations that lead IS supporters to favor certain file-sharing sites. The first two hypothesized strategic considerations that are examined are features of individual platforms and their level of enforcement activity. Once pro-IS users have stored the content on file-sharing sites, it is then made accessible via dozens of unique URLs. This means that even if one URL is deactivated, the others will still lead users to the same item on the same platform, and even if the item is removed from that platform altogether, it may still be accessed on other platforms. Therefore, the third hypothesized strategic consideration is that pro-IS users value the ability to generate large banks of URLs quickly and conveniently. The result of the propaganda dissemination process that has been described is a "fragmentation" of IS propaganda that makes these materials "less trackable by authorities" and results in a "relatively closed and stable digital propaganda ecosystem."[43] File-sharing platforms have accordingly been described as "black boxes" to "enable the rapid redistribution of content even under conditions of drastic policing and filtering."[44]

[35] Fisher, "Swarmcast".

[36] Fisher, "Swarmcast," 4.

[37] Fisher *et al*, *Mapping the Jihadist Information Ecosystem*.

[38] Conway *et al*, "A Snapshot of the Syrian Jihadi Online Ecology"; Macdonald *et al*, "Daesh, Twitter and the Social Media Ecosystem".

[39] Fisher et al, Mapping the Jihadist Information Ecosystem.

[40] Conway *et al*, "A Snapshot of the Syrian Jihadi Online Ecology"; Macdonald *et al*, "Daesh, Twitter and the Social Media Ecosystem".

[41] Bàrbara Molas, "Reddit's Hosting Service and the Dangers of Outlinking," accessed September 27, 2021, https://gnet-research.org/2021/09/17/reddits-hosting-service-and-the-dangers-of-outlinking/.

[42] Macdonald *et al*, "Daesh, Twitter and the Social Media Ecosystem".

[43] Bindner and Gluck, "Trends in Islamic State's Online Propaganda".

[44] Ahmad Shehabat and Teodor Mitew, "Black-boxing the black flag: anonymous sharing platforms and ISIS content distribution tactics," *Perspectives on Terrorism* 12, no. 1 (2018): 97.

# METHODOLOGY

Data collection took place from July 30, 2021 to September 12, 2021. To safeguard the welfare of the researchers, all data for the study were collected by Open Source Intelligence Analysts at Tech Against Terrorism. They employed three techniques to locate potentially relevant Telegram channels: keyword searches (including names of known media entities, outlets, propaganda videos and the name of the group itself, in both English and Arabic); monitoring IS on other platforms, in order to find joinlinks to relevant Telegram channels;[45] and monitoring known IS Telegram channels to identify links to new ones. For ethical and institutional policy reasons, access was limited to public channels and private channels with publicly available joinlinks (where no engagement with the channel administrator was necessary to join). Since none of the latter were discovered during the data collection period, all of the channels in the dataset were public channels.

To be regarded as an IS channel—and therefore to be included in this study—the channel must have demonstrated a pro-IS slant and must have met at least one of the following four criteria:

- It must have posted official IS content (such as claims of attacks, video/photo propaganda. or nasheeds[46]);
- It must have published unofficial, pro-IS media that praised the group and its efforts and/or promoted its ideology;
- The channel administrator must have published official IS content or content in support of IS on another platform; or
- The channel must have been promoted by IS affiliated networks or supporters on other platforms.

During the data collection period, Tech Against Terrorism continued to monitor for any new IS channels. When these appeared, they were added to the dataset. Tech Against Terrorism also added all terrorist content that was discovered to its Terrorist Content Analytics Platform (TCAP). The effect of this was to alert companies to the presence of terrorist content on their platform.

According to Telegram's terms of service, by signing up to Telegram users agree not to "Promote violence on publicly viewable Telegram channels, bots, etc."[47] Telegram has in the past taken part in Referral Action Days organised by Europol's EU Internet Referral Unit.[48] It is worth noting, therefore, that the channels in this study experienced significant disruption. Of the 13 channels included in the study, as of September 21, 2021 seven (53.85%) had been closed down.

[45] In this context, a joinlink is a URL which, when clicked, takes the user to a relevant Telegram channel.

[46] Relevant nasheeds would include those produced by Al-Ajnad and Al-Bayan Radio.

[47] "Terms of Service," Telegram, accessed March 11, 2022, https://telegram.org/tos.

[48] "Europol and Telegram take on terrorist propaganda online," Europol, accessed March 11, 2022, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

Given this significant level of disruption, data were extracted on a daily basis throughout the data collection period. Channels were downloaded using Telegram's in-built channel download feature and all other available data were exported using Telegram's export chat history function. It should be noted, first, that for a small number of posts it was not possible to determine which of the channels they appeared in, owing to the channel having been deleted prior to the data being extracted from Telegram, and, second, for those channels that had been in existence prior to the commencement of data collection, it was possible to collect posts and other content that predated the data collection period.

No channel names or domain names are identified in this report, for two reasons. The first reason is to ensure that the report does not make terrorist content more easily discoverable. The second reason is the possibility that some of the file-sharing platforms may currently be engaged in Tech Against Terrorism's mentorship program, and naming those platforms in this report could potentially impact the mentor–mentee relationship.

Lastly, it should also be noted that the project received institutional ethics approval. For additional security and privacy protection, the collected data were not shared outside of the project team.[49]

# FINDINGS

This section is divided into five parts. The first part provides an overview of the dataset. The second part examines the frequency of outlinking within these channels and the prevalence of file-sharing platforms within these outlinks. The third part examines the features of the file-sharing sites to which IS outlinked most frequently in our dataset. The fourth part compares the proportion of URLs that were live to those that were no longer live, while the final part focuses on the automated generation and dissemination of URLs.

## An Overview of the Dataset

Table 1 provides an overview of the 13 Telegram channels examined in this study. With just one exception, these were all broadcast channels—meaning that only the channel administrator could post. Six of the channels were known to be bots, meaning that the channel was not managed by a human but by software, such as the Telegram Bot API. The lifespans of the channels varied significantly. At the end of the data collection period, the two most long-standing channels were the 244-days-old Channel 2 (which purported to be a legitimate news outlet) and the 103-days-old Channel 3 (the sole user interaction channel). As of September 21, 2021, both of these channels were still live. In contrast, there were five channels that were closed down after less than a week (in two cases, after just one day).

[49] The project team did not attempt to contact any of the file-sharing sites in question, since platforms had already been alerted to the presence of the content via Tech Against Terrorism's TCAP.

**Table 1.** List of Channels[50]

| Channel | Type of Channel | Engagement of Channel | Predominant Language of Posts[50] | Total Posts | Total Posts with Outlinks | Date of First Post | Date of Last Post | Status of Channel (as of September 21, 2021) |
|---|---|---|---|---|---|---|---|---|
| Channel 1 | Public (Bot) | Broadcast | Arabic (72.2%) | 2,331 | 1,071 | July 30, 2021 | August 3, 2021 | Not Live |
| Channel 2 | Public | Broadcast | Arabic (74.2%) | 3,982 | 74 | December 30, 2020 | September 1, 2021 | Live |
| Channel 3 | Public | User Interaction | Arabic (31.8%) | 255 | 18 | May 20, 2021 | August 31, 2021 | Live |
| Channel 4 | Public (Bot) | Broadcast | Arabic (43.9%) | 107 | 0 | July 23, 2021 | August 12, 2021 | Live |
| Channel 5 | Public | Broadcast | English (61.5%) | 805 | 13 | June 15, 2021 | September 1, 2021 | Live |
| Channel 6 | Public | Broadcast | Arabic (61.4%) | 83 | 40 | August 20, 2021 | August 23, 2021 | Not Live |
| Channel 7 | Public (Bot) | Broadcast | Urdu (37.3%) | 397 | 8 | August 16, 2021 | September 12, 2021 | Live |
| Channel 8 | Public | Broadcast | Arabic (100%) | 3 | 0 | September 5, 2021 | September 6, 2021 | Not Live |
| Channel 9 | Public (Bot) | Broadcast | Arabic (87.5%) | 8 | 1 | September 18, 2021 | August 31, 2021 | Not Live |
| Channel 10 | Public | Broadcast | English (30%) | 10 | 5 | August 12, 2021 | August 13, 2021 | Live |
| Channel 11 | Public (Bot) | Broadcast | Arabic (77.3%) | 22 | 7 | September 1, 2021 | September 7, 2021 | Not Live |
| Channel 12 | Public (Bot) | Broadcast | English (66.7%) | 6 | 0 | August 10, 2021 | August 25, 2021 | Not Live |
| Channel 13 | Public | Broadcast | None | 5 | 0 | September 6, 2021 | September 7, 2021 | Not Live |
| Channel Could Not Be Determined | N/A | N/A | N/A | 66 | 13 | N/A | N/A | N/A |

[50] Some channels had a high incidence of posts containing no text (only URLs or attachments). In channels 3 and 7 this was the case for 51.4% and 61.7% of the posts, respectively. This is why the percentage figures for the predominant language in these channels is relatively low. For Channel 13, none of the posts in the channel contained any text.

Before continuing, it should be noted that four of the channels contained no outlinking posts at all (Channels 4, 8, 12 and 13), and 1,071 (85.68%) of the 1,250 posts in the dataset that did contain an outlink were posted in the same channel (Channel 1). Given the potential for this one channel to skew the study's findings, the analysis that follows examines the extent to which the trends that were evident in Channel 1 were also evident in the outlinks posted in the other channels.

## The Frequency of Outlinking to File-Sharing Platforms

A total of 8,080 posts were collected from these 13 channels. As Table 2 shows, in the dataset used for this study, inlinking—that is, the posting of URLs that lead to other spaces within the Telegram platform—was infrequent. A total of just 119 posts (1.47%) contained an inlink.[51] It should be noted that this low rate of inlinking reflects the channels examined in this study. There are pro-IS 'aggregator' channels on Telegram that are dedicated to disseminating links to other Telegram channels. However, no such channels were discovered during the data collection period for this study.

In contrast, outlinking was relatively widespread. A total of 1,250 posts (15.47%) contained an outlink. In other words, an outlink was found in roughly one in every 6.5 posts. This outlinking rate is higher than the equivalent figure of 12.5% in Conway et al's study of pro-IS users' outlinking practices on Twitter,[52] and markedly higher than the rate of 6.45% in Macdonald et al's study of the outlinking practices on Twitter of two European pro-far-right networks.[53] In total, these 1,250 posts outlinked to 98 different domains.

**Table 2.** Outlinking and Inlinking Rates

| | |
|---|---|
| **No. Of Channels** | **13** |
| **No. Of Posts** | **8,080** |
| **No. Of Posts Containing Outlinks** | **1,250** |
| **Outlinking Rate** | **15.47%** |
| **No. Of Posts Containing Inlinks** | **119** |
| **Inlinking Rate** | **1.47%** |

Table 3 (next page) shows the 30 domain names that appeared most frequently in the outlinks.[54]

[51] 24.0% of the inlinks led to one of the other channels in this study. The channels that were inlinked to were channels 1, 3, 5, 7, and 12.

[52] Conway *et al*, "Disrupting Daesh".

[53] Stuart Macdonald *et al*, *The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German and French Far-Right Online Ecosystems* (Washington, DC: RESOLVE Network, 2022).

[54] There were some domain names in the dataset that, although distinct, nonetheless led to the same platform (e.g., those ranked 1st, 12th, 17th, and 30th in Table 3). Where this was the case, the domain names were merged for counting purposes. Such mergers were identified by the research team manually checking each domain name individually.

**Table 3.** Top 30 Domains by Number of Posts Outlinking to the Domain[55]

| Ranking No. | Domains | Types of Service | Number of Posts that Outlink to the Domain | Proportion of Outlinking Posts (n= 1,250) that Outlink to the Domain | Channel 1 Posts | All Other Channel Posts |
|---|---|---|---|---|---|---|
| 1 | f****.** / f***.** | File Sharing | 1,032 | 82.6% | 970 | 62 |
| 2 | a******.*** | Archived Files/ Websites | 961 | 76.9% | 921 | 40 |
| 3 | p*********.*** | File Sharing | 819 | 65.5% | 818 | 1 |
| 4 | m***.** | File Sharing | 741 | 59.3% | 713 | 28 |
| 5 | d******.*** | File Sharing | 685 | 54.8% | 664 | 21 |
| 6 | 1***.** | File Sharing | 538 | 43.0% | 516 | 22 |
| 7 | t******.** | File Sharing | 452 | 36.2% | 427 | 25 |
| 8 | c****.****.** | File Sharing | 319 | 25.5% | 312 | 7 |
| 9 | m********.*** | File Sharing | 296 | 23.7% | 283 | 13 |
| 10 | s*********.*** | File Sharing | 269 | 21.5% | 254 | 15 |
| 11 | m***.** | Email Services | 255 | 20.4% | 249 | 6 |
| 12 | p*****.**** / p*.** | File Sharing | 207 | 16.6% | 206 | 1 |
| 13 | s*****.*** | File Sharing | 195 | 15.6% | 143 | 52 |
| 14 | u*****.*** | File Sharing | 154 | 12.3% | 142 | 12 |
| 15 | j**.** | File Sharing | 151 | 12.1% | 129 | 22 |
| 16 | c******.*** | File Sharing | 131 | 10.5% | 131 | 0 |
| 17 | d***.******.*** / y***.** | File Sharing | 123 | 9.8% | 121 | 2 |
| 18 | g*****.** | File Sharing | 122 | 9.8% | 70 | 52 |
| 19 | j**.** | File Sharing | 92 | 7.4% | 92 | 0 |
| 20 | o*.** | Social Network | 84 | 6.7% | 82 | 2 |
| 21 | f********.*** | File Sharing | 81 | 6.5% | 56 | 25 |
| 22 | u****.** | File Sharing | 74 | 5.9% | 42 | 32 |
| 23 | s******.*** | File Sharing | 60 | 4.8% | 51 | 9 |
| 24 | s*********.*** | File Sharing | 59 | 4.7% | 28 | 31 |
| 25 | j*******.** | File Sharing | 56 | 4.5% | 50 | 6 |
| 26 | b****.***** | Video Solutions | 55 | 4.4% | 54 | 1 |
| 27 | v****.*** | File Sharing | 50 | 4.0% | 50 | 0 |
| 28 | s*****.*** | E-Book/ Audio Book Service | 40 | 3.2% | 38 | 2 |
| 29 | d****.******.*** | File Sharing | 15 | 1.2% | 11 | 4 |
| 30 | a******.** / a******.** / a******.** | Archived Files/ Websites | 14 | 1.1% | 0 | 14 |

[55] An unredacted version of this table is available on request, at the discretion of the authors.

To determine frequency, the number of posts that contained a link to the relevant domain was counted.[56] So, for example, for the top-ranked domain name there were a total of 1,032 posts in the dataset that outlinked to this domain. For each domain name, Table 3 also lists the type of service offered. The fifth column in Table 3 shows the proportion of outlinking posts that included an outlink to the relevant domain. So, of the 1,250 outlinking posts in the dataset, 82.6% contained a URL that outlinked to the top-ranked domain. Lastly, in order to address the methodological concern that the majority of outlinking posts were contained in Channel 1, the final two columns break down the number of posts outlinking to the domain into two categories: Channel 1; and all other Channels. This allows an assessment of whether the findings for Channel 1 are representative of these other Channels.

Four key points emerge from Table 3. The first is the large number of file-sharing sites. Of the 30 domains listed in Table 3, 24 were file-sharing platforms (including nine of the top ten). Moreover, of the six domains that were not formally classified as file-sharing platforms, two provide access to archived files/websites and so could be used to share content in a similar way to file-sharing sites.[57]

The second point is that the most outlinked to file-sharing platforms within Channel 1 were also the most outlinked to file-sharing platforms in Channels 2-14. In fact, the most outlinked to file-sharing site in Channels 2-14 that was not also outlinked to in Channel 1 was a********.***. There were just six posts across Channels 2-14 that outlinked to this site. This is fewer than for 16 of the file-sharing sites listed in Table 3. In other words, the findings for Channel 1 were broadly in keeping with the findings for Channels 2-14.

The third point is the high incidence of use of the most common domain names. Each of the top eleven domain names was found in at least one-fifth of the outlinking posts. Each of the top five domain names was found in more than half of the outlinking posts. And the most outlinked to domain name was found in 82.6% of the outlinking posts. This shows a high level of use of certain sites.

Leading on from this, the fourth point is that the outlinking posts in the dataset generally contained multiple URLs. This is evident from the fact that the proportions in the fifth column of Table 3 total 650.5%. Indeed, the dataset as a whole contained a total of 12,510 outlinks, which, given the total of 1,250 outlinking posts, works out to an average of 10.01 outlinks per outlinking post. We return to this pattern of the posting of multiple URLs below.

## Platform Features

Having established that outlinking to file-sharing platforms is widespread, we turn next to an examination of the features of the 24 file-sharing platforms that appeared in Table 3. For each of these platforms, Table 4 shows the presence or absence of a total of 12 features. To create the table, three rounds of

[56] Other methods of counting would also have been possible, such as counting unique URLs or the sum of all URLs containing the relevant domain name (including duplicates). These other two methods of counting produced very similar results.

[57] The authors made a decision to distinguish between file-sharing sites and archiving services, notwithstanding the potential for the latter to be used as a de facto file-sharing service. This decision was made on the basis that the exploitation of archiving services raises distinctive issues, which require separate consideration.

coding were used. In the first round, a list of features was developed by studying the websites of each individual platform. Having constructed this list, in the second round of coding two researchers worked independently to complete Table 4. They then compared their results, finding an agreement rate of 76%. In the third round of coding, disagreements were resolved by reexamining the individual platforms. Almost all disagreements were the result of the relevant information being difficult to locate on the company's website.

**Table 4.** The Features of the Most Outlinked to File-Sharing Platforms

| *X = Data Factors<br>Y = File Sharing Platforms* | English | Western Europe / North America | Mandatory Registration for Services | Premium Available | All Content Types | Password File Protection Availability | More than 100GB of Data Storage | More than 5GB of Max. Upload Size | Encryption Available | Chat Function Available | Monetization Available | PII Storage Occuring |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| f****.**/ f****.** | ☑ | ☑ |  | ☑ | ☑ | ☑ |  |  | ☑ |  |  | ☑ |
| p**********.*** | ☑ | ☑ |  | ☑ | ☑ |  | ☑ |  |  |  |  | ☑ |
| m***.** | ☑ |  | ☑ | ☑ | ☑ | ☑ |  | ☑ | ☑ | ☑ |  | ☑ |
| d*******.*** | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |  | ☑ |  |  | ☑ |
| 1***.** | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |  |  |  |  |  | ☑ |
| t******.** |  |  |  | ☑ | ☑ |  |  |  |  |  |  | ☑ |
| c****.****.** |  |  | ☑ | ☑ | ☑ |  |  | ☑ |  |  |  |  |
| m********.*** | ☑ | ☑ |  | ☑ | ☑ | ☑ |  |  |  |  |  | ☑ |
| s*********.*** | ☑ | ☑ |  | ☑ |  | ☑ |  |  |  |  |  | ☑ |
| p*****.**** / p*.** | ☑ |  | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |  |  |  | ☑ |
| s*****.*** | ☑ | ☑ |  |  | ☑ |  |  |  | ☑ |  | ☑ | ☑ |
| u*****.*** | ☑ |  | ☑ |  |  |  |  |  | ☑ |  |  |  |
| j**.** | ☑ | ☑ | ☑ | ☑ |  | ☑ | ☑ | ☑ | ☑ |  |  | ☑ |
| c******.*** | ☑ |  | ☑ | ☑ | ☑ | ☑ |  |  | ☑ |  |  |  |
| d***.******.*** / y***.** | ☑ |  | ☑ | ☑ | ☑ |  |  | ☑ |  |  |  | ☑ |
| g*****.** | ☑ |  |  | ☑ | ☑ | ☑ | ☑ | ☑ |  |  |  | ☑ |
| j**.** | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |  |  |  |  |  | ☑ |
| f********.*** | ☑ |  |  | ☑ | ☑ | ☑ | ☑ |  | ☑ |  |  | ☑ |
| u****.** | ☑ |  |  | ☑ | ☑ | ☑ |  |  |  |  | ☑ | ☑ |
| s******.*** | ☑ | ☑ |  |  |  |  |  |  |  |  |  | ☑ |
| s*********.*** | ☑ | ☑ |  | ☑ | ☑ |  |  |  |  |  |  | ☑ |
| j*******.** | ☑ |  | ☑ | ☑ |  |  | ☑ | ☑ |  |  | ☑ | ☑ |
| v****.*** | ☑ |  | ☑ |  |  |  |  |  | ☑ |  |  |  |
| d****.******.*** | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |  |  |  |  |  | ☑ |

Three key points emerge from Table 4. First, there were four features that were present on at least 75% of the platforms. Three of these were: the platform interface was in the English language (22 platforms); a premium service was available (20 platforms); and the platform enabled users to store all types of content (18 platforms). While this may indicate that these features are prioritized by IS supporters, some caution is needed in interpreting these results. For example, the prevalence of English-language interfaces may reflect the prevalence of the English language in our dataset. Similarly, if the vast majority of file-sharing platforms offer a premium option, this would explain the high number for this feature in our study.

The other feature that was present on at least 75% of the platforms was that the platform stored personal identifying information (PII). A total of 20 platforms stated in their terms of service that they collect and store computational identifiers such as device identifiers and IP addresses. Of these, ten also required the creation of an account before allowing a user to share content, with seven of these ten verifying the user's email address as part of the account creation process.[58] This leads to the second key point, which is that potentially disincentivizing features did not appear to have any real deterrent

[58] In order to arrive at these figures, we attempted to share a file on each of the 20 platforms. We were able to share a file on seven of the platforms without first creating an account. It was not possible to test the remaining three, either because the site would not load or because of concerns about malware.

effect. Beyond the sharing of PII, there also did not appear to be a preference for platforms that lacked a mandatory registration requirement. In fact, a majority of the platforms (13 in total) did have such a requirement, including three of the top five. A mandatory registration requirement thus also seemed to have little deterrent effect.

Third, there were a number of features that did not seem to be prioritized. These included large storage capacity (only seven of the platforms offered more than 100 GB of storage) and a large upload size (only seven offered a maximum upload size of more than 5 GB). Security features also did not seem to be a priority. Whereas 14 platforms did offer the possibility of password file protection, only nine offered encryption. This lack of emphasis on security is consistent with the public broadcast nature of the channels studied. The public broadcast nature of the channels also explains the apparent lack of weight attached to monetization (three platforms) and a chat function (one platform).

## URL Deactivation Rate

In addition to the features of individual platforms, a further possible strategic consideration is the likelihood of URLs being deactivated. Table 5 accordingly examines the proportion of URLs that were live (as of September 28, 2021).

**Table 5.** Outlinks and Inlinks by Live or Not Live

| **Outlinking - Counted on the Basis of Unique Links** | | |
|---|---|---|
| | **Number** | **Percentage** |
| **Total Links** | 8,907 | N/A |
| **Links Investigated** | 2,326 | 100% |
| **Live** | 172 | 7.4% |
| **Not Live** | 2,135 | 91.8% |
| **Unknown** | 19 | 0.8% |
| **Total** | 2,326 | 100.0% |
| **Inlinking - Counted on the Basis of Unique Links** | | |
| | **Number** | **Percentage** |
| **Total Links** | 31 | 100.0% |
| **Live** | 31 | 100.0% |
| **Not Live** | 0 | 0.0% |
| **Total** | 31 | 100.0% |

The table covers both outlinks and inlinks.[59] To create the table, a random sample of 26% of the outlinks in the dataset was generated. The researchers manually clicked on each outlink, recording whether or

[59] Note that the table focuses on distinct URLs. That is, if a single URL was posted three times in our dataset, it is only counted once in Table 5. For this reason, the sum of the URLs in Table 5 differs from the sum of the URLs elsewhere in this report.

not the link remained live. For a small number (19), it was not possible to classify the link as either live or not live because a log in was required to attempt access to the file/website. These links were therefore recorded as unknown. The same approach was applied to the inlinks, except here the much smaller number of links (31) meant that it was not necessary to limit the investigation to a random sample.

Three key points emerge from Table 5. First, 2,135 (91.8%) of the outlinks were no longer live. While there are other possible reasons besides content moderation for content being unavailable (such as the user deleting the content), the primary reason for outlinks not being live is almost certainly content removal. Indeed, some platforms explicitly notified the visitor that the reason the content was unavailable was because it was violent extremist or terrorism-related. While it is not possible for us to say exactly how long it took for the file-sharing platforms to remove the content, the vast majority of outlinks in the dataset were posted no earlier than July 30, 2021 (see Table 6 below), meaning that they were deactivated within two months. At the strategic level, these findings suggest that file-sharing sites were not outlinked to because they had weak moderation practices. If anything, to the extent that moderation practices do in fact influence outlinking practices, the findings are more consistent with these platforms being the subject of higher numbers of outlinks because of their aggressive moderation practices, i.e., as a result of strong enforcement, it was necessary for IS supporters to repost new links to content stored on these platforms. Admittedly, the high enforcement rate in our sample may in part be due to the fact that, when Tech Against Terrorism collected the data, terrorist content was entered into the TCAP and platforms were alerted to terrorist content stored on their sites. Nonetheless, an enforcement rate of over 90% is still a strong number, especially given that the 2,326 outlinks in our sample spanned 98 different domains.[60]

Second, a total of 172 (7.4%) of the outlinks were still live at the time we tested them. While the majority of these were linked to terrorist content (n = 119), this was not always the case.[61] Other types of non-extremist content (n = 6) included news pieces, from outlets such as the U.K.'s The Guardian, and publications from NGOs, such as the Washington, DC-based Center for Global Development. We were unable to investigate the remaining outlinks (n = 47) due to access restrictions.[62]

Third, all 31 of the inlinks remained live. In all 31 cases, the URL linked to another Telegram channel. This signposting enables users to move between different Telegram channels with agility, thereby strengthening the resilience of the network.[63]

## Automated Generation and Dissemination of URLs

This final part of the findings focuses on the automated generation and dissemination of URLs. To show the significance of this issue, the section begins with a temporal analysis. Table 6 shows the number of

[60] For clarity, the researchers ensured that the random sample of URLs tested included ones from all 98 domains present in the wider dataset.

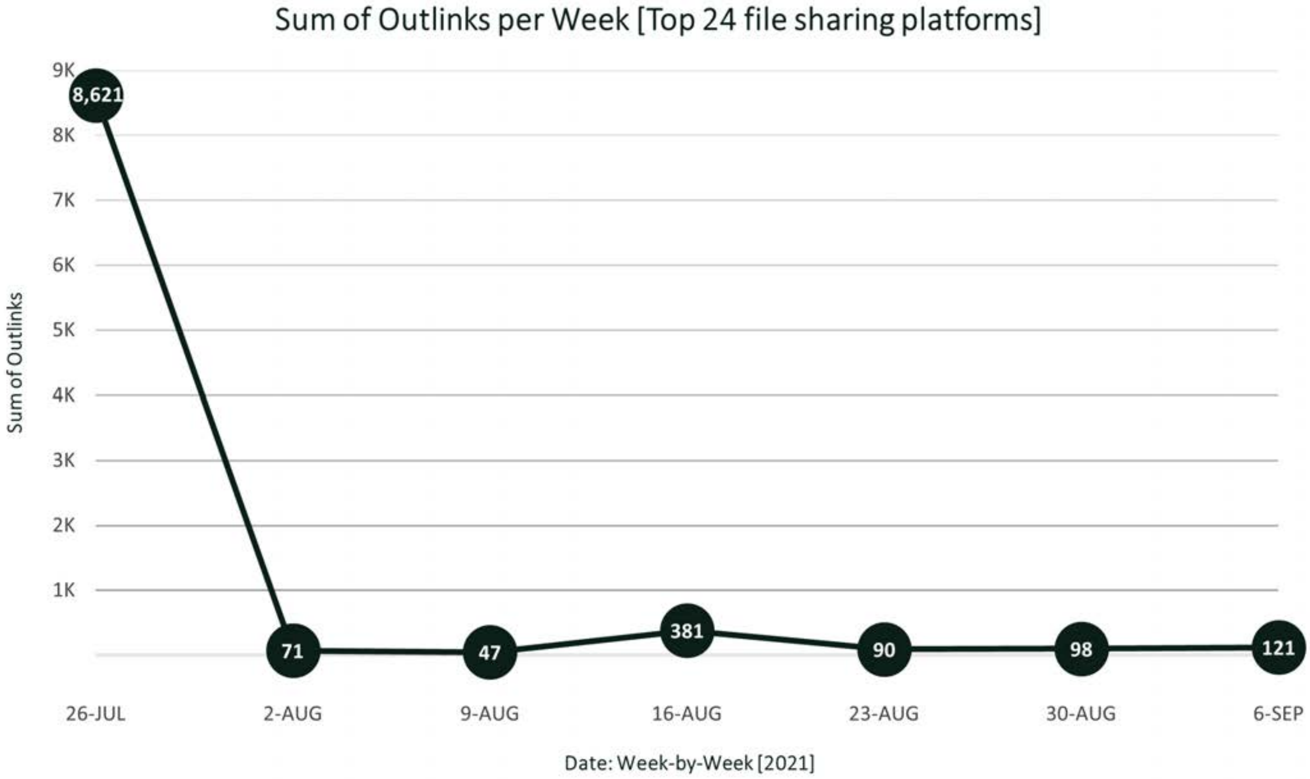
[61] Live links to terrorist content were referred to Tech Against Terrorism for further action.

[62] In these instances, the file page would appear and tell us that we could download the file, but we did not do so for security reasons.

[63] Fisher, "Swarmcast."

times an outlink to one of the 24 top file-sharing platforms was posted each week, for the seven-week period from July 26, 2021 to September 12, 2021 (n = 9,429). It shows that the vast majority (8,621; 91.4%) were posted in the same one-week period.

**Table 6.** Number of Outlinks Posted, by Week



Closer examination reveals two things: first, the vast majority (99.6%) of the outlinks that were posted during the week beginning July 26 were in fact posted during the two-day period from July 30 (7,325 outlinks posted) to July 31 (1,263 outlinks posted);[64] and, second, that all of the outlinks that were posted during this two-day period appeared in the same Telegram channel (Channel 1). The first post in this channel appeared on July 30 and the last post appeared on August 3. The channel is no longer live and, importantly, the channel was a bot.

Channel 1 is also a good example of the tendency, noted above, for outlinking posts in the dataset to contain multiple URLs. This is explored further in Table 7. As Table 7 shows, the dataset as a whole contained 12,510 outlinks. This figure includes reposts of URLs, i.e., if the same outlink appeared in three posts, this would be counted as three outlinks for the purposes of Table 7. These 12,510 outlinks appeared in a total of 1,250 posts. This works out to an average of 10.01 outlinks per outlinking post. Table 7 shows that the rate of outlinks per outlinking post varied significantly across the different channels. For Channel 1, the ratio was 10.5 outlinks per outlinking post (11,286 outlinks, compared to a total of 1,071 outlinking posts). This pattern of posts containing multiple outlinks was not confined to Channel 1. Three other channels in the dataset had equally high or higher ratios. Of these, two were confirmed by the research-

[64] It is possible that this was timed to coincide with the release of the 297th issue of Al Naba on July 29, 2021.

ers to be bot channels (the two with the highest ratio of outlinks per outlinking posts, channels number 7 and 11, which had ratios of 32.6 and 18.1, respectively). It is possible that the third channel (Channel 6) was also a bot, though the researchers were not able to confirm this with certainty. The ratio for the posts whose channel was unknown was also high, at 15.4.

**Table 7.** Ratio of Outlinks per Outlinking Post, by Channel

| Channel | Types of Channel | Sum of Outlinks | Sum of Outlinking Posts | Number of Outlinks per Outlinking Post |
|---|---|---|---|---|
| Channel 1 | Public (Bot) | 11,286 | 1,071 | 10.5 |
| Channel 2 | Public | 81 | 74 | 1.1 |
| Channel 3 | Public | 91 | 18 | 5.1 |
| Channel 4 | Public (Bot) | 0 | 0 | 0.0 |
| Channel 5 | Public | 13 | 13 | 1.0 |
| Channel 6 | Public | 419 | 40 | 10.5 |
| Channel 7 | Public (Bot) | 261 | 8 | 32.6 |
| Channel 8 | Public | 0 | 0 | 0.0 |
| Channel 9 | Public (Bot) | 2 | 1 | 2.0 |
| Channel 10 | Public | 30 | 5 | 6.0 |
| Channel 11 | Public (Bot) | 127 | 7 | 18.1 |
| Channel 12 | Public (Bot) | 0 | 0 | 0.0 |
| Channel 13 | Public | 0 | 0 | 0.0 |
| Channels Could Not Be Determined | N/A | 200 | 13 | 15.4 |
| Total | | 12,510 | 1,250 | 10.0 |

Having established this tendency for posts to contain multiple outlinks, two further questions arose on the theme of multiple posting. First, where URLs were posted on more than one occasion, were these reposts in the same channel or across different channels? Second, were there multiple outlinks to the same piece of content and, if so, were these posted simultaneously or over a period of time?

The first of these questions is explored in Table 8. This table shows the number of times each outlink in the dataset was posted. For example, there was one outlink that was posted a total of 16 times, while at the other extreme there were 5,443 outlinks that were only posted once.

**Table 8.** Frequency of Multiple Posting of URLs

| No. of Items the Outlink was Posted Within the Dataset | No. of Outlinks for Which this was the Case |
|---|---|
| 16 | 1 |
| 12 | 1 |
| 9 | 1 |
| 6 | 3 |
| 5 | 1 |
| 4 | 44 |
| 3 | 5 |
| 2 | 3,408 |
| 1 | 5,443 |

Three key points emerge from Table 8. First, the repeated reposting of individual URLs was relatively uncommon. Over half of the outlinks in the dataset (61.11%) were posted just once, while only 56 outlinks (0.62% of the dataset) were posted on three or more occasions. It should be emphasized that our study focused on public channels only, and so it is possible that these URLs were reposted in private channels that we were unable to access. Within these public channels, however, our findings suggest that outlinks were generally regarded as single-use, throwaway commodities.

Second, where outlinks were reposted, the reposts were almost always within the same channel. Of the 56 outlinks that were posted on three or more occasions in our dataset, there were just two that were posted in multiple channels. One of these outlinked to a secure open-source communications platform, the other to a decentralized alt-tech platform. Both appeared in a total of three posts that were spread across two channels (channels 7 and 10). Moreover, the reposting of outlinks largely took place within a short space of time. Of the 49 outlinks that were posted on three or four occasions, the reposting of 43 of these (87.76%) occurred within the space of six minutes or less.

Third, on the rare occasions where sustained, repeated reposting of an outlink did occur, this took place within a specific context. There were seven outlinks that were posted on five or more occasions within our dataset. For all seven outlinks: (a) the reposts were spread over a period of time (ranging from seven days to 72 days); and (b) all reposts appeared in the same channel as the original post. Five of the seven outlinks were posted in Channel 2.[65] This was the most long-standing channel in our dataset (244 days old at the end of our data collection period, and still live). It portrays itself as a legitimate news outlet, yet three of the URLs in question outlinked to Facebook pages and the other two outlinked to (suspended) Twitter accounts.[66] In this limited context, then, these URLs appeared to have a signposting function and were not regarded as throwaway items.

The second question on the theme of multiple posting is whether there were multiple outlinks to the same piece of content and, when this was the case, whether these outlinks were posted simultaneously or over a period of time. To investigate this, we began by examining a sample of ten posts that contained a large number of outlinks. These ten were selected by identifying the posts in Channel 1 that had the highest character count. Between them, these ten posts contained a total of 334 outlinks. An overview of these posts is contained in Table 9 on the following page.

[65] The others were posted in Channel 1 (a (deactivated) link to a file-sharing site that was posted six times) and in the purportedly journalistic Channel 5 (a link to a (suspended) Twitter account, that was posted six times).

[66] The three links to Facebook pages were shared 16, 12, and 6 times; the two links to (suspended) Twitter accounts were shared 9 and 5 times.

**Table 9.** Overview of Ten Posts from a Public Bot Channel Containing Multiple URLs[67]

| Post Date and Time | No. of URLs Contained in Post | No. of Different Platforms Outlinked | Details of Files |
|---|---|---|---|
| July 30, 2021 23:53:04 | 35 | 5 (inc. 4 file-sharing sites) | • None of the links were live.<br>• High mention of: "Battar", likely referring to the pro-IS media channel "Al-Battar".<br>• The outlinks appeared mostly to be PDF files. |
| July 30, 2021 23:53:07 | 32 | 8 (inc. 6 file-sharing sites) | • None of the links were live.<br>• High mention of: "Hadm Bashir Sabirin" and "Wa Bashir Sabirin", which means "and give glad tidings to those who endure".<br>• The outlinks appeared mostly to be MP4 files. |
| July 30, 2021 23:53:38 | 36 | 9 (inc. 8 file-sharing sites) | • None of the links were live.<br>• High mention of: "Quds Dawla". Here, "Quds" loosely translates as holy or pure, while "Dawla" might refer to State, potentially as part of the "Islamic State" word.<br>• The outlinks appeared mostly to be MP4 files. |
| July 30, 2021 23:53:40 | 36 | 9 (inc. 8 file-sharing sites) | • None of the links were live<br>• High mention of: "Quds Sinnai" and "Quds Raqqa". Sinnai is apparently a reference to the Sinai Peninsula, where IS is currently waging an insurgency against Egyptian security forces. It is likely that Raqqa refers to the Syrian city that was controlled by the Islamic State from 2014 to 2017.<br>• The outlinks appeared mostly to be MP4 files. |
| July 30, 2021 23:53:42 | 45 | 9 (inc. 8 file-sharing sites) | • None of the links were live.<br>• High mention of: "Quds", such as "Quds Furat", "Quds Khorasan", and "Quds Isdarat". Khorasan may be referring to the historic Khorasan region in the Middle East, whereas Isdarat likely refers to an old pro-IS website.<br>• The outlinks appeared mostly to be MP4 files. |
| July 31, 2021 00:48:57 | 30 | 10 (inc. 8 file-sharing sites) | • None of the links were live.<br>• One file was repeatedly shared, which was Al Naba's 293rd newspaper publication.<br>• The outlinks appeared mostly to be PDF files. |
| July 31, 2021 00:49:22 | 30 | 10 (inc. 8 file-sharing sites) | • Three of the 30 links remained live.<br>• Similar URLs were shared as the Al Naba URLs on the post above. In this case the focus was Al Naba's 295th newspaper publication.<br>• The outlinks appeared mostly to be PDF files. |
| July 31, 2021 00:49:23 | 27 | 10 (inc. 8 file-sharing sites) | • None of the links were live.<br>• High mention of: "Khilafah", which refers to "Caliphate", meaning an Islamic political governing system.<br>• The outlinks appeared mostly to be MP4 files. |
| July 31, 2021 00:50:08 | 33 | 11 (inc. 10 file-sharing sites) | • 2 of the 33 links remained live.<br>• One file was repeatedly shared, which was Al Naba's 297th newspaper publication. This had been released two days prior to the post.<br>• The outlinks appeared mostly to be PDF files. |
| July 31, 2021 00:50:08 | 30 | 10 (inc. 8 file-sharing sites) | • Three of the 30 links remained live.<br>• Here again, the 297th Al Naba newspaper publication was repeatedly shared.<br>• The outlinks appeared mostly to be PDF files. |

[67] Tracking Terrorism, "Islamic State Releases Newspaper "Al Naba" 297 - Released 29 July 2021 (Assaults on PKK, PMU, Afghan, Cameroonian, Congolese, Mozambican & Nigerian Armies)," accessed September 30, 2021, https://www.trackingterrorism.org/chatter/pdf-islamic-state-releases-newspaper-al-naba-297-released-29-july-2021-assaults-pkk-pmu-afgh.

As Table 9 shows, the file types that were outlinked to were largely MP4 and PDF files, i.e., the types of content tended to be videos and written publications. Importantly, the text of the URLs often contained an indication of the content being outlinked to. For example, some URLs contained the word 'Battar', apparently a reference to the pro-IS media channel 'Al-Battar', while the term 'N297B' was used to refer to the 297th Al Naba newspaper publication. Using the latter insight, we sought to identify other outlinks to Al Naba newspaper publications by searching for other URLs that contained an uppercase N, then a three-digit number, then an uppercase B. This yielded a total of 16 posts, which between them contained 74 distinct URLs that outlinked to ten different issues of the publication.[68] Each individual post focused on one issue, containing multiple outlinks to that issue that were spread across at least two different platforms. When two or more posts contained outlinks to the same issue, these posts appeared simultaneously or within minutes of each other. And all 16 posts appeared within the space of less than one hour. The overall finding was thus that batches of URLs were being generated and disseminated together.

Four further points emerge from Table 9. First, while each individual post in Table 9 contained multiple outlinks, it was noticeable that—while the URLs were all distinct—they generally all led to the same item. This is in keeping with our examination of the Al Naba outlinks and is also consistent with Bindner and Gluck's finding that multiple URLs are disseminated for each individual piece of content, in the anticipation that many of the links will potentially be deactivated.[69]

Second, as would be expected, the majority of the outlinks in Table 9 (276; 83%) led to file-sharing platforms.[70] Here it is worth noting that each individual post not only contained multiple outlinks to the content stored on specific platforms, but also contained outlinks to the same content on multiple different platforms. For example, the first post in Table 9 contained a total of 35 URLs. These outlinked to a total of four different file-sharing sites. In total, the 276 links to file-sharing sites outlinked to a total of 24 different platforms. IS supporters are thus striking a balance between, on the one hand, concentrating its content store activities on a number of file-sharing platforms, perhaps due to familiarity with these platforms on the part of both aggregators and consumers, while, on the other hand, spreading its storage activities across a number of different file-sharing sites, to boost resilience.

The final two points that emerge from Table 9 are the sheer number of different URLs that have been generated (all 334 of the links contained in these ten posts were distinct URLs) and the rapidity of the posting (the first five posts in Table 9 were posted within the space of 38 seconds; the last five posts were posted within the space of 71 seconds). Taken alongside the fact that this was a bot channel, these two findings strongly suggest that, in order to produce swathes of URLs swiftly and efficiently, pro-IS users make use of automated services.

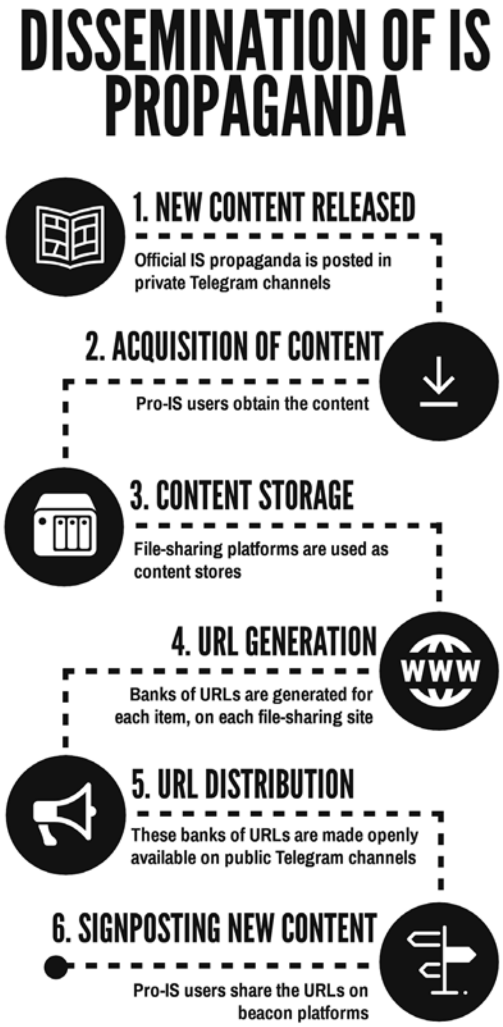
[68] These were issues 275, 277, 281, 285, 287, 289, 291, 293, 295, and 297.

[69] Bindner and Gluck, "Trends in Islamic State's Online Propaganda."

[70] It is worth noting that 46 of the URLs oulinked to archive.org. Since this study classified archive.org as an archiving service, not a file-sharing one (see Table 3), these 46 URLs are not included in this count (nor are the other URLs that led to other types of service).

# DISCUSSION

While this study was limited to public channels, and the vast majority of the dataset emanated from one particular channel, the findings are nonetheless consistent with previous descriptions of pro-IS users' propaganda dissemination strategy, as outlined in the literature review. File-sharing platforms appear to be used as content stores, with individual pieces of pro-IS propaganda being stored on multiple file-sharing sites and each piece being accessible via multiple unique URLs. The public-facing Telegram channels from which the data for this study were obtained appeared to be used as aggregators, gathering these collections of links and making them openly available for others to share on beacon platforms. The effect of this interconnected use of different sites for different purposes is to provide greater resiliency, as is the use of multiple content stores and the generation of multiple URLs for each individual item. Given the limited lifespan of the vast majority of these URLs, speed (of dissemination) and agility (moving between different platforms) are also critical.



DISSEMINATION OF IS PROPAGANDA

1. NEW CONTENT RELEASED

Official IS propaganda is posted in private Telegram channels

2. ACQUISITION OF CONTENT

Pro-IS users obtain the content

3. CONTENT STORAGE

File-sharing platforms are used as content stores

4. URL GENERATION

Banks of URLs are generated for each item, on each file-sharing site

5. URL DISTRIBUTION

These banks of URLs are made openly available on public Telegram channels

6. SIGNPOSTING NEW CONTENT

Pro-IS users share the URLs on beacon platforms

This study confirms previous studies in showing that IS supporters' content storage activities are not randomly distributed.[71] There is a concentrated use of certain file-sharing sites. The contribution of the study is the empirical examination of possible reasons for this focus on certain platforms. While the study's conclusions require further testing in future research, it is possible to draw initial conclusions about the hypothesized strategic considerations that inform IS supporters' use of particular file-sharing platforms. In terms of platform features, the study found that IS supporters did not seem to prioritize features that might appear to be beneficial to those wishing to store large quantities of content, such as large storage capacity and upload size. Nor did it seem to prioritize security features. Similarly, potentially disincentivizing features, such as a mandatory registration requirement, did not seem to have any deterrent effect. In terms of URL deactivation rates, the likelihood of content being taken down also did not appear to have any discernible deterrent effect. Indeed, the premise of the dissemination strategy appeared to be that URLs would be deactivated and have only a short lifespan.

[71] Conway et al, "A Snapshot of the Syrian Jihadi Online Ecology"; Fisher *et al*, *Mapping the Jihadist Information Ecosystem*; Macdonald *et al*, "Daesh, Twitter and the Social Media Ecosystem".

What our findings suggest is important to pro-IS users is the ability to generate large banks of URLs swiftly and disseminate these rapidly. Here, the role of automation—specifically, bots—is key. More than 90% of the outlinks in our dataset were posted by a single automated channel. Moreover, this channel posted an enormous number of distinct URLs in a short period of time: on average, one roughly every 20 seconds throughout the 30th and 31st of July. At times, there were bursts during these two days when an average of five URLs were being posted every second. This emphasis on speed is understandable, given the significant levels of disruption that our study has shown IS supporters face. It is important, therefore, that efforts to deactivate these URLs are similarly speedy. Yet, for all but the largest tech companies, attempts to identify such URLs and takedown the content behind them is a manual enterprise.[72]

Lastly, our experience in preparing this report of clicking on hundreds of URLs and being repeatedly greeted with the message "Content unavailable" leads us to wonder whether an opportunity is being missed to fill this "information vacuum".[73] There is the possibility here of using a tailored version of the Redirect Method, so that anyone who clicks on such a link instead sees a message signposting them to alternative content or to support services such as crisis counselling or psychosocial help.[74] Admittedly, some caution is required here. While recent research suggests that such work can yield positive outcomes—if it is tailored to reflect linguistic, cultural, and regional nuances and draws upon partnerships with, and the expertise of, counterspeech and disengagement practitioners[75]– there has, in general, been a lack of robust evaluation of online countering violent extremism efforts[76] and there are risks inherent in such work that must be addressed.[77]

# CONCLUSION

This report has detailed the dissemination process of IS propaganda. Once new content has been released and acquired by pro-IS users, it is stored on file-sharing platforms. Banks of URLs are then generated, distributed via public Telegram channels, and used on beacon platforms to signpost other users to the new content.

[72] Isabelle van der Vegt et al, *Shedding Light on Terrorist and Extremist Content Removal*, (London: Royal United Services Institute, 2019), https://static.rusi.org/20190703_grntt_paper_3.pdf.

[73] Alastair Reed, Haroro J. Ingram, and Joe Whittaker, *Countering Terrorist Narratives*, (Brussels: European Parliament, 2017), https://www.europarl.europa.eu/RegData/etudes/STUD/2017/596829/IPOL_STU(2017)596829_EN.pdf, 30.

[74] *Ibid.*

[75] Erin Saltman, Farshad Kooti, and Karly Vockery, "New Models for Deploying Counterspeech: Measuring Behavioral Change and Sentiment Analysis," *Studies in Conflict & Terrorism* (2021), https://doi.org/10.1080/1057610X.2021.1888404.

[76] Ghayda Hassan et al, *A systematic review on the outcome of primary and secondary prevention programs in the field of violent radicalization* (Montreal: Canadian Practitioners Network for the Prevention of Radicalization and Extremist Violence, 2021), https://cpnprev.ca/wp-content/uploads/2021/03/CPN-PREV-2nd-Systematic-Review-2.pdf; Michael Jones, *Through the Looking Glass: Assessing the Evidence Base for P/CVE Communications* (London: Royal United Services Institute, 2020), https://static.rusi.org/pcve_communications_final_web_version.pdf.

[77] Jacob Davey, Jonathan Birdwell, and Rebecca Skellett, *Counter Conversations: A model for direct engagement with individuals showing signs of radicalisation online* (London: Institute for Strategic Dialogue, 2018), https://www.isdglobal.org/wp-content/uploads/2018/03/Counter-Conversations_FINAL.pdf.

Based on this, the report proposes the following four-pronged RIDR strategy for combating pro-IS users' use of file-sharing platforms:

1. Remove terrorist content at the point of upload
2. Impede the automated generation and dissemination of banks of URLs
3. Disrupt the posting of these URLs on other platforms
4. Redirect users to other content and support services

The first strand of the RIDR strategy is to remove terrorist content at the point of upload. Here, the major social media companies have made significant progress in recent years. For example, Facebook has reported that, in the second quarter of 2021, it proactively found and removed 99.70% of terrorist content, with only 0.3% of such content flagged by users.[78] The formation of the GIFCT's hash-sharing database has also gone some way towards helping smaller companies to identify and remove such content at the point of upload. Given the widespread sharing of PDF documents found in this study, the GIFCT's recent announcement that the database will be expanded to include PDFs is also to be welcomed.[79] However, it remains the case that there are only 18 members of GIFCT and very few of the file-sharing platforms identified in this study are GIFCT members.[80] More fundamentally, there are many (particularly smaller) platforms that do not expressly prohibit terrorist content. Even when such prohibitions do exist, they may be vague or circumscribed.[81] As noted above, for example, Telegram's prohibition on the promotion of violence only applies "on *publicly* viewable Telegram channels", not private ones.[82] A publicly available policy that explicitly prohibits terrorist and/or violent extremist activity is a condition of GIFCT membership. Enlarging GIFCT membership must therefore be a priority, alongside assisting new member companies (particularly smaller ones) to operationalize their access to, and use of, the hash-sharing database. For non-member companies, there are simple detection tools that could be employed to flag items for review, for example by detecting certain keywords in the name of the uploaded file and by identifying relevant logos on the publications themselves. One limitation here, however, is the need for subject matter expertise to be able to deploy detection tools in this way, underlining the importance of Tech Against Terrorism's knowledge-sharing work.

Progress has also been made recently on the third strand of the RIDR strategy: disrupting the posting of URLs on other platforms. The GIFCT has announced that it will also add to its hash-sharing database URLs that Tech Against Terrorism has identified as hosting terrorist content.[83] This is undoubtedly important, although it should be remembered that this study found low rates of URL reposting and only a small proportion (5.1%) of the outlinks to terrorist content examined in this study were still live. Where links have

[78] Facebook, "Community Standards Enforcement Report: Q2 2021 Report," accessed October 11, 2021, https://transparency.fb.com/data/community-standards-enforcement/.

[79] GIFCT, "Broadening the GIFCT Hash-Sharing Database Taxonomy: An Assessment and Recommended Next Steps," accessed October 11, 2021, https://gifct.org/wp-content/uploads/2021/07/GIFCT-TaxonomyReport-2021.pdf.

[80] GIFCT, "Membership," accessed March 12, 2022, https://gifct.org/membership/.

[81] Macdonald, Correia, and Watkin, "Regulating terrorist content on social media".

[82] "Terms of Service," Telegram (emphasis added).

[83] GIFCT, "Broadening the GIFCT Hash-Sharing Database Taxonomy."

been deactivated, the fourth strand of the RIDR strategy is to redirect users, either to other content or to relevant support services, building on the potential for positive outcomes indicated by recent studies.

The part of the RIDR strategy that has received the least attention to date is the second strand: impeding the automated generation and dissemination of banks of URLs. Some platforms already check the content behind URLs before they are posted. For example, when a URL is shared on Twitter it is automatically processed and shortened to a http://t.co link.[84] As part of this process, links to content that violates Twitter's Terms of Service, including terrorist websites and content, are blocked.[85] From the current study, it appears that pro-IS users operate on the assumption that the links they share will be deactivated. The core of their strategy is therefore volume and speed, relying on the use of automation for the rapid generation and dissemination of banks of URLs. It follows that the identification and deactivation of these URLs needs to be equally swift. Here, pro-IS users' reliance on automation is in fact a double-edged sword, for it means that behavior-based indicators may be used to detect its URLs as well as content-based ones. The latter rely on such things as word and image use, which typically require human assessment, meaning that scaling is difficult. However, behavior-based cues—such as abnormal posting volume—can be picked up more easily by automated systems and often do not require any human involvement.[86] This study has revealed a number of potential behavior-based indicators, including: (a) the generation of multiple URLs, all to the same piece of content stored on one platform; (b) the simultaneous posting of URLs to multiple different platforms, all of which outlink to the same piece of content; (c) the repeated posting of large numbers of URLs in single posts; and (d) the rapidity with which such posts appear. Developing automated tools that employ indicators such as these to automatically detect and flag suspect URL generation and dissemination practices—and making such tools available for use by platforms that are used by IS supporters as content stores and aggregators—would mark a significant advance for efforts to combat the dissemination of IS propaganda.

[84] Twitter, "About Twitter's link service (http://t.co)," accessed March 14, 2022, https://help.twitter.com/en/using-twitter/url-shortener.

[85] Twitter, "Our approach to blocking links," accessed March 14, 2022, https://help.twitter.com/en/safety-and-security/phishing-spam-and-malware-links.

[86] van der Vegt et al, *Shedding Light on Terrorist and Extremist Content Removal*.

# BIBLIOGRAPHY

Alexander, Audrey. *Digital Decay? Tracing Change Over Time Among English-Language Islamic State Sympathizers on Twitter*. Washington, DC: George Washington University Program on Extremism, 2017. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.

Almohammad, Asaad, and Charlie Winter. *From Battlefront to Cyberspace: Demystifying the Islamic State's Propaganda Machine*. West Point, NY: Combating Terrorism Center, 2019. https://ctc.usma.edu/wp-content/uploads/2019/05/Battlefront-to-Cyberspace.pdf.

Awan, Akil N., and Al-Lami, Mina. "Al-Qa'ida's Virtual Crisis." *The RUSI Journal* 154, no. 1 (2009): 56-64. https://doi.org/10.1080/03071840902818605.

Ayad, Moustafa, Amarasingam, Amarnath, and Audrey Alexander. *The Cloud Caliphate: Archiving the Islamic State in Real-Time*. West Point, NY: Combating Terrorism Center, 2021. https://ctc.usma.edu/wp-content/uploads/2021/05/Cloud-Caliphate.pdf.

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

Berger, JM and Heather Perez. *The Islamic State's Diminishing Returns on Twitter: How Suspensions are Limiting the Social Networks of English-Speaking ISIS Supporters*. Washington, DC: George Washington University Program on Extremism, 2016. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/JMB%20Diminishing%20Returns.pdf.

Bindner, Laurence, and Raphael Gluck. "Assessing Europol's Operation Against ISIS' Propaganda: Approach and Impact." Accessed March 9, 2022. https://icct.nl/publication/assessing-europols-operation-against-isis-propaganda-approach-and-impact/.

Bindner, Laurence and Raphael Gluck. "Trends in Islamic State's Online Propaganda: Shorter Longevity, Wider Dissemination of Content." Accessed March 2, 2022. https://icct.nl/publication/trends-in-islamic-states-online-propaganda-shorter-longevity-wider-dissemination-of-content/.

Clifford, Bennett and Helen Powell. *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram*. Washington DC: George Washington University Program on Extremism, 2019. https://scholarspace.library.gwu.edu/work/9s161692z.

Conway, Maura, Khawaja, Moign, Lakhani, Suraj, Reffin, Jeremy, Robertson, Andrew and David Weir. "Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts." *Studies in Conflict & Terrorism* 42, no. 1-2 (2019): 141-160. https://doi.org/10.1080/1057610X.2018.1513984.

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

Davey, Jacob, Birdwell, Jonathan, and Rebecca Skellett. *Counter Conversations: A model for direct engagement with individuals showing signs of radicalisation online*. London: Institute for Strategic Dialogue, 2018. https://www.isdglobal.org/wp-content/uploads/2018/03/Counter-Conversations_FINAL.pdf.

Europol. "Europol and Telegram take on terrorist propaganda online." Accessed March 11, 2022. https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

Facebook. "Community Standards Enforcement Report: Q2 2021 Report." Accessed October 11, 2021. https://transparency.fb.com/data/community-standards-enforcement/.

Fisher, Ali. "Swarmcast: How jihadist networks maintain a persistent online presence." *Perspectives on Terrorism* 9, no. 3 (2015): 3-20.

Fisher, Ali, Prucha, Nico and Emily Winterbotham. *Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability*. London: Royal United Services Institute, 2019. https://static.rusi.org/20190716_grntt_paper_06.pdf.

GIFCT. "Broadening the GIFCT Hash-Sharing Database Taxonomy: An Assessment and Recommended Next Steps." Accessed October 11, 2021. https://gifct.org/wp-content/uploads/2021/07/GIFCT-TaxonomyReport-2021.pdf.

GIFCT. "Membership." Accessed March 12, 2022. https://gifct.org/membership/.

Hassan, Ghayda, Brouillette-Alarie, Sébastien, Ousman, Sarah, Kilinc, Deniz, Savard, Éléa Laetitia, Varela, Wynnpaul, Lavoie, Lysiane et al. *A systematic review on the outcome of primary and secondary prevention programs in the field of violent radicalization*. Montreal: Canadian Practitioners Network for the Prevention of Radicalization and Extremist Violence, 2021. https://cpnprev.ca/wp-content/uploads/2021/03/CPN-PREV-2nd-Systematic-Review-2.pdf.

Hossain, Md Sazzad. "Social media and terrorism: Threats and challenges to the modern era." *South Asian Survey* 22, no. 2 (2015): 136-155, https://doi.org/10.1177%2F0971523117753280.

Jones, Michael. *Through the Looking Glass: Assessing the Evidence Base for P/CVE Communications*. London: Royal United Services Institute, 2020. https://static.rusi.org/pcve_communications_final_web_version.pdf.

Macdonald, Stuart, Correia, Sara Giro and Amy-Louise Watkin. "Regulating terrorist content on social media: automation and the rule of law." *International Journal of Law in Context* 15, no. 2 (2019): 183-197. https://doi.org/10.1017/s1744552319000119.

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

Macdonald, Stuart, Yilmaz, Kamil, Herath, Chamin, Berger, JM, Lakhani, Suraj, Nouri, Lella and Maura Conway. *The European Far-Right Online: An Exploratory Twitter Outlink Analysis of German and French Far-Right Online Ecosystems*. Washington, DC: RESOLVE Network, 2022.

Macklin, Graham. “The Christchurch Attacks: Livestream Terror in the Viral Video Age.” *CTC Sentinel* 12, no.6 (2019): 18-29. https://ctc.usma.edu/wp-content/uploads/2019/07/CTC-SENTINEL-062019.pdf.

Milton, Daniel. *Pulling Back the Curtain: An Inside Look at the Islamic State’s Media Organization*. West Point, NY: Combating Terrorism Center, 2018. https://ctc.usma.edu/wp-content/uploads/2018/08/Pulling-Back-the-Curtain.pdf.

Moonshot. “The Redirect Method.” Accessed September 30, 2021. https://moonshotteam.com/redirect-method/.

Molas, Bàrbara. “Reddit’s Hosting Service and the Dangers of Outlinking.” Accessed September 27, 2021. https://gnet-research.org/2021/09/17/reddits-hosting-service-and-the-dangers-of-outlinking/.

Prucha, Nico. “IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram.” *Perspectives on Terrorism* 10, no. 6 (2016): 48–58.

Ramsay, Gilbert. *Jihadi Culture on the World Wide Web*. New York, NY: Bloomsbury, 2013.

Reed, Alastair, Ingram, Haroro J. and Joe Whittaker. *Countering Terrorist Narratives*. Brussels: European Parliament, 2017. https://www.europarl.europa.eu/RegData/etudes/STUD/2017/596829/IPOL_STU(2017)596829_EN.pdf.

Saltman, Erin, Kooti, Farshad and Karly Vockery. “New Models for Deploying Counterspeech: Measuring Behavioral Change and Sentiment Analysis.” *Studies in Conflict & Terrorism* (2021). https://doi.org/10.1080/1057610X.2021.1888404.

Shehabat, Ahmad and Teodor Mitew. “Black-boxing the black flag: anonymous sharing platforms and ISIS content distribution tactics.” *Perspectives on Terrorism* 12, no. 1 (2018): 81-99.

Tech Against Terrorism. “Analysis: New Zealand attack and the terrorist use of the internet.” Accessed March 7, 2022. https://www.techagainstterrorism.org/2019/03/26/analysis-new-zealand-attack-and-the-terrorist-use-of-the-internet/.

Telegram. “Terms of Service.” Accessed March 11, 2022. https://telegram.org/tos.

Tracking Terrorism. “Islamic State Releases Newspaper “Al Naba” 297 - Released 29 July 2021 (Assaults on PKK, PMU, Afghan, Cameroonian, Congolese, Mozambican & Nigerian Armies).” Accessed September 30, 2021. https://www.trackingterrorism.org/chatter/pdf-islamic-state-releases-newspaper-al-naba-297-released-29-july-2021-assaults-pkk-pmu-afgh.

Twitter. “About Twitter’s link service (http://t.co).” Accessed March 14, 2022. https://help.twitter.com/en/using-twitter/url-shortener.

Twitter. “Our approach to blocking links.” Accessed March 14, 2022. https://help.twitter.com/en/safety-and-security/phishing-spam-and-malware-links.

van der Vegt, Isabelle, Gill, Paul, Macdonald, Stuart and Bennett Kleinberg. *Shedding Light on Terrorist and Extremist Content Removal*. London: Royal United Services Institute, 2019. https://static.rusi.org/20190703_grntt_paper_3.pdf.

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

Whiteside, Craig. *Lighting the Path: the Evolution of the Islamic State Media Enterprise* (2003-2016). The Hague: International Centre for Counter-Terrorism, 2016. https://icct.nl/app/uploads/2016/11/ICCT-Whiteside-Lighting-the-Path-the-Evolution-of-the-Islamic-State-Media-Enterprise-2003-2016-Nov2016.pdf.

Whittaker, Joe. “The online behaviors of Islamic State terrorists in the United States.” *Criminology & Public Policy* 20, no. 1 (2021): 177-203. https://doi.org/10.1111/1745-9133.12537.

Winter, Charlie. *Media Jihad: The Islamic State’s Doctrine for Information Warfare*. London: ICSR, 2017. https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf.

## *About the Authors*

***Professor Stuart Macdonald** is Professor of Law at Swansea University, UK. Stuart is Director of the University's Cyber Threats Research Centre (CYTREC) and a Co-Director of its £7.5m EPSRC Centre for Doctoral Training in Enhancing Human Interactions and Collaborations with Data and Intelligence Driven Systems. Stuart is also the lead organiser of the biennial #TASMConf (Terrorism and Social Media Conference) and co-ordinates the University's contribution to the Global Network on Extremism and Technology (GNET). Stuart's research interests lie in criminal law and counterterrorism, particularly cyberterrorism and terrorists' use of the internet. His most recent work has examined violent jihadist narratives, their dissemination via online platforms, and legal and policy responses. Stuart has held visiting scholarships in the US, Australia and France and in 2016/17 was the holder of a Fulbright Cyber Security Award.*

***Connor Rees** is a PhD candidate at Swansea University. His work covers the role of content moderation by social media platforms, in the context of extremist content removal (specifically the extreme right). Whilst his research looks at online extremism, it expands to Human-Computer Interaction, Ethics, and regulation of Artificial Intelligence within the same remit. Connor teaches a range of classes related to his research and has engaged in numerous interdisciplinary projects in both academia and practice, including the Developing Resistance Against Grooming Online – Spot and Shield (DRAGON-S) project.*

***Joost S.** is an analyst at Moonshot with a focus on far-right extremism, influence operations and online harms in North America and Western Europe.*

RESOLVE NETWORK

better research.informed practice.improved policy on violent extremism.

www.resolvenet.org

RESOLVE is housed at the U.S. Institute of Peace, building upon the Institute's decades-long legacy of deep engagement in conflict affected communities.

United States Institute of Peace
Making Peace Possible

RESOLVE
NETWORK