Encrypted Extremism

Inside the English-Speaking Islamic State Ecosystem on Telegram

BENNETT CLIFFORD AND HELEN POWELL

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

ENCRYPTED EXTREMISM

Inside the English-Speaking Islamic State Ecosystem on Telegram

BY

Bennett Clifford and Helen Powell

June 2019

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

Program on Extremism
2000 Pennsylvania Avenue NW, Suite 2210
Washington, DC 20006
www.extremism.gwu.edu

CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

The authors wish to thank the Program on Extremism's Director Dr. Lorenzo Vidino, Deputy Director Seamus Hughes, and the Program's staff for their invaluable support during the planning, research, writing, and editing stages of this report. Audrey Alexander, Dr. Haroro Ingram, Jon Lewis, and Andrew Mines offered important feedback during multiple stages of project design and implementation. Finally, the authors thank Dr. Amarnath Amarasingam, Chelsea Daymon, and Charlie Winter, amongst others, for their insightful comments on earlier drafts of this report.

Program on Extremism research assistants were responsible for data collection, data cleaning, and processing data for the final version of the report. The authors wish to thank Adib Milani, Scott Backman, Gianluca Nigro, Grant Smith, Nandini Ajmera, Ira Clark, Paul Nestler, Caroline Fearnow, and Matthew Eady, without whom this project would not be possible.

The authors also thank Daniel Kerchner and the Scholarly Technology Group (STG) at the George Washington University Libraries for their indispensable assistance in designing innovative data collection and analysis tools for this project, and Larisa Baste for designing the report.

The views expressed in this publication are solely those of the authors, and not necessarily those of the George Washington University.

The Program on Extremism

The Program on Extremism at George Washington University provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public.

EXECUTIVE SUMMARY

Telegram, an online instant messaging service popular among adherents of the Islamic State (IS), remains vital to the organization's ecosystem of communications. The platform's functional affordances, paired with relatively lax enforcement of Telegram's terms of service (ToS), offers IS sympathizers a user-friendly medium to engage with like-minded supporters and content.

This report examines 636 pro-IS Telegram channels and groups that contain English-language content collected between June 1, 2017 and October 24, 2018. While this time-bound and linguistically limited sample represents a sliver of the pro-IS ecosystem on Telegram, the subsequent findings have important implications for policymakers assigned to the dual tasks of countering IS' online foothold and engaging with service providers like Telegram. Among other findings, this report assesses that:

- **English-speaking IS supporters exploit Telegram's suite of features to communicate with like-minded supporters across the world, disseminate official and unofficial IS media, and provide instructional material for operations.**

    - Pro-IS channels and groups can be categorized into five primary functions: forum, shoutout, instructional, core and distribution. Distribution channels are the largest category within the sample and serve to proliferate all types of pro-IS content without regard to their origin.

    - Across all channels in the sample, IS sympathizers use three primary tactics to ensure community resiliency: proliferating joinlinks, exploiting Telegram's internal file-sharing capabilities, and observing basic cybersecurity measures.

- **English-speaking IS supporters on Telegram are fundamentally concerned about operational security, but their continued reliance on public outreach results in inconsistent application of operational security measures and exacerbates vulnerabilities.**

    - The majority of the sample is comprised of private groups and channels, only accessible through URL keys (joinlinks), but public channels play an important role as key nodes for entry into the private network.

    - Despite Telegram's encryption protocols and privacy protections, English-speaking IS sympathizers continue to rely on insecure public-facing platforms to reach a wider audience. File-sharing sites are particularly popular, representing 15 of the top 20 website base domains shared within the sample.

- **The loss of IS territory and the crackdown against its presence on public-facing platforms forces English-speaking IS supporters to focus on the group's military activities, ensure resilience of their networks on Telegram, supplement official media with unofficial productions, and develop new measures for online guidance of operations.**

    - Within the sample, supporters discuss IS military activities in Iraq or Syria and the activities of IS' affiliates more than IS attacks or events in the West.

    - No single terrorist attack outside IS-held territory generated enough sustained conversation to register as one of the top 25 hashtags by name within the sample.

    - IS sympathizers respond to online and offline pressure against IS media by enabling grassroots actors, proliferating unofficial or "gray" media, and distributing operational and instructional material.

INTRODUCTION

Telegram is currently considered the preferred digital communication tool for IS sympathizers. It serves as a stable online platform for pro-IS content, an ecosystem for building extremist networks, an effective and secure internal communications tool, and a forum for recruiting new IS members. This report, representing an installation of the George Washington University Program on Extremism's "ISIS Online" project, hopes to shed light on IS activity on Telegram to critically inform counterterrorism policymakers, practitioners and researchers, as well as the interested public.

This study seeks to answer the following research questions:

1. **How do English-speaking IS supporters use Telegram's suite of features to build online networks, disseminate propaganda, and guide operations?**
2. **In which ways do English-speaking IS supporters on Telegram balance the need for broad-based messaging and recruitment with the necessity of operational security?**
3. **How do English-speaking IS supporters on Telegram react to pressure against the organization in the online and offline spaces?**

To answer these questions, Program on Extremism researchers collected and analyzed 636 English-language pro-IS channels and groups on Telegram from June 1, 2017 to October 24, 2018. This report presents the comprehensive findings and assessments, combining quantitative data, qualitative observations and case studies captured during the 16-month study.

Program on Extremism researchers collected and analyzed 636 English-language pro-IS channels and groups on Telegram from June 1, 2017 to October 24, 2018. This report presents the comprehensive findings and assessments from the 16-month study.

The report begins by examining background information about Telegram's unique suite of features, IS supporters' exploitation of digital communications technology, and Telegram's counterterrorism efforts. Next the report details the collection, coding and data cleaning process, including the PDF analysis method and limitations of the study. In the analysis section, the report answers each of the three research questions using both quantitative and qualitative findings, supplemented by case studies of individuals who were arrested in relation to their pro-IS activity on Telegram. To conclude, the report offers critical considerations for counterterrorism policymakers, practitioners, researchers, and the media in marginalizing IS supporters on Telegram.

BACKGROUND: ISLAMIC STATE SUPPORTERS' USE OF TELEGRAM

Prior to data analysis and investigating this study's research questions, it is imperative to understand background variables that inform IS supporters' use of Telegram. The following section is a primer on how IS sympathizers use digital communications technologies. It documents basic information about Telegram and the variety of communication options available on the service, explains the factors behind IS' initial adoption of Telegram, and compares Telegram's functionalities to those of other platforms preferred by IS and its supporters. Finally, it briefly examines how Telegram has responded to terrorist use of the platform.

Telegram's Suite of Features

Telegram is an online instant messaging service that is available via client applications for smartphones, tablets, and computers.[1] On August 14, 2013, Telegram's founders Pavel and Nikolai Durov launched the first version of the application, which is available today on dozens of platforms.[2]

According to its developers, Telegram distinguishes itself from similar services by its speed, multimedia capabilities, and security options. Users have the ability to access their accounts and the information stored in it from multiple platforms, simultaneously.[3] Telegram users can share an unlimited number of photos, videos, documents, audio messages, and voice recordings in four different communication options: direct one-to-one **secret chats** and **voice calls**, **groups** and **supergroups** that can include as many as 200,000 members, and **channels** that broadcast to a theoretically unlimited number of users.[4]

Telegram offers end-to-end encryption features for all secret chats and voice calls.[5] For all other forms of communication, the company offers client-server/server-client encryption. Administrators can create public groups and channels that are searchable within Telegram and openly accessible, and private groups and channels which are not searchable and require a URL invite key called a "joinlink" to access.[6] In addition to encryption and privacy settings, Telegram offers a strict pledge to "disclose 0 bytes of user data to third parties, including governments."[7] Furthermore, Telegram places their physical cloud servers around the world to prevent any particular government or authority from having sole jurisdiction.[8]

IS Supporters' Use of Telegram

IS' global network of supporters—whom they term *munasireen*—uses Telegram as part of a larger infrastructure of digital communications technologies with several, interrelated functions. These technologies offer a variety of functions that extremist groups exploit, including "content hosting, audience development, brand control, secure communication, community maintenance, financing, and information collection."[9] Laith Alkhouri and Alex Kassirer refer to this array of technology applications as the "digital toolbox."[10] IS, like other jihadist groups, appears to select applications from the toolbox that suit particular needs, and sometimes encourage adoption by their supporters. Simultaneously, the specific digital communications technologies that IS *munasireen* choose to utilize and the services technologies offer also shape the nature of jihadists' strategies for digital communication.[11]

IS' major goals in utilizing the digital toolbox include facilitating communications between supporters worldwide, disseminating propaganda, and distributing information and instructions from the group's central leadership to its acolytes. To this end, IS and its supporters make use of a variety of digital communications tools, including instant messengers, social media, file-sharing sites, browsers, and mobile security services.[12] The use of specific technologies ebbs and flows as service providers attempt to limit terrorist exploitation of their applications, supporters find new platforms, and IS' strategies change.

Today, Telegram is the centerpiece of IS supporters' online communications strategy. IS' use of Telegram is frequently cited in the media as evidence of a new frontier in online jihadist communications.[13] However, the current phenomenon and the trends behind it are not historically unique. First, IS is not the first jihadist group to leverage online communication tools. Beginning in the

1990s and moving into the 2000s, several jihadist groups built a stable presence on the internet, mainly through the establishment of top-down official websites, e-forums, and chatrooms.[14] When social media emerged as a facilitator for the Arab Spring, jihadist organizations adopted public-facing social media services like Facebook and Twitter, as well as online media-sharing platforms like YouTube.[15]

Many point to the recent trend towards terrorist groups exploiting privacy-maximizing services, including end-to-end encrypted messengers, virtual private networks (VPNs), secure browsers, and mobile security applications, as newfound policy concerns.[16] However, a more thorough review shows that supporters of jihadist groups consistently strived to occlude their online activities through encryption protocols. For instance, al-Qaeda's Global Islamic Media Front (GIMF) released the first version of its encryption software, *Asrar al-Mujahideen* (Secrets of the Mujahideen) in 2007, with several updated versions in the following years.[17] In 2013, GIMF released a follow-on program, *Asrar al-Dardashah* (Secrets of Chatting), which offered encryption for popular online instant messengers and chat forums, including Google Chat, MSN, Yahoo, and PalTalk.[18]

While IS supporters continue to be active on several public-facing sites, efforts to enforce terms of service (ToS) hampered IS' presence on the public web.

Moreover, encryption is only partially relevant in explaining why IS *munasireen* choose Telegram. While end-to-end encrypted messaging is often cited as the major, if not the only reason that jihadists built an infrastructure on Telegram, not all jihadist communications on the service are covered by end-to-end encryption.[19] Telegram's encryption protocol (MTProto) is widely criticized by experts in cryptography, and its security is questionable compared to its competitors in the instant messenger market.[20] It is not clear whether Telegram users that view the platform as secure believe that their privacy is protected by encryption, or by Telegram's pledge to not share data with governments. However, commentators often conflate these two features or mistake Telegram's privacy guarantee for "encryption." To understand why IS supporters gravitate towards the platform, it is imperative to take into account how Telegram fits into the broader digital toolbox, and how supporters exploit particular platforms.

Telegram emerged as the standard-bearer following a strategic relocation by *munasireen* away from mainstream, public-facing social media, chatrooms, and file-sharing services. A combination of factors, including enhanced enforcement of terms of service (ToS) on the public-facing web and the desire for improved operational security, caused a major shift of online IS supporters to Telegram and similar platforms. While IS supporters continue to be active on several public-facing sites, efforts by service providers to enforce ToS and the growing popularity of Telegram hampered IS' presence on the public web.[21]

The strategic use of Telegram and other encrypted messengers was initially part of a concerted effort by IS' external operations wing, which retained staffs of online facilitators directly responsible for such outreach.[22] These facilitators, referred to as "virtual entrepreneurs" or "virtual plotters," were responsible for directing 19 out of the 38 IS-related attacks in Western Europe from 2014 to 2016, and additionally played a role in several plots in the United States, Canada, and Australia.[23] Starting from mainstream social media platforms like Twitter and Facebook, virtual entrepreneurs would identify and contact individuals who were interested in planning attacks on behalf of IS, direct them to an instant messenger with end-to-end encryption (including Telegram), and provide instructions on successfully carrying out an attack.[24]

Aside from person-to-person operational communication, IS media divisions and affiliates also exploit Telegram as a dissemination outlet. Using channels and groups, IS supporters publish and re-post IS' official videos, audio messages, documents and rulings, photo albums, and press releases on the platform.[25] Following attacks or operations, Telegram channels and groups are usually key nodes in the dissemination of IS' official claims of responsibility, published through "official" and "unofficial" core news networks like Amaq News Agency and Nashir News Agency.[26] The groups' supporters continuously add and create new channels to remain abreast of new developments within IS territory, new media releases, and updates on critical news stories. They also augment these releases with unofficially produced propaganda and media.[27]

In a 2016 study, Nico Prucha describes Telegram as the coordination point for the "jihadist information highway," a multi-stage process for distributing IS' official videos, photosets, magazines and news releases across the internet.[28] As early as 2015, IS media teams used Telegram channels to encourage followers to spread the group's official media by 1) uploading content onto file-sharing sites and 2) sharing links on public-facing social media sites.[29] The same study also describes IS' procedure for circumventing ToS enforcement on specific social media platforms. On other Telegram channels, the group's media operatives organize coordinated *ghazawat* (raids), in which they request followers to upload a particular video or create new social media accounts on a specific platform like Twitter and Facebook.[30] Through this process, IS maintains a foothold on the public web and actively struggles against measures to enforce ToS, such as account suspensions or content removal.[31]

However, IS supporters' reliance on Telegram also entails significant drawbacks, as its privacy features can make outreach and recruitment more difficult. Due to the necessity of accessing a joinlink to enter a private channel or chat group, it is much less likely that an uninitiated observer will "stumble" upon jihadist propaganda on Telegram as compared to the public-facing web.[32] Miron Lakomy argues that the shift to closed forums like Telegram have slightly improved online operational security for IS supporters at the expense of expanding online networks and the virality of IS media campaigns.[33] In the early days of IS' Telegram usage, channels warned their followers about the limitations of the platform in this regard:

> Telegram is not a media platform for *dawa* [proselytization] to all Muslims and the West. No one will enter your channel except for the *Ansar* [supporters] who already know the truth… Rarely would you find someone from the general public following you. That's why our main platform is where the General Public is found. Like on Twitter and Facebook.[34]

The shift from public-facing social media platforms to Telegram and other reclusive services details how IS' online supporters responded to pressure against the organization online. Namely, English-speaking IS sympathizers demonstrated agility and alacrity in moving between a large array of digital communications technologies when sites like Twitter and Facebook scaled up their respective ToS enforcement. This history can be critically important in assessing how supporters on Telegram may respond if the company adopts a more stringent approach to regulating terrorist content.

Telegram, Terrorism, and Terms of Service

Telegram's security features, coupled with the company's reticence about cooperating with governments and third parties on data requests in its ToS, place it in the public eye and on the radars of law enforcement throughout the world. According to Pavel Durov, one of Telegram's founders, his contentious interactions with the Russian government when he owned the Russian social media site *vKontakte* significantly influenced Telegram's development.[35] The launch of Telegram was designed to provide a secure and private messaging platform to shield users in authoritarian countries from government monitoring and surveillance.[36] However, when malign actors who also seek to avoid online surveillance exploit Telegram's features, the company's response often becomes a critical test case for long-standing debates about online privacy, encryption, and balancing security with freedoms of speech and expression.

Perhaps the greatest test facing Telegram's stance on online privacy is how it chooses to respond to the exploitation of the service by terrorist groups. The guarantees that Telegram provides users—especially its promise to not provide information to governments—are understandably attractive to users with widely different intentions, including malicious ones. An inflection point in the debate over the use of Telegram by terrorist groups emerged after the November 2015 attacks in Paris, France when a cell of IS affiliates that used the application to communicate internally killed 130 people in the deadliest jihadist attack in French history.[37] Since the Paris attacks, IS inspired or directed additional attacks in Europe using Telegram's group and secret chat features.[38] Among the deadliest include the December 2016 truck-ramming attack on a Christmas market in Berlin, Germany, and the mass shooting at the Reina Nightclub in Istanbul, Turkey weeks later.[39] In each case, the attackers are believed to have received direct instructions from IS members in Syria and Iraq regarding their planned attacks via Telegram's secret chat function, alongside other sources.[40]

In a 2015 statement released days after the Paris attacks, Telegram claimed to have removed approximately 80 ISIS public channels that were active on the platform at the time of the attacks.[41] The company reiterated that despite this move, it would retain its policies of not shutting down groups, private channels, or secret chats, refrain from account suspensions, and most importantly, continue its pledge to withhold user information from governments.[42] This policy decision shaped Telegram's approach to terrorist content on its service. It created a dichotomy between secret chats, groups, and private channels—which the company views as private data not subject to regulation—and public channels, which the company argues are publicly available and therefore subject to limits. Since 2016, Telegram operates a channel called "ISIS Watch" which highlights its efforts to delete public channels and bots on the service that promote terrorist content.[43] To date, the channel claims Telegram removed over 200,000 ISIS public channels and bots.[44] The company's method for identifying and monitoring these channels is undisclosed, and presumably Telegram still will not suspend users, delete groups, or turn over profile information.

However, a shift in the Telegram Privacy Policy signals that the company may be changing its tune on information sharing with third parties, partially in response to the European Union's General Data Protection Regulation (GDPR).[45] In August 2018, Telegram published section 8.3 of its privacy policy, which claims that, "if Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities."[46] To date, Telegram reports that "this has never happened," but that the company will include any instances of enforcement in a semiannual transparency report.[47]

It remains unclear how this change in policy will affect decisions by groups like IS to utilize Telegram. In combination with the update to Telegram's privacy policy, law enforcement on both sides of the Atlantic have made high-profile arrests of IS-inspired suspects using evidence from Telegram.[48] In recent months, IS supporters attempted to create a presence on several other services which contain features similar to Telegram after an uptick in channel suspensions.[49] So far, none of IS' diversification efforts heralded the same success as the shift from public-facing social media to Telegram in 2015-2016.[50] For the time being, IS' online supporter networks may continue to be reliant on Telegram due to the unique blend of features that it offers.

In sum, conceptualizing jihadist use of digital communications technology as a coordinated, multi-platform infrastructure helps correct three common mistakes in assessing IS' use of Telegram. First, while neither Telegram nor IS' embrace of the service is unparalleled, the combination of several important tools (one-to-one, one-to-many, and group communications; expanded file-sharing; end-to-end encryption; and guarantees of online privacy and security) is highly desirable. Second, other services offer stronger encryption and only some communication on Telegram is end-to-end encrypted. Finally, the 2015-2016 shift to Telegram in the wake of pressure did not represent the end of IS supporters' fight to remain relevant on the public-facing web. Instead, it wrought new dimensions in the fight against IS online as supporters leveraged Telegram to circumvent ToS enforcement.

METHODOLOGY

The following section provides a comprehensive account of this study's methodology, with the intent of detailing the viability and limitations of the dataset and informing other researchers interested in conducting similar studies in the future. The study's methodology is designed to answer the following research questions:

1. **How do English-speaking IS supporters use Telegram's suite of features to build online networks, disseminate propaganda, and guide operations?**
2. **In which ways do English-speaking IS supporters on Telegram balance the need for broad-based messaging and recruitment with the necessity of operational security?**
3. **How do English-speaking IS supporters on Telegram react to pressure against the organization in the online and offline spaces?**

To answer these questions, researchers used a mixed-method approach. Somewhat limited by Telegram's privacy features, this method relied on manual coding, PDF analysis, and open-source research on case studies captured in the data set. This methodology section begins with a brief description of the project, followed by a detailed presentation of the collection, coding, and data cleaning approach. Next, the section presents the method for PDF capturing and analysis, and concludes by addressing the study's limitations.

About "ISIS Online" and the Telegram Project

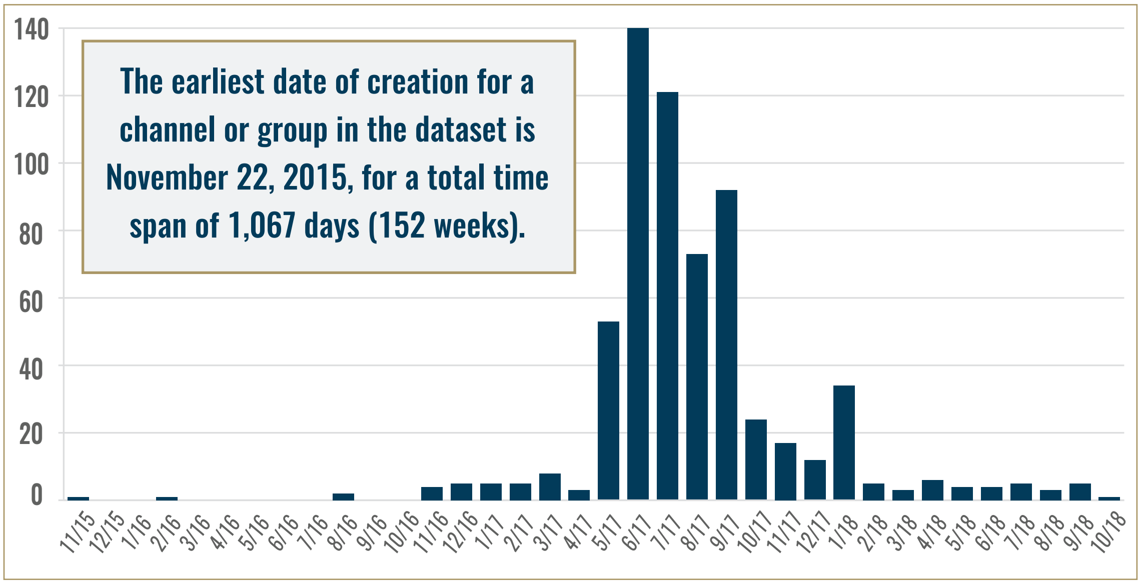
Researchers from the George Washington University Program on Extremism (PoE) conducted data collection on Telegram as part of PoE's "ISIS Online" project, which tracks the usage of digital communications technologies by English-speaking IS sympathizers. Following PoE's publication *ISIS in America: From Retweets to Raqqa* in 2015, researchers collected over 1,000,000 tweets from English-language pro-IS Twitter accounts, analyzing the data in the 2017 report *Digital Decay: Tracing Change over Time Among English-Language Islamic State Sympathizers on Twitter.* During the data collection process for *Digital Decay,* researchers also accessed pro-IS Telegram groups and channels from joinlinks shared on public social media. Starting from this initial "root" sample of channels and groups, PoE initiated systematic collection of pro-IS Telegram channels and groups with English-language content in June 2017.

From June 1, 2017, to October 24, 2018, PoE researchers collected 727 public and private Telegram channels and groups. The findings of this study are based on an analysis of 636 channels and groups which met final data selection standards. Notably, once a researcher joined a group or channel they gained access to posts dating back to the date of creation, backdating the sample.[1] Researchers were instructed to scroll back to the beginning of each channel to collect the channel, obtain a PDF capture and record its data.[2] At the time of collection, some groups and channels were active for an extensive period of time. The earliest date of creation for a channel or group in the dataset is November 22, 2015, giving the sample a total time span of 1,067 days (152 weeks). This allowed researchers to collect and assess content shared before data collection technically began. *Figure 1* shows the number of groups, supergroups, and channels created on each of the 1,067 days in the data timespan.

Despite limitations on scope and transferability, this snapshot of a specific, contextualized example of IS' exploitation of digital communications technology provides insight into how IS sympathizers use Telegram as both a communication and dissemination tool. The report adopts a mixed-method approach, pairing quantitative and qualitative assessments of the sample with individual case studies to shed light on how IS sympathizers use Telegram to further their goals.

Collection

This report's authors directed a research team of eight research assistants during the collection phase of the study, training each researcher in the selection and coding criteria detailed below. Using three



Date Created

The earliest date of creation for a channel or group in the dataset is November 22, 2015, for a total time span of 1,067 days (152 weeks).

Figure 1. This chart depicts the date of creation of the 636 groups/supergroups/channels in the sample.

anonymous Telegram accounts with jihadist credentials on designated computers, project researchers employed a snowball sample, adding channels and groups using joinlinks posted in previously added entries. Utilizing the selection criteria, researchers determined whether joined channels and groups should be included in the sample, and assigned several variables to channels and groups that met the threshold. To preserve the integrity of the sample and preclude ethical and security concerns, researchers were prohibited from posting in Telegram groups and channels, or directly messaging any Telegram user besides the project-designated accounts.

Selection Criteria

To qualify for selection, the study's parameters required that groups and channels were pro-IS and included English-language content. To meet the first criterion, researchers determined whether more than 50% of a channel's English-language content was explicitly pro-IS. Indicators of pro-IS sympathies included: re-posting or sharing official IS media, the creation of unofficial pro-IS media, or overt declarations of support by channel or group administrators for IS or its mission, goals, activities, and operations. Researchers avoided coding channels or groups which supported other jihadist groups or expressed general sympathy for the jihadist movement without endorsing IS specifically, and were instructed to exclude channels and groups that fell close to the threshold. As pro-IS Telegram channel and group administrators are generally strict in their enforcement of ideological allegiance, most of the sample easily surpassed the 50% threshold.

Additionally, Telegram groups or channels in the sample met a minimum requirement of one post in English. The report authors initiated this criterion to connect this study with PoE's broader focus on English-speaking IS sympathizers online, but adjusted the minimum standard to appropriately capture the notable language fluidity within pro-IS Telegram channels and groups. For instance, PoE's criteria for collection on a previous Twitter study ascribed to a minimum standard of over 50% English-language content.[3] The one post standard reflects an adaptation to Telegram users' utilization of a variety of languages in groups, frequently with English as a *lingua franca.*[4]

Coding Process

When the project began in June 2017, Telegram's regulated API and minimal download features placed limitations on data collection.[5] To circumvent these obstacles, researchers used the print-save-as function while accessing Telegram from its web client to obtain Portable Document Format (PDF) files of group and channel histories. As previously mentioned, when researchers joined channels and groups, they could access all posts (including shared URLs, joinlinks, documents, videos, and photos) dating back to the creation of the group or channel.[6] This feature allowed the database time variable to extend retroactively beyond the data collection period to November 2015.

PDF capturing allowed researchers to record channel and group histories, retaining a backup copy of all posts in the channel or group in the event of loss of access. It also created a stable, accessible format for data analysis tools. However, this method also limited data collection to a snapshot of activity at the point in time of coding, preventing documentation of what occurred in the channel or group after coding. In addition, researchers frequently encountered disabled channels or groups. The parameters of the study and Telegram's protections on metadata prevented the determination of the date of closure, whether the closure was voluntary or the result of Telegram's ToS enforcement, and whether administrators banned or removed researchers' accounts from their channel or group.

Researchers compiled a database of all collected channel and group PDFs. Using the PDFs, researchers added entries to an Excel spreadsheet of quantitative and qualitative observations at the time of snapshot. The PDF database enabled retroactive analysis of shared content, including external links, hashtags, and joinlinks. In the spreadsheet, researchers recorded basic information about the channel or group, including quantitative and binary observations. (See table below.)

Additionally, researchers coded qualitative assessments of entries. First, using a classification system developed by the report authors, researchers sorted the groups and channels into five categories separated by primary function. (See table on next page.)

Using seven binary variables, researchers also noted the presence or absence of discussions within channels and groups on six topics determined by the project team prior to data collection. These topics, modeled on previous studies of IS online propaganda,[7] include:

- IS military activities, battles, attacks, and campaigns in Syria and Iraq
- IS non-military activities in Syria and Iraq
- IS external provinces' (*wilayat*) activities outside Syria and Iraq
- IS attacks in Europe and North America
- News and events in Europe and North America
- Cybersecurity, information security, or operational security

This sample presents a window into English-speaking IS sympathizer activity on Telegram using data gathered from collection, supplementing the information with

Observation Variables

Qualitative Variables

Name of Channel/Group	Channel/Group Information
Date and Time of Channel/Group Creation	Type (Channel/Group/ Supergroup)
Access (Public or Private)	Joinlink to Access
Primary Language	Date and Time of Data Entry

Quantitative Variables

Photos	Videos
Audio Files	Documents
Voice Messages	Members

Figure 2. These tables list the observations collected about Telegram channels and groups.

Categories of Groups and Channels

Category	*Explanation*
Core	Dedicated to content from IS propaganda brands understood to be directed by IS central media divisions in Iraq and Syria
Distribution	Dedicated to distributing a collection of pro-IS content, including both official and unofficial media
Forums	Groups and supergroups with multiple posters and user interaction
Shoutout	Dedicated to sharing joinlinks to other pro-IS groups or channels
Instructional	Dedicated to informative material, including cybersecurity measures or operational instructions

Figure 3. This table defines the five categories assigned to channels and groups in the study.

qualitative assessments and case study analysis. While the dataset does not represent the entirety of IS activity on Telegram, it reveals important insights for this specific demographic of English-speaking IS online *munasireen.*

Data Cleaning

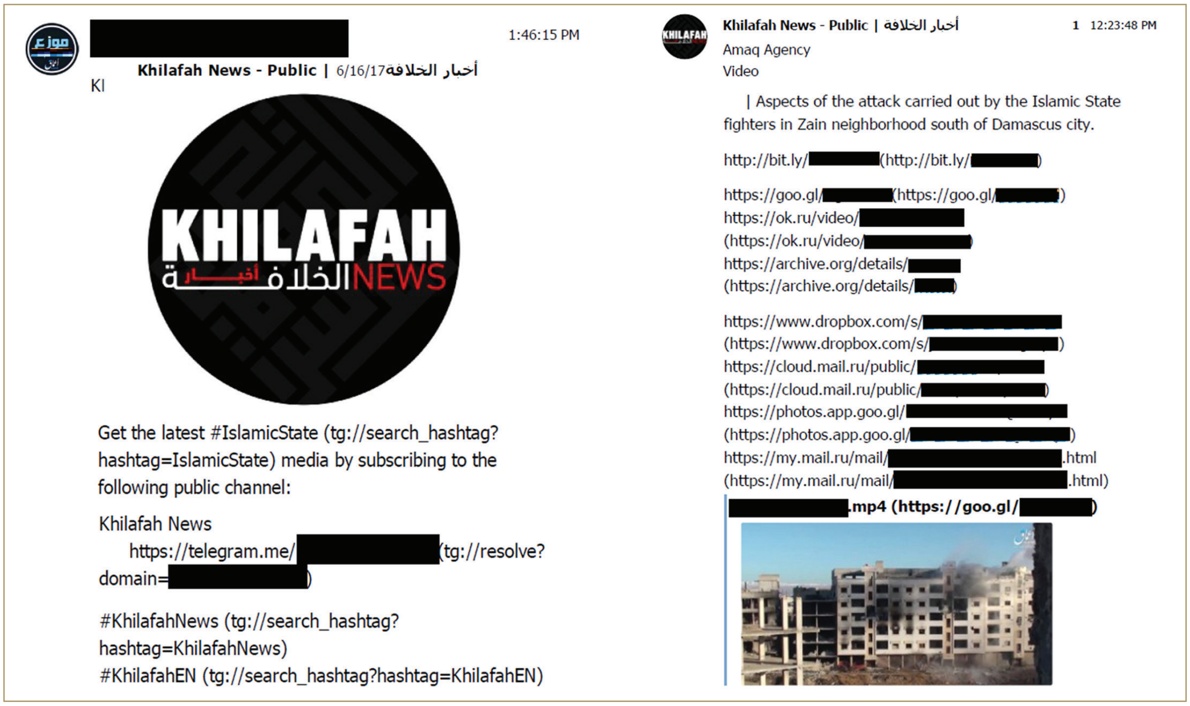
To ensure the veracity of the sample, researchers periodically searched for entries with missing variables, joinlinks, or PDF captures. Researchers verified that all entries included a PDF capture of the group or channel and a copy of the joinlink. Additionally, during data cleaning, the report authors checked PDF entries to ensure that the channel or group in question both 1) met selection criteria and 2) were coded correctly. Throughout the course of data collection, researchers conducted four rounds of data cleaning, followed by a final check in February 2019. The conclusive data cleaning resulted in a final database of 636 groups and channels, including 38,498 pages of PDF snapshots.

PDF Analysis

To conduct a complete analysis of the 636 PDF snapshots in the sample, PoE partnered with the Scholarly Technology Group (STG) of the George Washington University Libraries.[8] STG developed URIScrape, a custom Python tool, using freely available Python libraries such as "pdfminer"[9] for extracting text from PDFs, "re"[10] for regular expression pattern matching, and "urllib"[11] to facilitate parsing of URLs. Researchers utilized URIScrape v0.2.2 to extract URLs from the PDF to capture and refine them into structured data.[12] With each URL discovered in the text, the tool collected the date and time posted in the corresponding group or channel. Secondly, the print-save-as function's translation from Telegram's web client to PDF resulted in some URL duplication, so the code deduplicated these using pattern-matching to a set number of characters beyond the URL's domain name. URIScrape also matched Telegram-specific URL patterns to classify each URL into three categories: internal hashtags, internal joinlinks, and external URLs.[13] Finally, URIScrape exported the URLs, along with each URL's posting date, category, link domain, and other components, into an Excel spreadsheet.

Next, researchers imported the spreadsheet into Jupyter Notebook, loading the data into a Pandas[14] data frame to facilitate analysis. Researchers generated various statistical reports from the data and exported these to .csv files for data visualization.

The analysis in Jupyter Notebook transformed the 17,482 URLs classified as joinlinks into a list of nodes and edges, exported this table into .csv format, and imported the .csv table into Gephi for data visualization as a network graph. This graph represents connections among the 636 collected Telegram groups and channels, as well as connections to groups and channels outside the sample.



[redacted] 1:46:15 PM

Khilafah News - Public | 6/16/17أخبار الخلافة

Kl

Get the latest #IslamicState (tg://search_hashtag?hashtag=IslamicState) media by subscribing to the following public channel:

Khilafah News
https://telegram.me/[redacted](tg://resolve?domain=[redacted])

#KhilafahNews (tg://search_hashtag?hashtag=KhilafahNews)
#KhilafahEN (tg://search_hashtag?hashtag=KhilafahEN)

Khilafah News - Public | أخبار الخلافة 1 12:23:48 PM

Amaq Agency
Video

| Aspects of the attack carried out by the Islamic State fighters in Zain neighborhood south of Damascus city.

http://bit.ly/[redacted](http://bit.ly/[redacted])

https://goo.gl/[redacted](https://goo.gl/[redacted])
https://ok.ru/video/[redacted]
(https://ok.ru/video/[redacted])
https://archive.org/details/[redacted]
(https://archive.org/details/[redacted])

https://www.dropbox.com/s/[redacted]
(https://www.dropbox.com/s/[redacted])
https://cloud.mail.ru/public/[redacted]
(https://cloud.mail.ru/public/[redacted])
https://photos.app.goo.gl/[redacted]
(https://photos.app.goo.gl/[redacted])
https://my.mail.ru/mail/[redacted].html
(https://my.mail.ru/mail/[redacted].html)

[redacted]**.mp4 (https://goo.gl/[redacted])**

Figure 4. Left: Example of a joinlink to a public Khilafah News Channel accompanied by internal hashtags. Right: Example of an Amaq video shared via external URLs to various file-sharing sites. Both images are taken from the PDF database which rendered all clickable links into full URLs causing the parenthetical duplication.

The URL sample included 55,423 internal hashtags. Hashtags were grouped by week based on their posting dates, to determine the top hashtag per week. In addition, the tool extracted 46,579 external URLs (all links with destinations outside of Telegram) with the date of share. Borrowing an established methodology from *Hyperlinked Sympathizers: URLs and the Islamic State,* a study of URLs shared within PoE's Twitter collection database, researchers used customized code to resolve and classify URLs by their base domain. The code also resolved accessible link-shortened URLs (such as those using bit.ly) to their final destination where possible.[15]

Researchers then classified the database of external URLs into categories based on domain type. First, researchers sorted the 20 most frequent base domains into website types, allowing for automatic categorization of 77% of the URL sample. Researchers manually coded the remaining 23% of the 46,579 base domains into ten different categories. (See table on next page.)

Additional Comments on Limitations

While many limitations are addressed throughout this section, some deserve additional consideration. The final database of 636 groups and channels provides insight into how a specific demographic of IS sympathizers use Telegram as both a communication and distribution tool. Due to its narrowed scope, the transferability of this sample is limited. Telegram's metadata constraints prevented researchers from identifying information typically available on open API social media platforms such as the location of users, when a group or channel closed, or if a channel or group closed voluntarily or was taken down. Moreover, the linguistic focus of the sample (on content in English) restricts the assessments made by this report to only a small percentage of IS activity on Telegram.[16]

The time variable is particularly restrictive as the sample is a snapshot of 636 groups and channels collected at different times throughout the year. Data collection

Categorization of External URL Base Domains

Category	*Explanation*
File-sharing: General	File-sharing sites for any or multiple media, including cloud storage.
File-sharing: Video	File-sharing sites used exclusively to share videos.
File-sharing: Photo	File-sharing sites used exclusively to share photos.
Social Media	Social media and social networking sites.
News and Commentary	News sites, blogs, and political commentary.
Government Website	Any official government website.
Jihadist Website	Any website maintained by a jihadist group.
Unresolved Link Shorteners	URLs using link shorteners with an inaccessible final destination.
Other	
Website Inaccessible	Website could not be accessed.

Figure 5. This table defines the categories used in defining the domains for external links shared in the groups and channels.

revolved around the academic schedule of the project's research assistants and was limited to working hours (0900-1700), resulting in inconsistent collection over time and throughout the day. Due to irregular collection, the sample is insufficient for assessing whether activity increased or decreased over the term of the collection period. The working hours limitation also prevented researchers from collecting channels and groups which were created and rendered inaccessible outside of that timeframe, especially content created in different time zones. Finally, the project team consistently tracked channels and groups on Telegram through the collection period, however, not all observed channels and groups met the threshold for the final sample.

Researchers also recorded the number of members in each channel and group. At the time of snapshot, the sample captured a total of 100,633 members, yielding an average of 158 members per channel or group. While this is a tempting metric for analysis, membership is not a reliable indicator of a Telegram channel or group's popularity or activity.[17] Within this study, member counts are skewed by the varied time of snapshot within the lifecycle of a channel or group. In general, the inability to determine who is operating a Telegram account prohibits membership from being an accurate measure of a channel or group's reach into the pro-IS community. Not every member of a channel or group is an IS sympathizer. It is highly likely that other researchers, counterterrorism officials, curious onlookers, and trolls are captured in the membership count to an indeterminate degree. Furthermore, individuals can operate multiple Telegram accounts using fake phone numbers and duplicate their appearance in groups and channels. This report offers analyses of individual users' activities on Telegram where effective data is available, such as in case studies or analyses of actions taken by channel or group administrators, but it cannot assess the intentions or strategies of individual members of channels or groups.

ANALYSIS

To answer the study's research questions, the following section uses quantitative and qualitative analysis to discuss notable trends within the 636 pro-IS Telegram channels and groups in the sample. Subsequently, it evaluates three cases of English-speaking IS supporters whose activity on Telegram was observed within the sample. These case studies highlight critical dynamics in the IS ecosystem on Telegram, and provide context to the study's results.

While the limitations of this study preclude the findings from representing the entirety of IS activity on Telegram, they reveal important insights about how and why this specific demographic of English-speaking IS online *munasireen* utilize the platform.

Results

This study finds that:

- **English-speaking IS supporters exploit Telegram's suite of features, including communications options, joinlinks, internal file-sharing capabilities, and privacy protections, to communicate with like-minded supporters across the world, disseminate official and unofficial IS media, and provide instructional material for operations.**

- **English-speaking IS supporters on Telegram are fundamentally concerned about operational security, but their continued reliance on public outreach results in inconsistent application of operational security measures and exacerbates vulnerabilities.**

- **The loss of IS territory and the crackdown against its presence on public-facing platforms forces English-speaking IS supporters to focus on the group's military activities, ensure resilience of their networks on Telegram, supplement official media with unofficial productions, and develop new measures for online guidance of operations.**

1. How do English-speaking IS supporters use Telegram's suite of features?

In their use of Telegram, English-speaking IS supporters have access to a plethora of different tools to generate, package, and distribute their messaging. When a Telegram user decides to initiate a multi-user message stream, they must first choose from a list of communications options which includes channels, groups and supergroups.[1] *Figure 6* shows a breakdown of the 636 pro-IS channels, groups and supergroups. Channels dominate the sample at 88%. This is an expected result, as channels offer several specific features that benefit IS sympathizers. Primarily, channels allow the administrators to control the flow of information. Only those with administrator status can post within a channel, as opposed to groups or supergroups where multiple members can post. Administrators of channels can post their own multimedia content, forward content from other channels and groups, and share files, joinlinks, or external URLs.

Channels, Groups, and Supergroups

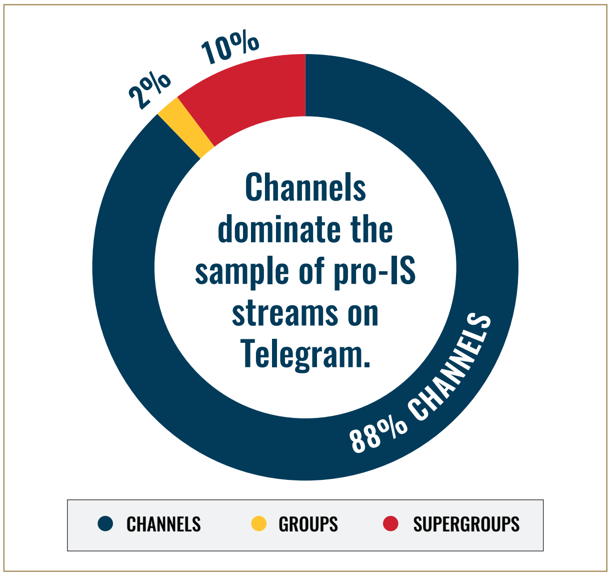


Figure 6. This chart depicts the breakdown of channels, groups, and supergroups in the sample.

Supergroups make up 10% of the sample, with regular groups representing less than 2%. Supergroups are likely preferred to groups due to the increased administrator capabilities and higher member limit. Whereas regular groups can give equal administrator privileges to each member, supergroups can limit privileges to specific administrators and provide more variety in these privileges. For example, the supergroup creator can designate administrators with distinct privileges to approve new users or block members.[2] These functions enable multiple people to share some responsibilities of running a supergroup, while the creator remains in control. Another useful feature of supergroups is the higher member capacity. Telegram exponentially increased the maximum capacity of supergroups over the years, from 5,000 in 2015[3] to 10,000 in 2017[4], and 200,000 in 2018.[5] The largest supergroup in the sample, however, only contained 3,891 members. Though the idea of the increased maximum capacity of supergroups is likely appealing, it is not a feature of necessity for IS sympathizers in the sample.

Once pro-IS users choose a communication option to create a multi-user message stream, they also select a main objective for their communication outreach. Researchers categorized these goals into five primary functions of groups and channels: interacting with like-minded supporters (Forum), sharing joinlinks (Shoutout), sharing operational instructional material (Instructional), sharing "official" IS media (Core), or sharing all pro-IS media (Distribution). Though channels and groups can combine functionalities, researchers found that channels and groups tended to serve one of these five specific purposes in the IS ecosystem on Telegram.

Primary Function

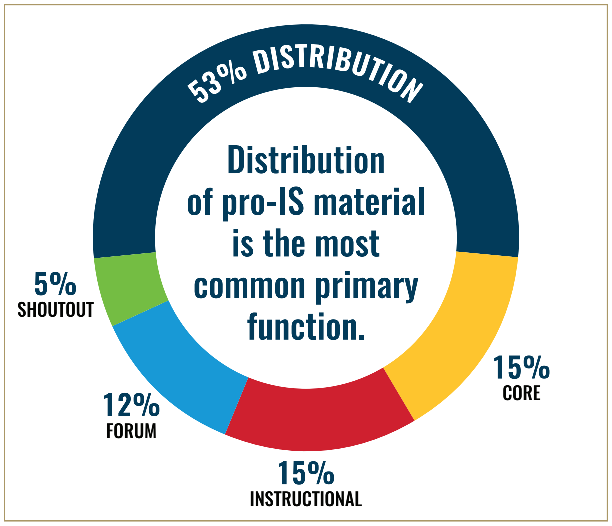


Figure 7. This chart depicts the sample categorized by primary function.

Forums, which represent 12% of the sample, provide space for users to interact, distribute media, and communicate. Comprised of groups and supergroups, the forum function importantly allows multiple users to post their own messages, a disabled feature in channels. Conversations in forums are often multi-tiered, with different pairs of users having distinct conversations. Users can randomly interrupt conversations to consecutively post pro-IS content, trying to jettison propaganda into the group repository as quickly as possible. In forums, administrators act as minor authorities, maintaining order, posting rules, and threatening to remove those who disobey. Occasionally, members request administrators to remove specific users who they believe are trolls, spies, or disbelievers. These requests can be ignored or heeded by administrators. Forums often have a general topic or purpose, such as regional interests or propaganda distribution, though the topic can easily change given the group dynamics.

Shoutout channels represent a small but influential portion of the sample. Shoutout channels systematically distribute joinlinks to other groups and channels of interest. Reminiscent of the use of "Baqiya family shoutouts" by IS sympathizers on Twitter,[6] shoutout channels ingrain resiliency in the community by creating updated joinlink repositories. Some shoutout channel administrators appear to use Telegram bots to automatically forward joinlinks from other channels, reducing the amount of effort required to maintain shoutout channels and multiplying the impact of a single active administrator. Additionally, shoutout channels often use general, benign channel names and refrain from posting IS propaganda to limit the possibility of discovery. Aside from the occasional channel profile image and the destination of shared joinlinks, shoutout channels typically remain innocuous.

Instructional channels distribute instructional material, defined as compiled, published, and disseminated information on how to assist terrorist groups successfully and inconspicuously.[7] Broadly classified, the bulk of pro-IS, English-language instructional material on Telegram can be split into three categories of content: explosives construction, low-tech methods, and operational and cybersecurity measures.[8] This study's sample of Telegram channels and groups contains 94 channels whose main purpose is the dissemination of instructional material, representing 15% of the total. These channels maintained an average member count of 113 members, and in total, the channels shared 7,692 photos, 3,712 files, 1,365 videos, 1,622 links, 293 audio files, and 25 voice messages. Telegram's massive internal file-sharing capabilities make it easy for administrators to disseminate instructional material like large PDF textbooks, step-by-step video tutorials, or screenshotted instructions with successive administrator notes.

Broadly classified, the bulk of pro-IS, English-language instructional material on Telegram can be split into three categories of content: explosives construction, low-tech methods, and operational and cybersecurity measures.

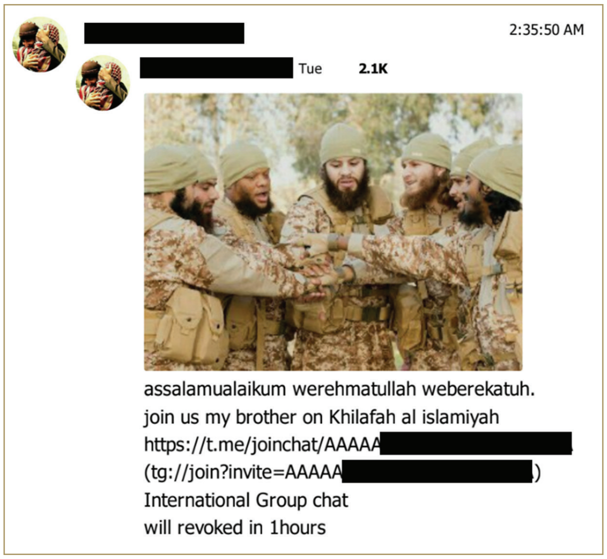
The final two functional categories are **distribution** and **core channels**. Core channels, representing 15% of the sample, are exclusively dedicated to the dissemination of core IS media. Core IS media includes IS propaganda brands understood to be directed by IS' central media department, ranging from outlets within the IS central media department itself (e.g. al-Hayat Media Center, al-Bayan Radio, al-Furqan Media Foundation) to outlets that take strategic direction from the central media division (e.g. Amaq News Agency, Nashir News Agency). Using the terms "official" or "unofficial" to designate core content is limiting, as some core outlets rely on strategic ambiguity, portraying themselves as independent outlets while receiving direct orders and information from IS' central media department.[9] Ultimately, core channels serve a meaningful role in the Telegram ecosystem as they are assumed by supporters to be authoritative outlets of IS central media, regardless of their positioning vis-a-vis IS' central media departments. Importantly, core channels self-identify as IS media outlets in their channel names. It is difficult if not impossible to determine a specific channel's true relation to an IS media outlet or leadership, as individual IS sympathizer could easily create or replicate a core channel. In core channels, administrators rarely share comments and instead post pre-packaged media updates alongside files using Telegram's internal file-sharing capabilities, and/or links to content hosted on external file-sharing sites. While some core channels exclusively share content from a single media outlet, others share an assortment content including repositories of *Dabiq* and *Rumiyah*, updates from IS *wilayat*, and previously-released propaganda films.

Distribution channels, representing the majority of the sample, also share pro-IS media, but without regard to its origin. Combining elements from the other channel functions, distribution channels broadcast any and all information that could be of use, or interest, to the pro-IS community on Telegram. These channels share a smattering of core propaganda, pro-IS media from unofficial outlets, cybersecurity instructions, operational instructions, primary source materials from IS ideologues, forwarded messages from other channels, and select joinlinks. Occasionally, administrators use distribution channels to share original messages, such as musings on IS, commentary on pro-IS content or cybersecurity best practices. The catch-all function of distribution channels contributes to its prominence in the sample. Many distribution channels could be further categorized to determine a main content topic; however, the overall function of distribution channels is to broadcast an array of content for the IS sympathizer.

Across the five categories of channels and groups in the sample, IS sympathizers employ three key tactics to increase the resiliency of the pro-IS community on Telegram. IS sympathizers adopt certain features and practices, creating a unique ecosystem with its own behaviors and norms.

The first observed tactic is the **proliferation of joinlinks**. While there are entire channels dedicated to the distribution of joinlinks, other channels and groups also post joinlinks to keep members abreast of the latest updates within the community. Administrators or users will share joinlinks to consecutive channels or groups, sometimes instructing users to join a page without content and wait for it to become active, to join at a specific time, or to join only after the previous iteration is removed. Additionally, administrators can post time-sensitive joinlinks that deactivate at the whim of the administrator, sometimes in a matter of hours or minutes. Using Telegram's administrator toolkit, administrators can manually change the joinlink or set an automatic expiration time to render the joinlink inaccessible.[10]

Supplementing this qualitative observation with quantitative data, URIScrape captured 17,482 joinlinks shared by channels and groups in the sample. Using Jupyter Notebook and Gephi, researchers ascertained the source and target of each joinlink, as well as how many times each source channel or group shared a link to a specific target channel or group. Using a dummy variable for each target whose Telegram unique identifier did not appear in the sample, the research team categorized each joinlink as "internal" (between a source and target that are both within the sample) or "external" (between a source in the sample and a target outside of the sample). *Figure 9* is a network diagram of all joinlinks captured in the sample. Interestingly, most joinlinks were internal: 10,389 joinlinks (59%) were internal, while the remaining 7,093 joinlinks (41%) were directed towards external channels and groups.[11]



[redacted] 2:35:50 AM

[redacted] Tue 2.1K

assalamualaikum werehmatullah weberekatuh.
join us my brother on Khilafah al islamiyah
https://t.me/joinchat/AAAAA[redacted]
(tg://join?invite=AAAAA[redacted])
International Group chat
will revoked in 1hours

Figure 8. Example of a time-sensitive joinlink to a private group chat.

Joinlink Network

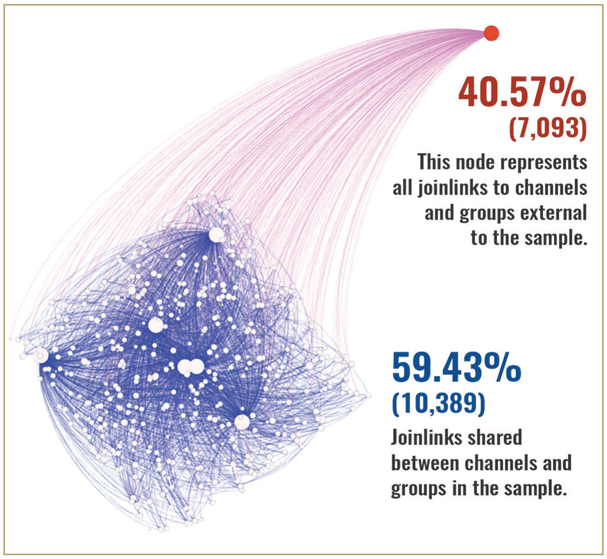
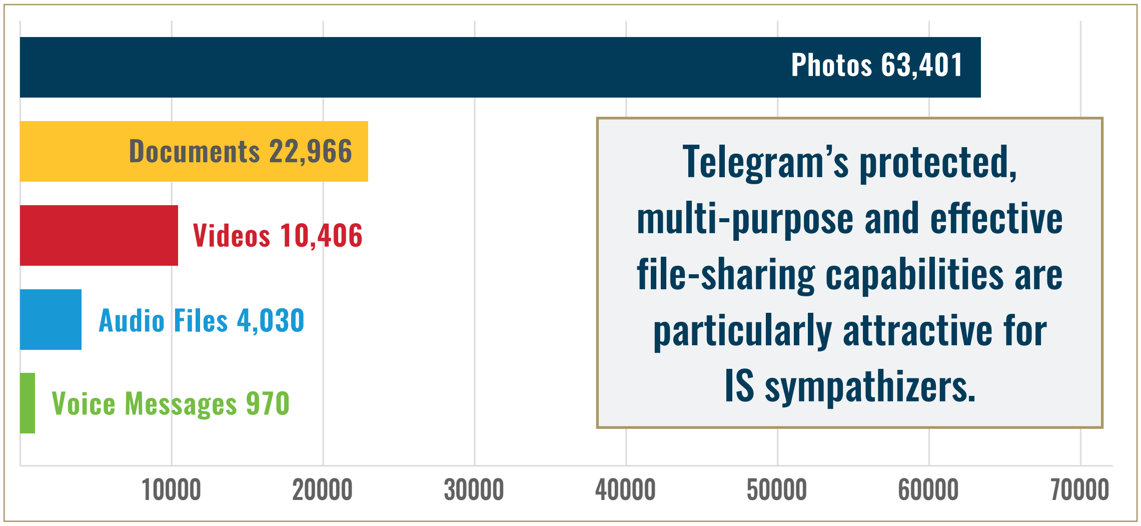


Figure 9. This is a visualization of all 17,482 joinlinks within the sample, created in Gephi. The majority of joinlinks are between channels and groups within the sample, although a substantial percentage direct users towards external Telegram channels and groups.

This network analysis is affected by the snowball sample method utilized for this report. Joinlinks shared in channels and groups represented the main way of finding new channels and groups. However, the result also coincides with known strategies of IS supporters on Telegram and other platforms. To protect against adversaries and shield new public groups and channels from ToS enforcement, administrators prepare multiple variations of channels and groups, instructing members to join them all and wait for them to become active.[12] This is similar in function to a strategy used on Twitter, where suspended IS sympathizers quickly created new accounts and used the "*Baqiya* family" network of

Internal File-Sharing



Telegram's protected, multi-purpose and effective file-sharing capabilities are particularly attractive for IS sympathizers.

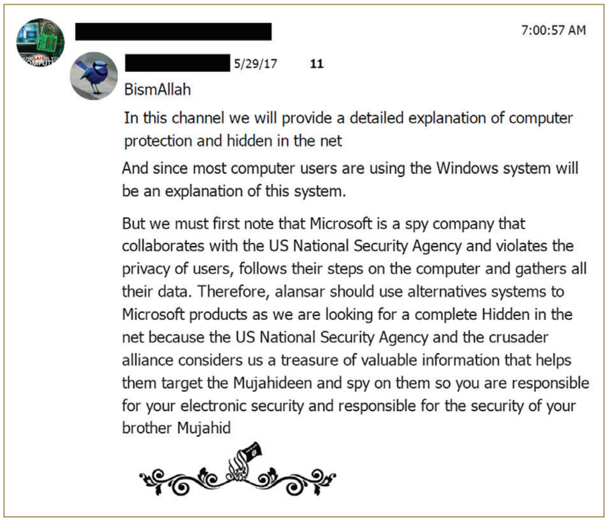
Figure 10. This graph depicts the breakdown of files shared internally within the 636 groups and channels.

"shout-outs" to inform the community of their new account information.[13] These operational resiliency tactics transferred to Telegram, and also partially explain the interconnectedness of the sample.

The second observed key tactic is the use of **internal file-sharing** to distribute a variety of content. At the time of snapshot, users in the sample internally shared a total of 63,401 photos, 22,966 documents, 10,406 videos, 4,030 audio files, and 970 voice messages across the 636 channels and groups. These files range in content, from core IS propaganda to grassroots generated pro-IS memes, from speeches by jihadist ideologues to press releases from IS' adversaries, and from bomb making instructions to VPN tutorials.

Telegram's internal file-sharing capabilities and its tactical employment by IS sympathizers is significant for three primary reasons. First, Telegram's file-sharing size allotment is unparalleled compared to other popular social media and messaging services. Telegram allows users the ability to share large files of up to 1.5GB, approximately one full-length standard definition film.[14] Contrarily, WhatsApp only allows users to share 16MB videos equaling about 90 seconds.[15] Second, Telegram allows users to share multimedia files beyond just photos and videos to include audio files, voice messages, and all document types such as PDFs and Word documents. Twitter, on the other hand, only allows users to share small videos, photos or GIFs.[16] Third, files shared on Telegram benefit from the same protections as chats and posts, meaning they remain accessible unless the entire group or channel is closed or taken down (in the case of public channels). Users in the sample appear to take advantage of this feature and the security afforded by internal file-sharing. Combined together, Telegram's protected, multi-purpose and effective file-sharing capabilities are particularly attractive for IS sympathizers hoping to collect and distribute pro-IS content. This unparalleled suite of file-sharing features allows Telegram to operate as a "clearinghouse" for IS material, acting as itinerant, but persistent, cloud storage for members.[17]

The third observed tactic concerns the adoption of **general cybersecurity practices** when accessing and communicating on Telegram. Across the sample, users employ basic cybersecurity measures to obscure any potentially identifying information. Using Telegram's file-sharing features, IS sympathizers frequently distribute instructions on how to use VPNs, create fake Telegram accounts and phone numbers, and adopt privacy software. Channel and group administrators urge members to employ these tactics to protect themselves from IS' enemies. Whereas on Twitter, some pro-IS users would tweet pictures of themselves or openly share their location,[18] IS sympathizers on Telegram safeguard this information. Within the sample, IS sympathizers tend to use generic profile images, post minimal information on their profiles, and refer to each other only by username or pseudonym (*kunya*). Users are observant of these cybersecurity tactics and weary of anyone who does not follow suit, occasionally calling them out as spies.



[redacted] 7:00:57 AM

[redacted] 5/29/17 11

BismAllah

In this channel we will provide a detailed explanation of computer protection and hidden in the net

And since most computer users are using the Windows system will be an explanation of this system.

But we must first note that Microsoft is a spy company that collaborates with the US National Security Agency and violates the privacy of users, follows their steps on the computer and gathers all their data. Therefore, alansar should use alternatives systems to Microsoft products as we are looking for a complete Hidden in the net because the US National Security Agency and the crusader alliance considers us a treasure of valuable information that helps them target the Mujahideen and spy on them so you are responsible for your electronic security and responsible for the security of your brother Mujahid

Figure 11. This post served as the introduction to a channel dedicated to cybersecurity tactics, followed by detailed instructions on how to use non-Microsoft operating systems.

Notably, Telegram already has inherent cybersecurity measures in place to protect user data. Telegram does not take down individual accounts, or require anything more than a phone number to sign up. Even then, IS sympathizers on Telegram encourage each other to use fake phone numbers, adding another degree of separation. Researchers observed periodic comments from pro-IS users who noted that Telegram is generally unsafe and filled with spies, journalists and other adversaries, giving necessity to protective measures. Regardless of the debatable necessity of cybersecurity and resiliency measures, one could argue that these measures are now inherent within the larger IS online ecosystem.[19] With plenty of time to learn tactics and methods on public facing media, these practices transferred onto Telegram and will continue to evolve.

2. In which ways do English-speaking IS supporters on Telegram balance the need for broad-based messaging and recruitment with the necessity of operational security?

In utilizing digital communications technologies like Telegram, IS supporters must use tools to distribute messaging and propaganda, communicate internally, contact potential recruits, and inject the group's narrative into wide-reaching public debates. Simultaneously, they must also protect these messages and conceal their operations from the watchful eyes of adversaries, namely counterterrorism authorities and other IS opponents. As highlighted in the background section, these two objectives are generally at odds with one another, and require IS' supporters to strike a delicate balance. Understanding this dilemma between mass messaging and operational security can help reveal key vulnerabilities in IS' use of Telegram and other digital communications technologies.

A simple metric for examining how English-speaking IS supporters on Telegram navigate this dynamic is through the privacy feature. Unsurprisingly, the majority of the sample (70%) is comprised of private groups and channels, only accessible through joinlinks. Telegram's private setting is the simplest form of its security offerings, protecting content through client-server/server-client encryption. Private groups and channels are inaccessible from search functions and insulated from the general conversation on Telegram. However, using private groups and channels alone would close off pro-IS content to a predetermined number of recruits, preventing the possibility of a potential recruit accessing channels and groups. As a result, a substantial minority (30%) of all groups and channels in the sample are public. They can be accessed through searches within Telegram, and do not require a joinlink.

In a breakdown that disaggregates channels, groups, and supergroups by their privacy settings, as shown in *Figure 12*, private channels represent a decisive majority

Privacy Settings

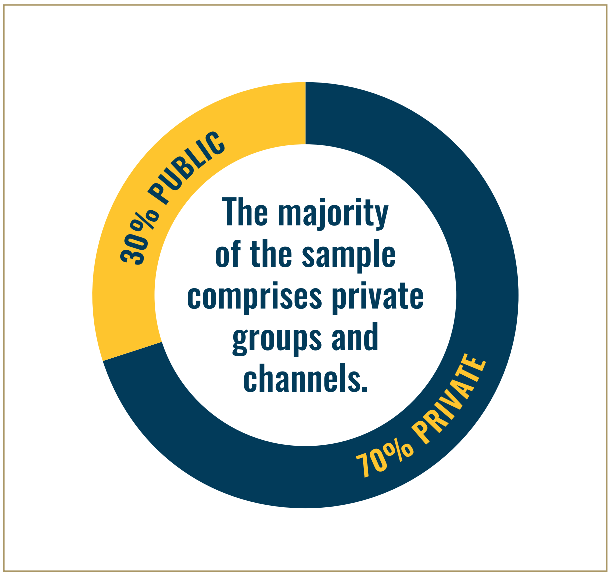


Figure 12. This chart depicts the privacy settings of the 636 groups, supergroups, and channels in the sample.

Channels, Groups, and Supergroups by Privacy Setting

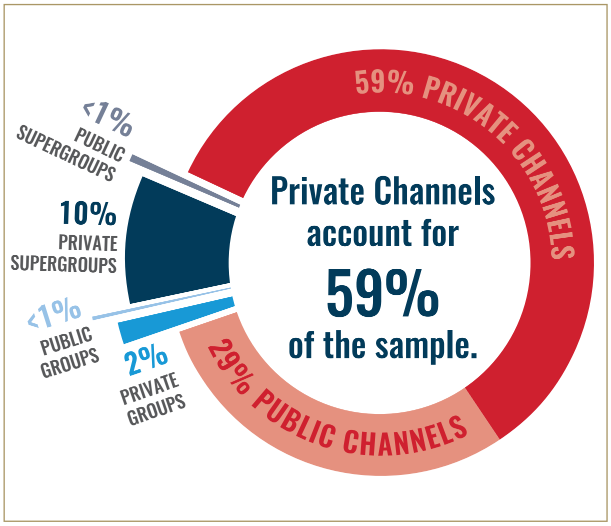


Figure 13. This chart depicts the breakdown of the privacy setting and message type of each of the 636 entries in the sample.

at 59% of the sample. The combination of privacy and channel features explained above illustrate the assessed motivations for using this message stream. Public channels are the second most popular messaging stream, representing 29% of the sample. These public channels are accessible through search functions, though still relegated to Telegram and separate from other public search engines. Public channels are also accessible from URLs, which can be shared and copied freely, with the only barrier to entry being a prompt to login. These public channels often served as key nodes in the network and systematically shared joinlinks to access private groups and channels.

Collection captured only three public supergroups and groups, comprising a negligible percentage of the sample. While public supergroups and groups are still insulated from the general internet and provide ample administrator privileges, they appear to be an unpopular tool with the sample. This is likely due to the perceived operational security vulnerability. Supergroups and groups are designed to facilitate conversation and interaction, which IS supporters would logically prefer to do within a private environment.

Interestingly, Telegram treats private channels, private groups, and public groups equally when it comes to enforcing its ToS. Telegram's policy states that "all Telegram chats and group chats are private amongst their participants," and its current approach precludes takedowns of private channels. In addition, Telegram does not process any requests related to groups, even those concerning illegal content.[20] Therefore, under Telegram's current approach to ToS enforcement, only public channels, which represent 29% of the collected sample, would be eligible for takedowns.

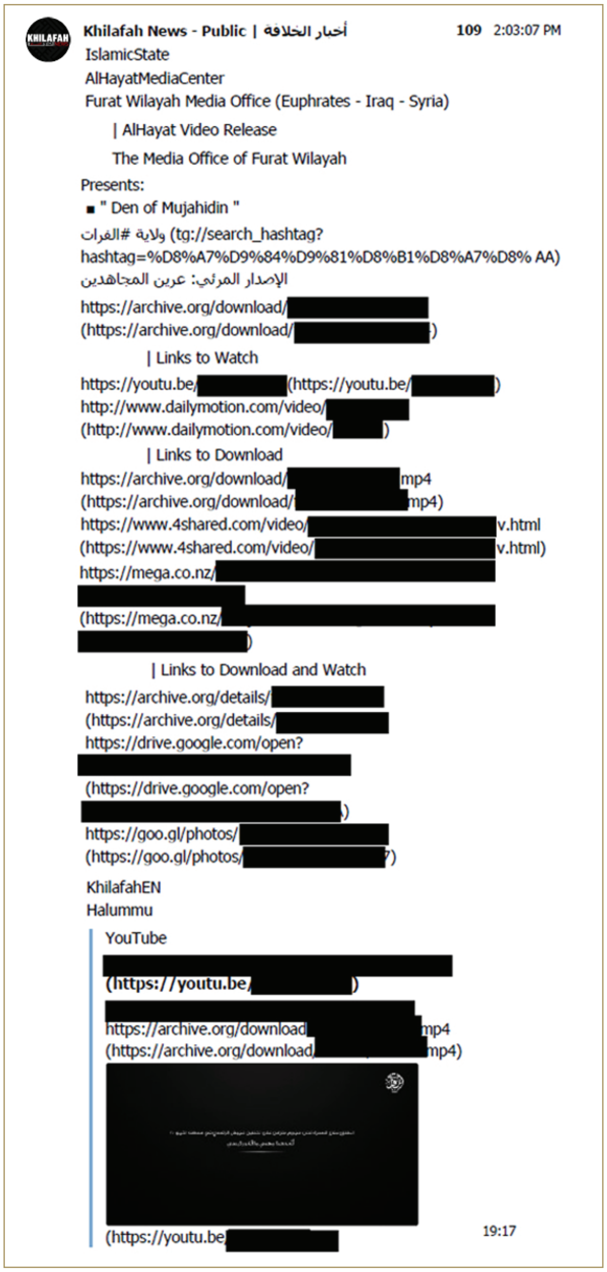
Telegram's reluctance to take down private content helps demonstrate why English-speaking IS supporters are attracted to the platform, and provides context to their fundamental desire for operational security. On public-facing social media, where this demographic's content, accounts, and networks are removed at an increasingly quick rate and can also be shared with third parties, supporters expect limited freedom of movement and potential repercussions for sharing terrorist content. The breakdown of public and private content within the sample shows that English-speaking IS supporters are, at the very least, concerned about operational security and make some attempts to conceal their activities.

At the same time, however, this demographic of IS supporters also lead frequent engagements to ensure that their narrative reaches a wider audience. Two pertinent examples are external file-sharing and distributing URL links to major social media platforms. These are major aspects of IS' online strategy of *ghazawat*, wherein supporters coordinate outreach and attempt to retain access to public-facing social media in the face of ToS enforcement. These efforts demonstrate that English-speaking IS supporters desire to communicate with a wider audience, despite their relative seclusion on Telegram.

While using Telegram's file-sharing features to disseminate content internally, IS sympathizers on Telegram use external file-sharing sites to ensure IS content remains on the internet and resilient to takedowns. Using channels and groups, they distribute dozens of unique URLs to a single piece of pro-IS material on different file-sharing sites external to Telegram. This ensures that if content is removed from one site, stable access exists to others. The resultant URLs can then be copied onto Twitter, Facebook, and other mainstream social media platforms.

To examine English-speaking IS supporters' external engagements, researchers analyzed 46,579 URLs leading to destinations outside of Telegram. URIscrape resolved URLs to their base domain and categorized them by website type. In total, the sample includes 731 unique base domains. The top 20 base domains by frequency are displayed in *Figure 15.* These results show a clear preference for file-sharing sites, which represent 15 of the top 20 most frequent base domains within the sample and 55% of the total URL count.

Using Telegram as a node for distribution, this demographic of IS supporters attempts to exploit a wide range of different file-sharing sites. Within the 46,579 URLs in the sample, IS supporters generated 27,161 links to 130 unique file-sharing platforms. *Figure 16* shows a breakdown of URLs by base domain type, wherein a majority of URLs shared in the sample were towards file-sharing platforms. These data demonstrate a key link in the chain of distribution of media releases from Telegram to public-facing platforms. When online *munasireen* distribute a major media release, such as a new video, photo series, or claim of responsibility for an



Khilafah News - Public | أخبار الخلافة 109 2:03:07 PM
IslamicState
AlHayatMediaCenter
Furat Wilayah Media Office (Euphrates - Iraq - Syria)
| AlHayat Video Release
The Media Office of Furat Wilayah
Presents:
■ " Den of Mujahidin "
ولاية #الفرات (tg://search_hashtag?
hashtag=%D8%A7%D9%84%D9%81%D8%B1%D8%A7%D8% AA)
الإصدار المرئي: عرين المجاهدين
https://archive.org/download/[redacted]
(https://archive.org/download/[redacted])
| Links to Watch
https://youtu.be/[redacted](https://youtu.be/[redacted])
http://www.dailymotion.com/video/[redacted]
(http://www.dailymotion.com/video/[redacted])
| Links to Download
https://archive.org/download/[redacted]mp4
(https://archive.org/download/[redacted]mp4)
https://www.4shared.com/video/[redacted]v.html
(https://www.4shared.com/video/[redacted]v.html)
https://mega.co.nz/[redacted]
(https://mega.co.nz/[redacted])
| Links to Download and Watch
https://archive.org/details/[redacted]
(https://archive.org/details/[redacted]
https://drive.google.com/open?
[redacted]
(https://drive.google.com/open?
[redacted])
https://goo.gl/photos/[redacted]
(https://goo.gl/photos/[redacted]7)
KhilafahEN
Halummu
YouTube
[redacted]
(https://youtu.be/[redacted])
[redacted]
https://archive.org/download[redacted]mp4
(https://archive.org/download[redacted]mp4)
(https://youtu.be[redacted]
19:17

Figure 14. Example of an Al Hayat video shared via numerous URLs to external file-sharing sites for streaming and downloading.

Top 20 Base Domains

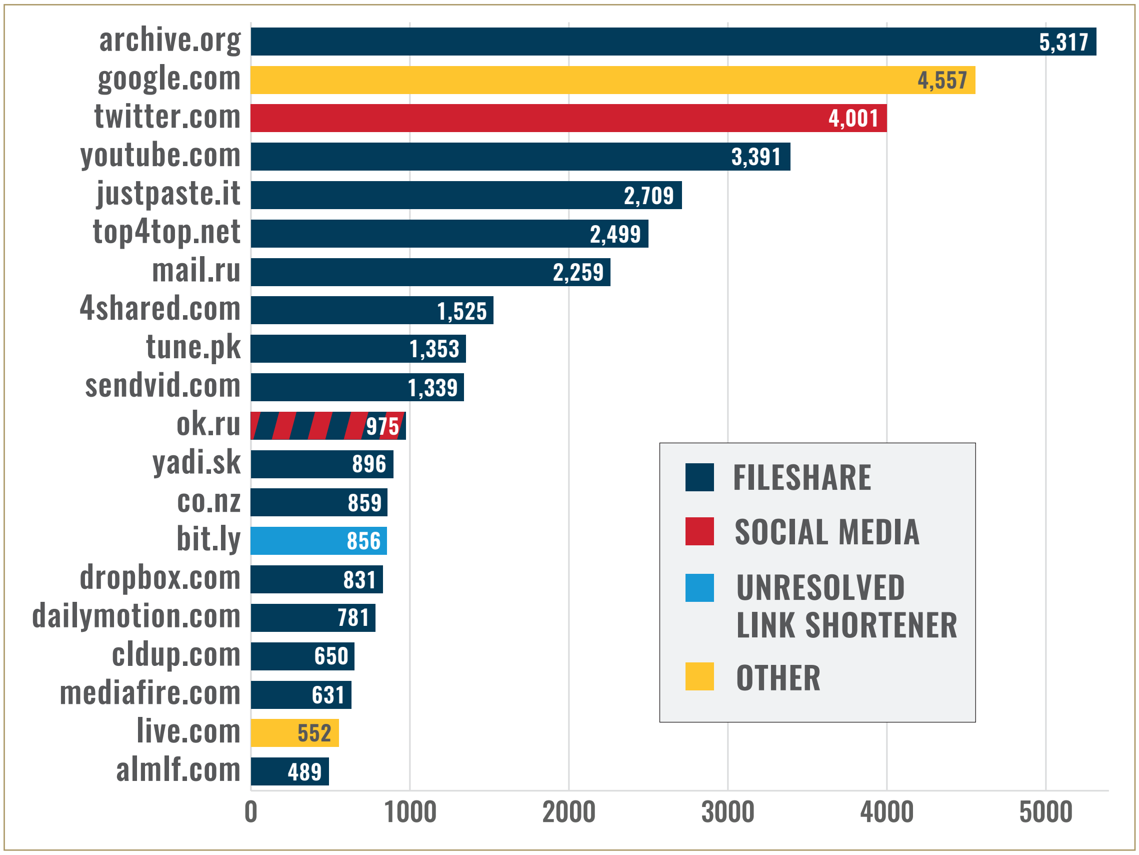


Figure 15. This chart shows the top 20 base domains of external URLs by order of frequency in the sample.

attack, they immediately share external links on Telegram to a variety of file-sharing sites.[21] Using their arsenal of generated URLs, they re-post content from the file-sharing sites to public-facing social media platforms *ad infinitum*.[22] In this fashion, if one platform removes the content, it remains accessible on several others. Additionally, some of the file-sharing sites that were most frequently used may not have the resources, expertise, or interest to adequately monitor and moderate terrorist content.

Three of the four most frequently used general file-sharing domains (archive.org, justpaste.it and top4top.net) are pertinent examples. Despite their small size, these three platforms account for 42% of all file-sharing links and 22% of all external URLs in the study. Archive.org is the home of the Internet Archive, which includes a non-profit, multimedia file hosting platform and the Wayback Machine, which allows users to access archived versions of websites saved over time.[23] Justpaste.it is a free-to-use, non-profit hosting platform initially managed by a Polish graduate student, that supports video, photo, and text content.[24] Top4top.net is another small content hosting site that is popular in the Middle East.[25] Unlike their larger competitors, smaller platforms face additional barriers to removing pro-IS content on their platforms, and stringent enforcement of ToS may not be feasible given the resources at their disposal.[26]

Besides file-sharing, the category of base domains that was most frequently linked to was social media platforms, showing IS supporters' continued insistence in exploiting mainstream social media. Twitter, the former nexus of English-speaking IS online activity, remains a popular destination for external links from Telegram. Sampled channels and groups shared 3,933 unique URLs

Domains by Category

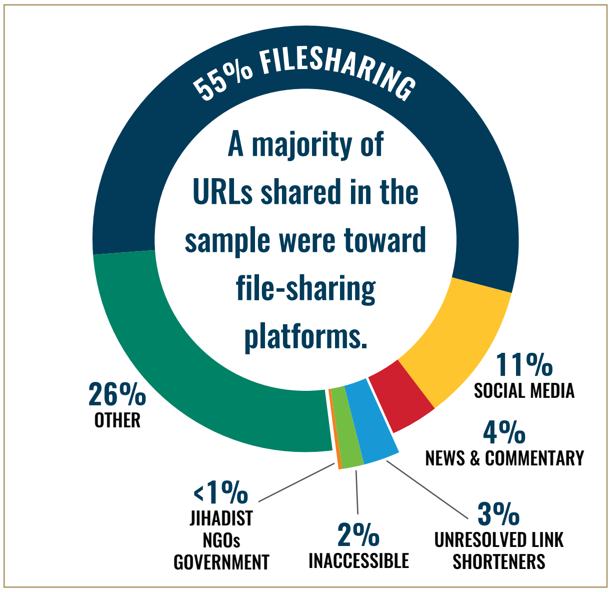


Figure 16. This graph categorizes base-level domains based on website type and shows the share of each category in the total external URL count.

with a Twitter base domain. The second most-linked social media platform was the Russian social network service *Odnoklassniki,* although this platform also allows content hosting. Interestingly, despite its popularity in the West, the sampled channels and groups only shared 146 links to Facebook base domains, making it the 37th-ranked base domain overall.

The ubiquity of external file-sharing and efforts to engage on major social media demonstrates that despite moving to Telegram, English-speaking IS supporters continue to rely on public-facing platforms to disseminate their message to a wider audience. Despite what initially appears to be a predominant concern with operational security, a closer look reveals that this reliance on reaching a wider audience can, at times, override or even conflict with the necessity to implement operational security protocols. For instance, a substantial percentage of supporters in the sample created public channels, even though they are indexed on Telegram, subject to takedown, not end-to-end encrypted, and observable to an unknown number of adversaries. In external file-sharing and posting on social media, supporters potentially release information that could provide a link between their Telegram account and their presence elsewhere online, such as an IP address. These interplays clearly demonstrate the difficulty that many English-speaking IS supporters face in using Telegram for both mass messaging and operational security functions, and the opportunity for counterterrorism authorities to exploit vulnerabilities.

3. How do English-speaking Islamic State supporters on Telegram react to pressure against the organization in the online and offiine spaces?

During the period of data collection for this study, IS faced overwhelming pressure in both its physical territory and the online realm. The sample coincides with IS' key military defeats, including the conclusions of months-long sieges of the towns of Raqqa and Mosul, which displaced IS from major bases of operations in Syria and Iraq. Meanwhile, major social media providers and technology companies engaged in extensive campaigns to remove pro-IS users and content from their platforms.

This study's findings suggest two notable responses by English-speaking IS supporters in the wake of online and offline pressure. First, in times of duress for IS, this demographic of supporters more frequently engages with content that highlights the group's military activities, as well as the efforts of its worldwide affiliates. Sympathizers discuss these topics more often than news, events, or IS-claimed attacks in the West, or IS' non-military activities (governance, infrastructure, economy, etc.). Second, evidence suggests a decentralization of IS media command and control due to ongoing pressure, resulting in three growing strategic themes in English-speaking IS supporters' activities on Telegram: the rise of grassroots actors, the proliferation of "gray" media, and the distribution of operational and instructional material.

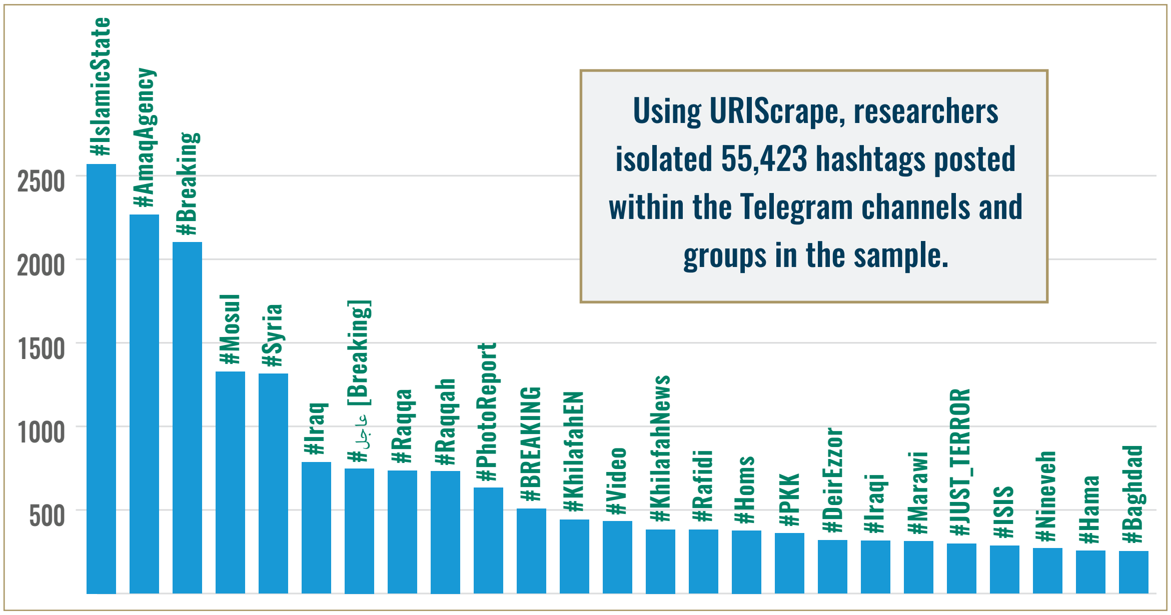
Two queries of this study's data establish the content shift towards military activities. First, researchers conducted basic analysis of IS' supporters' reactions to current events using a binary variable to note the presence or absence of six popular topics. Of these topics, the most frequent were discussions about IS' military activities in Syria or Iraq, which took place in approximately

60% of channels and groups within the sample, and the activities of IS' affiliates, which occurred in 44%. Between the most frequent topics and the four remaining topics, there is a significant drop in frequency. For instance, 16% discussed news and events in Europe or North America, 13% discussed cybersecurity or information security, and 11% discussed IS' non-military activities in Syria or Iraq. Notably, from these six variables, the least-frequent topic concerned IS attacks in Europe or North America, which was discussed in less than 11% of all channels and groups.

Secondly, using URIScrape, researchers isolated 55,423 hashtags posted within the Telegram channels and groups in the sample. While hashtags are not as ubiquitous on Telegram as on other social media platforms, they are consistently used by IS sympathizers, particularly when trying to disseminate news and rally the conversation around specific topics. The top 25 hashtags used throughout the sample are included in *Figure 17*. In general, the main hashtags used by this demographic of supporters during this timeframe include the names of key news agencies and media releases (#AmaqAgency, #KhilafahNews, #Rumiyah), locations of battles involving IS and its affiliates (#Mosul, #Raqqa, #Homs, #DeirEzzor, #Marawi), and markers for IS' adversaries (#PKK, #Rafidi,[27] #Iraqi).

Notably, supporting other analyses of IS hashtag campaigns on social media, no hashtags in the top 25 directly reference IS-inspired terrorist attacks in the West, despite the sample's focus on English-language channels and groups. During the period of collection, IS was involved in critical military campaigns in Iraq, Syria, and elsewhere. In July 2017, as data collection formally began, the siege of Mosul concluded; months later, IS was forced out of its *de facto* capital city in Raqqa.[28] Other key battles, such as IS-affiliated forces' takeover and subsequent defense of the town of Marawi in the Philippines (May–October 2017) also register as top hashtags.[29] The use of hashtags generally correlates with IS official media releases, which during this period generally focused on the group's military campaigns, battles, and defenses of its strongholds. They serve as markers for content that can later be re-posted on other social media platforms,

Top 25 Hashtags



Using URIScrape, researchers isolated 55,423 hashtags posted within the Telegram channels and groups in the sample.

Figure 17. This figure shows the top 25 hashtags within the sample by frequency.

especially on Twitter, while packaging IS media products for other audiences.[30]

While no single terrorist attack outside IS-held territory generated enough sustained conversation to register as a most-used hashtag by name, one hashtag, #JUST_TERROR, is a harbinger for IS supporters' campaigns to promote claims of responsibility for major attacks and incite further violence outside of Syria and Iraq.[31] #JUST_TERROR is one of the top 25 most-used hashtags, but to further understand when and why it was used, a time-series analysis is necessary. *Figure 18* is a chart showing the five weeks in which #JUST_TERROR was the most-used hashtag during 68 weeks of data collection for the sample, alongside the event that resulted in the proliferation of the hashtag during that week.

The five weeks in which #JUST_TERROR was the most-used hashtag contain significant media campaigns by IS supporters to take credit for major attacks outside IS-held territory. However, only two of these weeks coincided with attacks in the West. During the week of July 14, 2017, IS supporters promoted a shooting on the Temple Mount in Jerusalem using the #JUST_TERROR hashtag.[32] Throughout the week of August 25th, 2017, IS Telegram channels and groups pushed claims of responsibility, calls for further attacks, and unofficial media products following two truck-ramming attacks in Barcelona and Cambrils, Spain on August 17, 2018.[33] Three weeks later, *munasireen* launched another campaign using the hashtag after a botched bombing by an IS supporter at the Parsons Green Underground station in London.[34] Two other

Weeks with #JUST_TERROR as Top Hashtag

Week	*Event*	*IS Claim*
July 14, 2017	Three gunmen shoot at Israel Border Police officers near the Temple Mount in Jerusalem, killing two police officers. The resulting firefight kills all three attackers.	IS claims responsibility through Amaq News Agency.
August 25, 2017	Several members of a terrorist cell conduct vehicular and bladed weapon attacks in Barcelona and Cambrils, killing 16. Police killed four of the five perpetrators at the site of the second attack, and the fifth after a manhunt.	IS claims responsibility through Amaq News Agency.
September 15, 2017	An improvised explosive device detonates on a train at Parsons Green Underground station in London, causing no deaths and over 30 injuries. The perpetrator is arrested a day later.	IS claims responsibility through Amaq News Agency.
December 1, 2017	On November 24, 2017, 40 gunmen stormed the al-Rawda mosque in Egypt's North Sinai Governorate, killing over 300 people.	No group formally claims responsibility; reporting assesses IS Sinai Province to be responsible for the attack.
March 30, 2018	An attacker in Southern France hijacks a car and opens fire on police officers before driving to a supermarket, shooting several civilians, and taking hostages. Police storm the supermarket and kill the attacker. Including the attacker, five are killed and 15 wounded.	IS claims responsibility through Amaq News Agency.

Figure 18. Weeks with #JUST_TERROR as the top hashtag and the coinciding event.

attacks— the November 2017 attack on a Sufi mosque in al-Rawda, Egypt,[35] and a shooting that led to a standoff with hostages in Trèbes in March 2018[36]—also resulted in #JUST_TERROR becoming the most-used hashtag during the week of the attack.

Overall, however, #JUST_TERROR and other hashtag campaigns to refer to IS attacks in the West do not generally sustain frequency beyond one week, and metrics relating to this sample demonstrate a sustained engagement with IS' military campaigns in Syria and Iraq through Amaq News Agency updates and geographic hashtag markers relating to Syrian and Iraqi cities. These findings parallel other studies on IS online media from both the supply-side and demand-side perspective. Daniel Milton and Charlie Winter independently found that as IS lost territory in Syria and Iraq, it released more content pertaining to military activity and cut back on depictions of governance, commerce, and religious affairs.[37] Examining a similar demographic to this study, Audrey Alexander also found that terrorist attacks in the West failed to sustain discussion among English-speaking IS supporters on Twitter, despite the makeup of the demographic.[38] In combination with the results of this study, these findings suggest that IS' military activities in Syria and Iraq are a much stronger determinant of the content of discussions by English-speaking IS supporters on Telegram than other topics, especially events in Western Europe and North America.

While English-speaking IS supporters have always fluctuated between strict adherence to IS central media's guidelines and agendas and determining their own course, the weakening of IS' centralized institutions due to military and digital pressure arguably prompted a decentralization in command and control over its media. Leaving aside debates about the quantity or quality of IS' official media productions, IS' English-speaking supporters are increasingly emboldened to become producers of media rather than consumers in response to pressure on the group. Within the study, researchers observed three notable themes in how this demographic responds to online and offline pressure against IS media. First, individual users take action to ensure the resiliency of online networks and exert authority. They build personalities behind usernames, avatars, and *kunyas,* establish media brands, connect with users around the world, distribute pro-IS propaganda, share cybersecurity best practices, and attempt to recruit and mobilize new members using Telegram. By creating name and brand recognition, individual supporters on Telegram become sought-after commodities and take up the mantle of promoting the IS cause in the digital space. With the decline of IS official institutions in Syria and Iraq and the evolution of internal disputes within the group, these individuals are empowered to take an active role in leading networks and producing pro-IS material online.

Second, "gray media" outlets with vague IS connections produce extremist content that is in line with IS' ideological goals and occasionally in direct support of IS. These outlets include media groups with questionable affiliations to IS, as well as grassroots media labels ostensibly run by individuals.[39] Both create propaganda stylized in the IS image but branded as third-party content. Enabled by Telegram's internal file-sharing capabilities and external links to file-sharing sites, Telegram hosts a spectrum of unofficial content which is difficult to precisely categorize. The spectrum of "gray media" includes singular images marked by rudimentary editing, translations of official core content, and products by branded media groups.[40] This content often replicates or modifies core content, superimposing different imagery or adding commentary.

Finally, operational and instructional materials distributed through Telegram contain pertinent examples of how online, grassroots IS supporters respond to a lack of official guidance. To account for the dearth of available, officially-produced English instructional material, administrators of pro-IS channels and groups often re-appropriate English-language instructional material from non-IS sources, create it themselves, or both. Administrators of pro-IS Telegram channels and groups dedicated to the dissemination of core media, propaganda, and ideological products often enforce guidelines that ensure that all posters maintain strict allegiance to IS.[41] In the operational/instructional space, however, administrators seem to assume that their audiences are generally less discerning in the distinctions between various strands of jihadist material. This is reflected in the diversity of media posted within pro-IS Telegram channels dedicated to instructional material.

Aspects of these themes were present within IS media before the uptick in pressure against the organization on the public-facing web and IS' territorial downfall. But recent online and offline developments intensified the relevancy of these trends in studying the activities of IS' sympathizers in the virtual realm. Namely, as IS transitions from a territory-holding organization, it will be critically important to understand how online *munasireen* react to the collapse of the Caliphate and new strategic directions from IS leadership.

CASE STUDIES

While quantitative and qualitative data are vital aspects of studying IS content on Telegram, individual case studies provide concrete examples of how English-speaking IS sympathizers utilize the platform for a variety of functions. During the data collection period, three individuals were arrested in relation to their pro-IS efforts on Telegram whose activity was also observed in the sample: Karen Aizha Hamidon, Ashraf Al Safoo, and Husnain Rashid. Pairing open-source research on these cases with original data from Telegram provides a unique window to what goes on behind the screen of an English-speaking IS supporter.

Notably, each case embodies one of the three key themes observed during data collection on Telegram: the rise of grassroots actors (Hamidon), the proliferation of gray IS media (Al Safoo), and the distribution of operational and instructional material on Telegram (Rashid). The three profiled IS supporters used different tactics pursuant to their specific goals and aims, shedding light on the variety of ways Telegram can be used in the IS online ecosystem. Overall, the cases serve as examples of how IS' English-speaking *munasireen* exploit Telegram's suite of features, balance outreach and operational security, and react to ongoing pressure against the organization.

Karen Aizha Hamidon: Grassroots Actors in the English-Speaking IS Online Ecosystem

On October 11, 2017, authorities in the Philippines arrested Karen Aizha Hamidon on 14 counts of inciting to rebellion or insurrection for her online activity in support of IS.[1] Hamidon, a 36-year old resident of Taguig City, Philippines, reportedly recruited individuals to join and fight with IS affiliates.[2] Hamidon is the widow of Mohammad Jaafar Maguid, the leader of the IS-affiliated jihadist group Ansar Al-Khilafah Philippines and a suspect in the 2016 Davao bombing.[3]

Though Hamidon's case received scant coverage in Western news sources, her actions on Telegram are emblematic of the many ways IS sympathizers can leverage digital communications to become semi-authoritative figures in the pro-IS online ecosystem. By building her own persona on Telegram, Hamidon mobilized individuals in several countries, including the United States, India, the Philippines, and Singapore, and inserted herself within a transnational network of IS supporters. She became known by name as a facilitator and directed new members to her network. An analysis of connected court cases in India and the U.S. shed light on her online operations, as well as key vulnerabilities in English-speaking pro-IS networks on Telegram.

India's National Investigation Agency (NIA) found that Hamidon worked as an IS online network facilitator, directing and welcoming new members to pro-IS groups on several platforms.[4] In one pertinent example from February 2015, Hamidon added an Indian man named Mohamed Naser to her "Islam Q&A" WhatsApp group where, "subsequently, the accused started doing graphic designing work on the instructions of Karen [Hamidon]." By April 2015, Hamidon added Naser to three of her pro-IS groups on Telegram, where he attained information

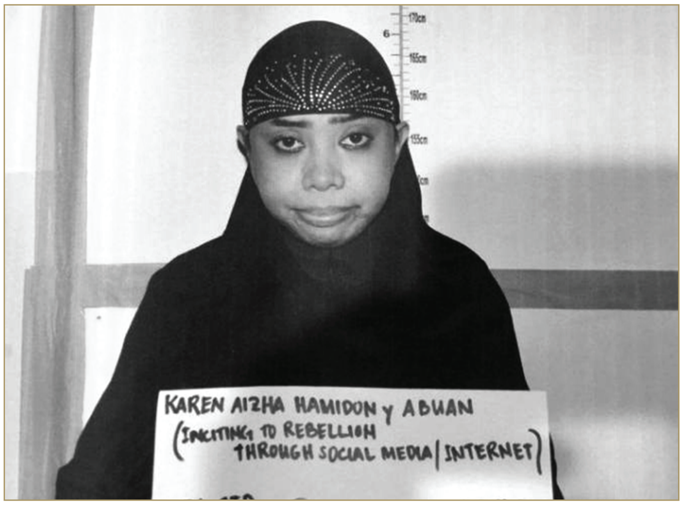


Figure 19. Karen Hamidon upon arrest in the Philippines. (Source: Newsweek)

on traveling to Syria to join IS.[5] During Naser's failed attempt to travel to IS-controlled territory via Sudan in 2016, he was arrested with a piece of paper containing the phone numbers for members of Hamidon's "Islam Q&A" WhatsApp group, indicating the perceived operational viability of this network.[6]

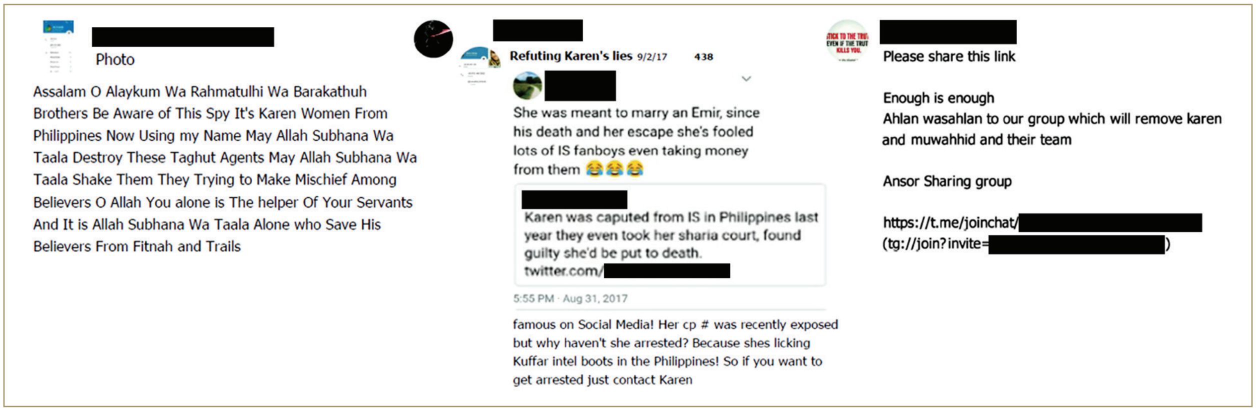
The subsequent NIA investigation into Naser and Hamidon's online presence led to the indictment of 17 members of a cell of IS operatives trying to establish a Caliphate in India under the name *Jund al-Khilafa al-Hind*.[7] The cell was directed by Shafi Armar (Yusuf al-Hindi), an Indian national who joined IS in Syria and reportedly died on the battlefield in March 2019.[8] In Hamidon's extended Indian network, she served as an integral facilitator, using Telegram to propagate IS ideology, recruit others into IS, and facilitate and raise funds for the travel of recruits to Syria.[9] NIA documents claim that network members "in connivance with Karen... were involved in propagating ideology of the ISIS by sharing and circulating text messages, images, videos and making telephonic calls to Indian youths inciting them for recruitment of the ISIS."[10]

Though Hamidon's contacts primarily resided in South and Southeast Asia, some evidence suggests that her online network extended into the United States.[11] On December 30, 2017, the Federal Bureau of Investigation arrested Virginia resident Sean Duncan after he destroyed evidence during an authorized search of his residence pursuant to an international terrorism investigation. According to court documents, FBI agents interviewed Hamidon on July 25, 2017, while she was in the custody of a foreign government. In the interview, Hamidon claimed that Duncan was "one of" her U.S. based contacts.[12] Hamidon and Duncan first made contact on social media in January 2015, then moved to "encrypted mobile messaging applications."[13] Together, they talked about support for IS, traveling to join IS, attacks, homemade bombs, and the prospect of marriage. Their contact dwindled after Hamidon rejected Duncan's proposal of marriage and *hijrah* to join IS in Syria in March 2015.[14]

Interestingly, this is not the only time Hamidon toyed with the idea of marriage to a new contact. Hamidon reportedly had unofficial, online marriage agreements with at least three pro-IS contacts.[15] Hamidon's use of marriage as a recruitment tactic likely contributed to the confusion around her relationship with Singaporean Muhammad Shamin Mohamed Sidek, who was arrested in August 2015 on IS-related charges in Singapore.[16] Reports claimed the two were married, but the Singapore Ministry of Home Affairs dispelled this inaccuracy.[17]

However, Hamidon's assumed online authority, networking style, and personal idiosyncrasies created tensions. A document from the NIA investigation recounts a dispute between Hamidon and another member of her network, Mohammed Sirajuddin, on Telegram, apparently over Hamidon's willful disclosure of users' personal telephone numbers.[18] This is the first spark of dissent against Hamidon's haphazard approach towards operational security. To rally opposition Sirajuddin started a Telegram group dedicated to spreading negative information on Hamidon. In this group, Sirajuddin speculated that Hamidon was involved in the disappearance of Abu Hatim "Mad Mullah," a prominent online facilitator of foreign fighter travel believed to be operating from Sudan. In retaliation, Hamidon removed Sirajuddin from her Telegram groups.[19]

This tactic is frequently observed in groups within this study's sample, as members attempt to remove "spies." During data collection, researchers observed several Telegram-based campaigns against Hamidon, which peaked in intensity before her arrest in the Philippines in October 2017. In several Telegram groups, users shared Hamidon's usernames, profiles, Telegram IDs, and phone numbers with warnings against contacting Hamidon. Users also asked other members to delete Hamidon's contact information and asked group administrators to remove her. Posts against Hamidon were frequently forwarded from groups with names like "Exposing Karen's Lies" or "Karen Watch." Longer posts accuse Hamidon of involvement in the arrests of Mohammed Sirajuddin and Musa Cerantonio, a prominent Australian IS supporter, and allege that she is a government spy. Users lambasted Hamidon for her braggadocio, shameless demands for money from men, and penchant for confrontation, and



[redacted]
Photo

Assalam O Alaykum Wa Rahmatulhi Wa Barakathuh Brothers Be Aware of This Spy It's Karen Women From Philippines Now Using my Name May Allah Subhana Wa Taala Destroy These Taghut Agents May Allah Subhana Wa Taala Shake Them They Trying to Make Mischief Among Believers O Allah You alone is The helper Of Your Servants And It is Allah Subhana Wa Taala Alone who Save His Believers From Fitnah and Trails

[redacted]
Refuting Karen's lies 9/2/17 438

[redacted]
She was meant to marry an Emir, since his death and her escape she's fooled lots of IS fanboys even taking money from them 😂😂😂

[redacted]
Karen was caputed from IS in Philippines last year they even took her sharia court, found guilty she'd be put to death.
twitter.com/[redacted]

5:55 PM · Aug 31, 2017

famous on Social Media! Her cp # was recently exposed but why haven't she arrested? Because shes licking Kuffar intel boots in the Philippines! So if you want to get arrested just contact Karen

[redacted]
Please share this link

Enough is enough
Ahlan wasahlan to our group which will remove karen and muwahhid and their team

Ansor Sharing group

https://t.me/joinchat/[redacted]
(tg://join?invite=[redacted])

Figure 20. Messages captured in the sample posting against Karen.

claimed that if she was telling the truth about her connections to IS, she would have already been arrested.

Through forwarded messages from other users, the Telegram data also captures Hamidon's attempts to defend herself. Hamidon sent private messages to users, defending her allegiances and claiming a network of connections to IS affiliates in the Philippines. Hamidon claimed she had run-ins with the Filipino justice system but avoided sentencing through luck and good lawyers. When her outreach failed, Hamidon infiltrated groups by creating fake online identities with similar usernames to her accusers to "ruin their reputations." Some users appeared to take her side and asked group administrators to remove those "slandering" Hamidon. These users, however, appeared to be in the minority of the sample.

Shortly before her arrest, users speculated Hamidon's whereabouts and shared images of identification cards including her Postal Identity Card and Tupperware Brand Saleswoman ID card. When Hamidon was arrested on October 7, 2017, those who accused her of being a spy celebrated the arrest as a victory for the Islamic State.

Hamidon's case exemplifies the English-speaking pro-IS ecosystem's reliance both on mutual trust and individual diligence. During data collection, researchers often observed users accusing each other of being spies. These frequently appeared as one-off instances where the "spy" would be removed, or the administrators would ignore the accusations. Telegram's security measures prevent users from knowing who controlled accounts behind the screen.[20] While users directed campaigns against "spy" accounts, removed "spies" could create new accounts or change their username, update their profile information and continue using Telegram. These observations support existing research which notes trending suspicion, hesitancy, and cybersecurity practices within IS activity online.[21] Hamidon, however, inspired a movement across channels and groups, intent on removing her and all her accounts from the entire ecosystem. Users drew direct lines between her numerous Telegram accounts and her real-world identity, freely sharing her personally identifiable information.

The case of Karen Hamidon provides an invaluable window into the ecology of English speaking IS sympathizers on Telegram. Hamidon's extended network spans over 25+ countries, demonstrating how the decentralized structure of IS sympathizers on Telegram allows individuals to quickly become part of a larger, online movement. Though Hamidon's exact role remains unconfirmed, her actions illustrate the value of network facilitators online. While based in the Philippines, Hamidon was able to create international networks, insert herself in conversations, and wage campaigns against users. Her actions potentially included facilitating the travel of IS supporters to Syria and the Philippines, raising funds to facilitate travel, directing propaganda creation, and convening users in support of IS primarily using Telegram. Additionally, she demonstrated a command of Telegram and used its security features to her advantage when challenged: creating fake profiles to endorse her side of the story, making copies of her enemies' profiles to sabotage their reputations, and removing users with whom she disagreed from her groups and channels.

Hamidon's case also supports the idea that the functions of digital communications technologies, like anonymity and profile duplication, can reduce obstacles to women's activism in terrorist groups which traditionally do not support female leadership.[22] Though Hamidon faced scrutiny for disobeying gender norms within the IS community on Telegram, she exploited Telegram's suite of features to remain an authoritative figure.

To date, Hamidon's exact role as both a source to authorities and an IS supporter is unclear. On one hand, she is a common thread between numerous successful arrests. Her tactics, such as demanding money and keeping contact lists, could indicate a desire to gather information for authorities. On the other hand, she deliberately connected IS supporters. Her cooperation with authorities and willingness to provide information may have been an act of self-preservation. In both situations, her case presents an example of the potential value and opportunity of sowing discord in pro-IS communities on Telegram. The inability to prove who operates a Telegram account, while frequently a disadvantage for investigations, could be a positive feature for counter-IS operations. The delicate balance of trust and suspicion that characterizes the pro-IS ecology on Telegram is ripe for exploitation. The international reach of online networks, coupled with Telegram's provision of backdated data when a user joins a group or channel, provides an opportunity to multiply successful leads. Counterterrorism authorities can take note of these issues highlighted in Hamidon's case for future operations.

Ashraf Al Safoo and Khattab Media Foundation: Gray Media

On October 17, 2018, the FBI arrested Ashraf Al Safoo, a 34-year-old resident of Chicago, Illinois. Al Safoo is charged with one count of conspiracy to provide material support and resources to IS for his actions as part of the Khattab Media Foundation (KMF).[23] Allegedly, Al Safoo "aided ISIS in using social media to spread propaganda supporting violent jihad, to recruit operatives, and to encourage others to carry out terrorist attacks."[24] An FBI undercover employee spearheaded the investigation by posing as an aspiring KMF contributor, communicating with Al Safoo directly, and infiltrating the private KMF Staff and Writers groups on Telegram. Court documents from the Al Safoo case detail the complex, virtual organization behind KMF. Within the data collected for this study, KMF was a notable gray media outlet, producing content that was actively redistributed by English-speaking IS supporters across Telegram.

KMF produced a variety of propaganda products, including "edited video content, articles, essays, and infographics."[25] The videos mentioned in the criminal complaint give insight into how KMF combined elements from official IS propaganda, open-source media, and original content. For instance, on October 19, 2017, KMF released a video titled, "The Brothers in Marawi."[26] The video used footage of IS fighters in the Philippines and an English-language *nasheed* which was released five

Figure 21. Top: Ashraf Al Safoo (Source: Chicago Sun-Times*); Bottom: Khattab Media Foundation logo.*

days earlier by al-Hayat Media Center.[27] Additionally, in December 2017, KMF released a video titled, "Our Gifts Are Ready," which uses a combination of original low-quality animation, mainstream news footage, and IS videos to communicate a Christmastime threat against multiple Western states.[28]

The criminal complaint also details KMF's organizational structure, which consisted of Al Safoo and at least 17 unnamed co-conspirators. On Telegram, KMF operated within two private groups—the "Staff Group" with join-link access and 21 members, and the "Writer's Group," a private group with 13 members.[29] The Writers Group functioned as a forum for KMF's leaders, wherein decisions could be discussed before communication to the more general Staff Group. Structurally, KMF is divided into six divisions: writing, design, production, audio, upload and publishing, each with its own division head. Al Safoo was allegedly promoted to the head of the writers' division in March 2018.[30] Before publication on Telegram and other sites, KMF content passed through the appropriate division, moving through a standard approval process. After the final product was approved, a translation department translated content from Arabic into several languages, including English, French, Bengali, and Italian, often by using online translator applications.[31]

When products were ready for publication, KMF strived to improve their online outreach. Like other IS propagandists, KMF attempted raids on social media, primarily Twitter, to inject their products into the public sphere.[32] KMF members were aware of social media companies' efforts to remove extremist content from their platforms, and thus took steps to circumvent these policies.[33] To maintain a presence on Twitter, KMF members created numerous fake accounts, shared account logins, and hacked the accounts of legitimate social media users. Using TOR and VPN software when operating on public platforms, they employed operational security measures to hide their identities.[34] To execute Twitter raids, members arranged publications, set times for release, gathered accounts, implemented cybersecurity measures, and prepared hashtags. Specific channels were dedicated to sharing the prepackaged raid information, streamlining distribution.[35]

Two KMF tactics highlight how IS sympathizers adapt to ToS enforcement on public-facing social media sites. First, IS sympathizers hack legitimate social media accounts to avoid account suspensions, presenting another challenge for social media companies seeking to de-platform IS sympathizers. One KMF member directly acknowledged this fact, claiming that a hacked account "is better because it stays with you longer," and, "you are better off spending an hour hacking than a minute in create an account."[36] In general, KMF members seemed keenly aware of takedown policies and were intent on staying one step ahead. This assessment supports established concerns with reactive takedown policies and the need for proactive marginalization of extremist actors online.[37]

The second tactic of note is the integration of cybersecurity measures within KMF's operations. The FBI assessed that Al Safoo practiced "sophisticated" cybersecurity measures, by using TOR, VPNs, a pre-paid cash phone, different email addresses, and multiple Telegram accounts.[38] Al Safoo's cybersecurity skills likely stemmed from his 10-year career in IT and master's degree in computer science.[39] Despite his unique professional experience, Al Safoo is not the only IS sympathizer with an interest in cybersecurity techniques. Across Telegram, researchers observed a prevalence of cybersecurity information concerning VPNs, TOR, creating multiple accounts, and basic skills. The integration and proliferation of cybersecurity practices by IS-sympathizers on Telegram is a reality that law enforcement, policymakers, and social media companies must consider when trying to combat terrorist content online.

The day-to-day operations of KMF also reveal a great deal about the positionality of ostensibly "unofficial" pro-IS media outlets vis-a-vis the group's central apparatus. Three incidents detailed in the criminal complaint illustrate KMF's connection to the IS central media department. On November 30, 2017, a member posted a set of rules in the Staff group for disseminating information. These rules gave KMF the freedom to create original content while conforming to the most basic level of strategic messaging from IS core. Four months later, Al Safoo allegedly re-posted a message to the Staff group with a reminder to "Adhere to the official media," which "knows when to publish or avoid publishing; which means not every news is good for publishing."[40]

In another telling interaction, KMF members mobilized in response to direct instructions from IS central media following the mass shooting in Las Vegas on October 1, 2017. Amaq News Agency released a claim of responsibility for the attack the next day, despite the absence of evidence connecting the perpetrator to IS.[41] On October 2, 2017, the same day of Amaq News Agency's official claim, a KMF member posted in the Staff Group relaying a message that the attack was conducted by a "soldier of the caliphate," and another member called to "launch an interactive campaign along with the blessed operation."[42] A day later, KMF released an infographic mentioning the attack.[43] This release occurred in accordance with one of the rules set by IS central media for unofficial groups: "Commitment to the official [ISIS] announcement stipulating that it's not allowed to claim responsibility for any operation or attack which hasn't been announced by the State, may Allah glorify it."[44]

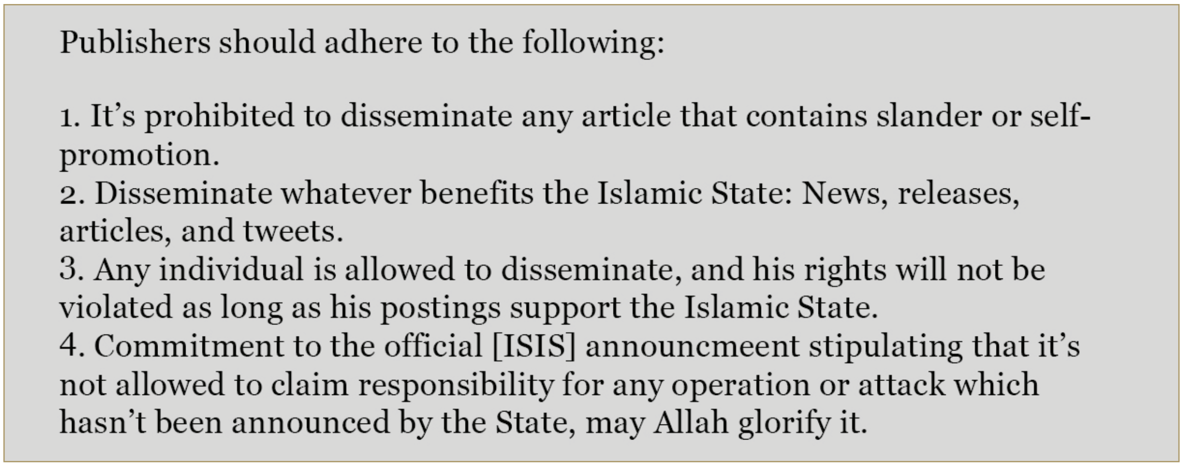
The clearest indication of a nexus between IS' central media department and KMF concerns a merger between KMF and al-Wafa Media Foundation, another gray pro-IS media group. KMF leadership in the Writers Group discussed a merger with al-Wafa, but ultimately abandoned the move "in accordance with the State's instructions."[45] In messages to the Staff Group, KMF leadership asked members to leave the al-Wafa groups, noting it was a well-intended mistake to begin a merger.

This chain of information depicts a hierarchical structure with IS core dictating major decisions from the top, the Writers Group discussing and debating them, then delegating down to the Staff Group.[46]

While further studies are necessary to determine how KMF interacted with IS' central media apparatus, this evidence documents that KMF consulted the core media operatives on major decisions, including sourcing, important media operations, and its relationships to other pro-IS media groups. KMF was encouraged to produce propaganda independently within a broad set of guidelines and obtained course corrections from IS core when necessary. In this manner, KMF provides a compelling example of strategic media decentralization embraced by IS core as it loses territory. Strategies that intend to counter IS media should understand and address the reality of gray media organizations within the IS propaganda machine.

Husnain Rashid and "Lone Mujahid": Operational and Instructional Material

On November 22, 2017, authorities in the United Kingdom arrested 31-year-old Husnain Rashid at his home in Nelson, Lancashire.[47] He was charged with terrorism-related offenses, prompted by his threats on Telegram against the school of Prince George and other targets in the UK.[48]



Publishers should adhere to the following:

1. It's prohibited to disseminate any article that contains slander or self-promotion.
2. Disseminate whatever benefits the Islamic State: News, releases, articles, and tweets.
3. Any individual is allowed to disseminate, and his rights will not be violated as long as his postings support the Islamic State.
4. Commitment to the official [ISIS] announcmeent stipulating that it's not allowed to claim responsibility for any operation or attack which hasn't been announced by the State, may Allah glorify it.

Figure 22. Rules posted to the KMF Staff Group by co-conspirator #17.

By the time of his arrest, Rashid administered channels inciting IS-inspired attacks in European cities for at least two years under a common brand. His private channels, named "Lone Mujahid," "LM," or other derivations, were notorious for spreading English-language operational instructions to would-be attackers.[49] The Lone Mujahid channels included step-by-step instructions for a successful jihadist plot in a Western country, from attack methods and means to locations for attack and operational security measures. While the threat against Prince George likely resulted in Rashid's arrest and conviction, his Telegram channels also contained a multitude of other incitements, alongside a deep library of jihadist instructional material.

This report's sample contains 25 channels with the "Lone Mujahid" brand. The earliest example was created in March 2017 and the latest weeks before Rashid's arrest in October 2017. Like other channel brands dedicated to distributing instructional or operational material, administrators of "Lone Mujahid" forums utilized a common method for disseminating information across the various channels and encouraging their followers to safeguard the material.

First, Lone Mujahid's administrators developed several ways of inoculating the material they posted from takedowns, while ensuring that followers retained constant access to the information. Many of the Lone Mujahid channels start with a brief warning to subscribers, in the information section of the channel or as the first post. "This channel will more than likely be deleted by them smelly dirty kuffs [*kuffar*]," the channel advises, "so make sure you save all the posts you (sic) ASAP."[50] Indeed, many of the early examples of Lone Mujahid channels within the dataset were public channels, making them available to a larger range of supporters but also making the channel itself vulnerable to takedowns. To sidestep regulation, Lone Mujahid's administrators stored all base content for the channels on a backup "master channel." Administrators rarely shared joinlinks to this private master channel, ensuring that it would not be deleted or reported. When a new Lone Mujahid channel was created, administrators simply shared all the material stored on the master channel to the new channel.

Figure 23. Husnain Rashid undated photograph. (Source: Reuters)

The "master channel" method not only benefited Lone Mujahid's administrators but also followers of the channel interested in consistent access to the channel's repository of operational guides. Using the suite of services available on Telegram, IS supporters could retain the channel's posts in two separate ways—either by downloading the individual PDFs, documents, videos, and photos, or by forwarding the content in the channel to their own personal accounts, which automatically backs up the posts to Telegram's cloud feature.[51] By utilizing either of these features, supporters can access and view information posted in Lone Mujahid channels even after the channel was suspended or deleted by administrators.[52]

Additionally, Lone Mujahid channel administrators compiled an extensive amount of supplemental instructional material, including PDF links and video files showing how to follow specific instructions within particular manuals. Much of the seed content for Lone Mujahid channels was instructional material contained in "The Book of Terror," a multi-part volume compiled by Abu Kitaab al-Ingaltarra which first appeared on the internet in 2015.[53] The book includes chapters detailing the religious justifications for jihadist attacks in the West, instructions for different types of attacks (explosives, knife attacks, truck-rammings, etc.), combat training, operational security, and finally, how to make *hijrah* by traveling to IS-held territory.[54]

Lone Mujahid channels also included other compilations, including "Resources for the Mujahid: The Art of War Collection," which contained operational instructions alongside histories of the military strategies used in the early Islamic period and more modern treatises on war and insurgency (the table of contents includes works by Niccolo Machiavelli, Sun Tzu, Carlos Marighella, Mao Zedong, and Che Guevara). Moreover, like other channels, it re-appropriated instructional material produced by other jihadist groups, especially by re-posting full copies of *Inspire*'s "Open Source Jihad" series. Finally, Lone Mujahid devised its own "operational playbooks," detailing the planning and execution of several notorious IS-inspired attackers, including Mohamed Lahouaiej-Bouhlel, responsible for a deadly 2016 truck-ramming attack in Nice, France, and Omar Mateen, the 2016 Orlando Pulse Nightclub shooter. It released operational playbooks in the "Knights of Lone Jihad" series, which encouraged individual supporters to carry out attacks in their home countries on behalf of IS using the models of previous successful attacks.

Finally, Lone Mujahid's administrators reacted to current events, updating information within the channel as new attack opportunities or methods arose. During the run-up to the 2017 Wimbledon Championships and the UEFA Women's Euro 2017, the channel posted a full layout of the Wimbledon championship grounds and the arena where the UK national women's football team was scheduled for a match. "I luuurve tennis, don't you?" the post accompanying the Wimbledon arena map read, followed by the hashtags #JustTerror, #Wimbledon, and lastly, echoing the 2017 Manchester arena bombings, #Copycat_ManchesterArena.[55]

Following an attack on Israeli policemen at the Temple Mount in Jerusalem in July 2017, Lone Mujahid channels began inciting violence against synagogues and kosher restaurants in the United Kingdom. "Indeed these apes have barred the muslims [sic] from praying salat al Jum'ah [Friday prayers] at Masjidul Aqsa [al-Aqsa Mosque]," one post argues, "therefore prevent the Apes from attending their places of disbelief."[56] Continued incitements and updated operational playbooks on the LM channels emerged in the late summer and early fall of 2017, especially following the October 2017 mass shooting in Las Vegas, for which Amaq News Agency erroneously claimed IS responsibility. More importantly, unofficial outlets dedicated to operational material cited the shooting in playbooks, highlighting the gunman's process and planning as an example for would-be jihadist attackers.

During the late fall of 2017, Lone Mujahid channels distributed propaganda threatening attacks on the upcoming 2018 World Cup in Russia, a prominent terrorism researcher in the UK, and British supermarkets. In conjunction with a trend in instructional material posted on other channels, Lone Mujahid distributed instructions related to the production of ricin, cyanide, and other poisons during the fall of 2017. Using these poisons, the administrators called for supporters to poison produce and other food products in grocery stores on behalf of IS.

The now-infamous post threatening Prince George appeared on a Lone Mujahid channel for the first time in October 2017. "Even the royal family will not be left alone, school starts early," Rashid posted, alongside pictures released by Kensington Palace of the young prince walking to school with his father.[57] Weeks later, police arrested Rashid, and in December 2017, a UK court charged him with seven terrorism-related counts, including encouraging terrorism, preparation of terrorist attacks, and dissemination of terrorist publications.[58] After the legal process, in which prosecutors used evidence from the Lone Mujahid Telegram channels to argue that Rashid created an "e-toolkit for terrorism,"[59] Rashid pleaded guilty in May 2018. A court later sentenced him to a term of 25 years to life in prison.[60]

While Husnain Rashid was eventually apprehended and brought to justice, the Lone Mujahid channels remain instructive in how IS supporters may choose to use Telegram to distribute instructional material in the future. Evidence from after Rashid's sentencing potentially highlights the impact of the "Lone Mujahid" model. A BBC Monitoring report from July 2018 tracked a new iteration of the Lone Mujahid channel which appeared after Rashid's sentencing, using Rashid's mugshot as a profile picture.[61] This raises the possibility that the Lone Mujahid channels were either coordinated by a number of separate administrators like other unofficial IS media brands on Telegram, or that IS supporters were copying

Rashid's methods.[62] In either case, the model used by Rashid to distribute instructional material on Telegram may have important ramifications for how supporters in the future attempt to disseminate operational guides to the benefit of IS-inspired attack planners in the West.

Ultimately, Telegram provides a conducive environment for individual personalities and channel "brands" to flourish as pro-IS grassroots actors. Inconsistently balancing cybersecurity protections with public accessibility, IS sympathizers use Telegram's suite of features to communicate with like-minded supporters across the world, disseminate IS' official and unofficial media, and provide instructional material for operations. With this assessment in mind, it is important to explore the implications of IS sympathizers' continued use of Telegram and options for counterterrorism policymakers and practitioners to combat terrorist exploitation of the platform.

CRITICAL CONSIDERATIONS: MARGINALIZING IS SUPPORTERS ON TELEGRAM

Addressing the challenges posed by IS supporters' use of digital communications technologies is a critical area of responsibility for counterterrorism authorities worldwide. In these efforts, it is highly important for policy to reflect the landscape of IS supporters' exploitation of the digital toolbox, and formulate strategies that limit the dexterity and influence of violent extremists online. While this study examines a small demographic on a specific but important platform, the findings from the study's overarching research questions contribute to broader assessments about how IS supporters utilize a wide range of tools to achieve strategic aims.

The following considerations for policymakers, practitioners, and technology companies strive to integrate the findings of this report into a strategic architecture to confront violent extremists online. After defining the current parameters of the problem set, these considerations are designed to influence policies that marginalize the impact of IS supporters in the online space.

Among the study's demographic, a short-term, large-scale shift away from Telegram or to another digital communications platform is unlikely.

This report found that English-speaking IS supporters tend to prefer Telegram because it offers several invaluable features, including expanded file-sharing services and groups of up to 200,000 members. These, among other features, are vital for IS sympathizers' online communication and distribution of media products. In addition, Telegram is relatively user-friendly; creating an account only requires a working phone number, and all that is needed to access pro-IS content is either a search for public groups and channels or a single joinlink. Telegram also offers basic security, including by restricting access to channels and groups to users with valid joinlinks, providing relative anonymity, offering encryption features, and guaranteeing that information shared on private groups and channels will not be disclosed to third parties.

Yet, if complete operational security was an overriding goal, English-speaking IS supporters would have already shifted towards other digital communications tools with better security affordances. Cryptologists frequently pillory Telegram's security, some arguing that "the safest way to use Telegram would be not to."[1] Across the duration of this report's dataset, members of pro-IS Telegram channels and groups would periodically comment that Telegram was unsafe, filled with spies, and lacked the ability to reach the public. But almost three years after this demographic's exodus from Twitter to Telegram, no other platforms appear to have developed the same balance of features, user-friendliness, and basic security that could warrant a new switch.

IS media outlets continuously attempt to influence a shift away from Telegram towards other platforms. During this report's data collection, outlets like Nashir News Agency and Amaq News Agency urged followers to diversify from Telegram, either by exploiting new, upstart social media and file-sharing platforms or attempting to move towards more technologically sophisticated or secure options. As an example of the former, in the summer of 2017, IS supporters created several accounts on the social media feed aggregator Baaz.[2] Baaz is a small U.S. company which, despite limited resources, quickly responded to the exploitation of its platform.[3] Although Nashir News Agency and Amaq News Agency attempted to develop a network of Baaz accounts, the platform has not gained traction amongst English-speaking IS supporters.[4]

Concerns persist about IS supporters exploiting other online instant messengers, particularly with more advanced security protocols. In December 2018, after a reported increase in Telegram's enforcement of ToS, Amaq News Agency and Nashir News Agency promoted Rocket.Chat, another online messenger.[5] Nashir

News Agency exhorted its followers to join Rocket.Chat, claiming that it would begin to publish news releases on Rocket.Chat before Telegram, and distributed an instructional guide detailing how to use the service.[6] Around December 2018, several researchers of IS online activity argued that IS supporters have also made multiple attempts to build an infrastructure on decentralized web platforms like ZeroNet and Riot, which distribute access to data across its participants rather than storing it in a centralized location.[7]

An unknown number of intervening variables over the medium and long-term make predictions nearly impossible. Yet, as it stands today, there is little evidence to suggest that a massive shift of IS supporters from Telegram to elsewhere, on the scale of the departure from public-facing social media in 2015-2017, is currently underway. While Telegram has made notable changes to its ToS enforcement and executed some notable takedowns of IS content, its mixed signals and opacity weaken its signal to supporters that the service is no longer a safe haven for them. Without another application that outmatches Telegram's blend of public outreach, file-sharing, user-friendliness, and security features, it is reasonable to forecast that in the short-term, many English-language IS supporters will remain on the platform.

The principle of marginalization should undergird efforts to counter IS supporters online, including on Telegram.

Currently, the implicit intent of efforts to counter terrorist exploitation of digital communications technologies is to completely eliminate terrorists' accounts and content online through takedowns, namely through account suspensions and content removal. This approach heavily mirrors offline counterterrorism efforts such as leadership decapitation and kinetic clearing operations. But in this case, the online and offline realms are not analogous. Online supporters of terrorist groups are highly dexterous, moving between platforms and constantly recreating accounts while uploading content at a higher pace than it can be theoretically taken down.[8] Unlike taking a leader of a terrorist group off the battlefield through an arrest or targeted killing, takedowns do not prevent extremist actors from continuing support online.[9]

Nevertheless, the takedown-centric approach to online terrorist content is popular in several Western countries, with a variety of governments attempting to respond to radicalization and terrorist attacks by calling in turn for digital service providers to take a harder line on terrorist content. In Germany, the *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (also referred to as NetzDG or the Facebook Law) fines companies that fail to take down objectionable content within an allotted time period up to €50 million.[10] In the United Kingdom, policymakers constantly threaten social media providers with boycotts, advertising bans, and fines, over claims that the companies are "not doing enough" to counter the spread of extremist propaganda on their platforms.[11]

This approach is logical when technology companies have an incentive and interest in complying with government requests or risk economic disincentives when they fail to remove terrorist content from their platforms. For these reasons, this type of government pressure is especially unlikely to work with Telegram. Telegram's distributed data infrastructure allows it to dodge subpoenas, it displays little interest in cooperating with governments on data requests, and it has no shareholders or advertisers for governments to leverage. Even in the case where government pressure on Telegram is successful, all it would accomplish is forcing extremists to find new platforms to disseminate media and communicate, replicating what some have termed the "whack-a-mole" problem.[12]

The marginalization paradigm represents one conceptual alternative to takedown-centric online counterterrorism policy. As argued originally by Audrey Alexander and William Braniff, marginalization of online extremism would involve "a swathe of empowered actors," who "[help] to depreciate the influence of violent extremists by progressively undermining, drowning out, and sidelining radical perspectives."[13] Marginalization-driven policies differ from the current approach in two ways. First, rather than aiming for the untenable goal of taking down 100% of terrorist content on any platform, marginalization seeks to contain extremist actors within platforms where it is both 1) difficult for extremist ideas to reach the public, and 2) possible for law enforcement to detect, monitor, and investigate extremist activity on the platform.[14]

Applying the marginalization paradigm entails strategic recommendations for the wide array of actors who are currently involved in online counterterrorism and helps clarify roles and responsibilities between them. The competing objectives of law enforcement, intelligence, the military, researchers, journalists, and technology companies in the online space impedes coordination when actors fail to realize how their own policies could potentially conflict with the efforts of others, or accidentally empower the voices of violent extremists online.[15] For instance, social media providers have an incentive to remove content from their platforms, but their policies may cause an unintended migration to another platform with fewer resources. As another example, journalists and researchers occasionally rebroadcast unofficial IS media, but erroneously cite it as signs of an imminent threat or a declaration on behalf of the groups' official media apparatus.[16]

A marginalization-based online counterterrorism strategy proportionally responds to the actual capabilities and credibility of violent extremists, rather than immediately and preemptively responding to a hypothetical ability that they could develop. Media and public hype about the strength and frequency of extremist content online can accidentally amplify extremist propaganda and narratives by rebroadcasting them into public discourse.[17] In contrast, marginalization-focused policies aim to cordon off extremists into low-visibility online spaces and limit their reach to public-facing mass media, while taking the opportunity to monitor their actions and behavior.

Compared to public-facing social media and file-sharing platforms, IS supporters are marginalized on Telegram.

English-speaking IS supporters' reliance on Telegram sidelines many of their viewpoints from reaching the public. The arguments made by IS official media distributors in the early days of Telegram usage—that it was effective only for secure communications and internal media distribution, but not for *da'wa*, radicalization or recruitment— appear to have borne out.[18] While it is still relatively easy to access pro-IS content on Telegram, even for a new user, the hurdles in place to ensure communication security also weed out potential recruits. More importantly, they nearly eliminate the risk that an uninitiated individual would "stumble across" IS' online media.[19]

Governments and service providers should shape their responses to IS' use of Telegram based on the marginalization paradigm: *Do the benefits that extremists gain from using Telegram outweigh their losses from not being able to exploit other digital communications services?* Reliance on Telegram stunted English-speaking IS supporters efforts to develop a foothold on more secure or more publicly-accessible platforms, and lured supporters into a false sense of operational security. These downsides outweigh the strategic benefits of Telegram for IS supporters. Consequently, efforts by governments and service providers should focus on containing, monitoring, surveilling and investigating English-speaking IS supporters on Telegram, rather than pressuring the company to de-platform IS supporters.

In accordance with the first principle of marginalization, Telegram is one step removed from access to mainstream media, limiting the public reach of IS *munasireen*. When English-speaking IS supporters were highly active on platforms like Twitter and Facebook, the possibility that IS narratives or media releases would penetrate public discourse and directly interact with the public was higher. Supporters' attempts to repost content from Telegram to mainstream, public-facing social media and file-sharing platforms are charitably described as an uphill battle.[20] Sympathizers can create repositories of content on Telegram, but since joinlinks are necessary to access most channels and groups, the number of people who will view the content on Telegram is inherently limited. Even public channels are restricted to users already on Telegram, with prior knowledge of key words to effectively search for IS content.

Fulfilling the second principle of the marginalization paradigm, IS supporters' dependence on Telegram benefits counterterrorism authorities. There are opportunities for law enforcement to detect, monitor, and investigate extremist activity on Telegram, as evidenced by the arrests of Karen Hamidon, Ashraf Al Safoo, and Husnain Rashid. The "going dark" problem does engender important challenges for law enforcement as they attempt to investigate the activities of malicious and criminal actors, including terrorists.[21] As a digital communications service, Telegram includes a suite of features, some that exacerbate the "going dark" problem and some that do not. Telegram's channels and groups, the subject of this report, notably lack many of the security options that other features on Telegram boast.

More broadly, the cybersecurity protocols that sympathizers employ are often rendered ineffective by substandard operational security. IS supporters face a conundrum in the use of online messaging tools like Telegram—employing iron-clad security measures can isolate online networks from adding potential new members. IS' reliance on public outreach for new recruits can result in online breaches by the organization's adversaries. Taking this risk, many pro-IS Telegram administrators open their groups and channels, and sometimes even direct communications to unknown and unverified accounts. This vulnerability is ripe for exploitation by law enforcement, allowing an entryway for investigators to breach the network, garner evidence of criminal activity and in some cases, arrest and prosecute supporters.

In engagement with Telegram, governments should encourage Telegram to participate in industry-driven forums for counterterrorism collaboration.

To date, government responses to terrorist exploitation of Telegram have been largely disincentive-based. Threatening to levy fines, bans, or other punishments towards platforms who fail to moderate terrorist content can theoretically be effective in pressuring companies into taking tougher stances, provided that the company would avoid economic or legal issues by complying. Telegram, as a multinational, data-distributed, shareholder-free entity, would not be affected by many of the disincentives that governments attempt to apply to social media providers. A potential alternative is for governments to encourage Telegram to participate in industry-led mechanisms for cooperation between technology companies.

This is not to say that governments should completely abandon disincentives in cases of non-compliance by Telegram, but that a prerequisite to applying targeted disincentives is encouraging Telegram to come to the table. Though Telegram may still refuse to directly respond to government requests for data, governments can encourage the service provider to employ best practices developed through industry-led, not government-mandated, forums.

While they are still developing, several forums for technology industry collaboration on countering terrorist propaganda online emerged during the past few years. Chief among them is the Global Internet Forum to Counter Terrorism (GIFCT), a forum established in 2017 by Facebook, Twitter, Google, and Microsoft.[22] Among other initiatives, including collaboration on technological solutions, support and engagement with the research community, and coordination with governments, GIFCT aims to "[share] best practices around counterterrorism...in particular focusing on knowledge sharing with smaller tech companies."[23] In these endeavors, they are supported by Tech Against Terrorism, a program established by the United Nations Counter-Terrorism Executive Directorate (UN-CTED), which holds roundtables and trainings for smaller service providers on addressing terrorist content on their platforms.[24]

To date, Telegram has taken multiple steps to increase public transparency, including by making their API more accessible and available. The August 2018 update of Telegram's privacy policy to include provisions for law enforcement cooperation, combined with the decision to issue a transparency report, should also be commended. A further step that governments could encourage is Telegram's contribution to Tech Against Terrorism's Knowledge Sharing Platform (KSP), which would allow Telegram to share its perspectives with its industry partners.[25] Telegram, as a central node for IS propaganda and activity, could provide valuable insight to other technology companies by sharing their observations of trends.

Telegram's participation in the KSP would also be invaluable for smaller file-sharing services and social media sites. Telegram could alert these service providers when IS supporters are attempting to bandwagon or promote the use of their platforms. Moreover, knowledge-sharing between Telegram and other platforms could improve their collective capacity for effective content moderation, preventing pro-IS content on Telegram from springboarding onto the public-facing web through file-sharing or lesser-known social media platforms.

In turn, Telegram could gain new insight into practices that can benefit their platform, while contributing to other technology companies' bodies of knowledge on terrorist use of digital communications services. Beyond ToS enforcement, Telegram can learn about other critical methods in online counterterrorism, such as transparency reporting, anti-spam tools and crowdsourced or automatic detection of terrorist content. Even absent participation in industry-led forums, Telegram may consider investments in research about terrorist use of Telegram, or bringing in independent reviewers to monitor and assess trends. Ultimately, government encouragement of these developments builds the capacity of technology providers to proportionally respond to terrorist use of the internet.

Heavy-handed approaches—such as weakening or limiting encryption, or banning Telegram—are disproportionate, ineffective and create negative side effects.

Successful terrorist attacks, facilitated using services that offer encrypted messaging, spark responses by numerous governments to weaken or limit encryption protocols, or even ban particular services. Authorities in the United States, United Kingdom, Germany, and other Western democracies have previously called for the installation of backdoors into popular messaging services or weakening the strength of encryption.[26] Meanwhile, other governments have attempted outright bans on the use of particular messaging services that offer encryption. This study's findings demonstrate that adopting either response would not constitute an effective solution to the use of digital communications technologies by IS sympathizers. These approaches represent disproportionate responses to the use of encrypted communications by terrorist groups. Encryption technology is used daily by hundreds of millions of people for legitimate and necessary purposes.[27] It is irresponsible to existentially target encryption due to its use by a small group of malign users.

In an August 2017 article, Aaron Brantly argues that weakening encryption or installing backdoors in messaging applications would entail little to no national security benefit for Western governments.[28] Should the government ban or weaken encryption, the code to produce an encrypted messaging platform is already open-source, and malicious actors could simply create their own platform free from government monitoring.[29] The pressure to install backdoors creates a perception of distrust of law enforcement amongst service providers, inhibiting cooperation between government and technology companies.[30] Brantly argues that weakening encryption could force terrorists onto platforms that complicate surveillance efforts, and that the prudent alternative is to increase the capacity for law enforcement to monitor terrorists on existing platforms.[31] While targeting encryption is an "easy punching bag," the professed cure is worse than the disease: "undermining the digital security of society without improving the capability of security services in a sustained way to detect terrorist activity is a worse than futile exercise."[32]

Complete bans against Telegram are even more disastrous. To date, the governments that banned Telegram are largely authoritarian: two notable examples are Russia and Iran.[33] In 2018, Iran's judiciary and Russia's chief communications authority both declared the service a threat to national security and banned it on the grounds that it was used to facilitate terrorist attacks.[34] Both bans were unmitigated disasters. In Iran, some estimates claimed that over half the population used Telegram daily, and that half of Iran's daily internet bandwidth came from individuals accessing the service. The ban struck major blows to Iran's economy, and ultimately led to circumvention as users installed VPNs and other services to side-step the ban and access Telegram.[35] In Russia, collateral damage from the Telegram ban nearly shut down the Russian internet, after the Russian communications authority mistakenly blocked over 15 million IP addresses on Google and Amazon web-hosting services.[36]

So far, calls for platform bans in Western democracies appear to represent political bluster rather than actual commitment to carrying out a policy. Yet, even the suggestion of targeting encryption has the potential to create a chilling effect that could threaten an already fragile relationship between the government and digital communications service providers. Heeding examples from around the world, the economic, social, and political costs of threatening bans or forced backdoors against messaging platforms far outweigh the debatable national security benefits. Western governments, including the U.S. government, should consider the potential negative effects of such statements and policies before action.

CONCLUSION

The Islamic State's global band of online *munasireen* are at a unique but unstable precipice. The organization's self-proclaimed Caliphate in Syria and Iraq—complete with physical territory, proto-governance capabilities, and an extensive media architecture—is currently in disarray. Across the world, English-speaking IS supporters responded to these tribulations, fighting to stay active on platforms on which they could reach the masses while attempting to fill gaps in officially produced IS propaganda.

This report found that for English-speaking IS *munasireen*, Telegram's suite of features provided ample opportunities to create a host of innovative, multimedia content and distribute it amongst like-minded sympathizers. A distinctive ecosystem of accounts, channels, and groups became the first link connecting IS' central media outlets to worldwide grassroots actors. Using a maddening range of file-sharing services and lesser-known social media platforms, supporters waged an active insurgency against major platforms' ToS enforcement. Moreover, individuals and unofficial entities generated their own media and developed unique personalities. At times, they strategically coordinated content production, following guidance from the official IS structure. Others deviated from this path and concocted homemade content to complement official releases, adding to the repository of propaganda for English-speaking IS supporters.

Telegram's suite of features provided ample opportunities to create a host of innovative, multimedia content and distribute it amongst like-minded IS sympathizers.

These efforts, combined with the use of Telegram's secret chat function by IS-affiliated attack planners and perpetrators, wrought intense focus by scholars, analysts, and journalists. As policymakers and technology companies prepare for the next stage of the fight against IS online, sober assessments of how IS supporters currently use digital communications technologies are of the utmost importance. With regard to Telegram specifically, it is now an understood fact that the platform is preferred by IS sympathizers and that pro-IS content is readily available. However, findings from this report help to dispel some popular misconceptions about how and why English-speaking IS supporters utilize Telegram.

First, while the common assessment is that IS *munasireen* strategically moved to Telegram from mainstream social media sites for impenetrable cybersecurity, further analysis shows that this move balanced a desire for increased cybersecurity with the necessity for public accessibility. Telegram is an online messenger that offers end-to-end encryption in some features. It is not, as commonly claimed, an end-to-end encrypted messaging platform. Nevertheless, IS sympathizers still use Telegram's channels and groups, sometimes with the misconception that it will conceal illegal activity. Telegram's refusals to provide information on individual users to law enforcement and reticence on ToS enforcement are highly attractive to English-speaking IS supporters. Even under Telegram's newly-adopted guidelines, private channels and groups, constituting 70% of this report's sample, are still exempt from enforcement. Thus, regardless of Telegram's security (or lack thereof), IS *munasireen* will likely continue using the service because it is a relatively safe online haven for propaganda and messaging.

Second, despite some barriers to gathering information about the individuals behind accounts, law enforcement agencies in several countries have built successful prosecutions of IS-affiliated individuals and networks using data from Telegram. Turning sympathizers' lack of effective operational security against them, law enforcement can use tried and tested tactics to gain access to Telegram groups and channels, build relationships with sympathizers using undercover accounts or cooperating sources, and demolish trust within online networks. *Munasireen* are forced into a corner due to the success of law enforcement investigations on Telegram. Without resources or wherewithal, they either continue connecting with unverified accounts to build networks or reject all new entrants, denying them the ability to garner support.

Overall, much like IS' precarious position in the physical space, its online supporters face a rapidly changing environment that forces the demographic to be quick thinkers, making agile, strategic decisions as they are allowed or denied access to new services. Governments and technology companies are arguably in the consistent, unenviable position of being one step behind developments in terrorist exploitation of digital communications technologies. Telegram, and the governments which engage with it, should draw key lessons from how IS sympathizers are using the platform in formulating policy responses. They should also draw from the last major exodus of IS *munasireen* when public-facing social media sites employed the aggressive ToS enforcement that forced IS supporters onto services like Telegram.

Today, Telegram appears to be increasing its ToS enforcement and potentially changing its tune on cooperation with law enforcement. It remains unclear whether these developments may cause IS supporters to turn to other online platforms, but it is important to consider that this demographic consistently demonstrates agility in the adoption of new, underexplored platforms during times of pressure. Thus, while attempts to de-platform IS supporters from Telegram may neutralize IS networks on the service, this may come at the expense of the broader fight against IS online, as IS *munasireen* delve deeper into obscure or opaque digital communications platforms.

NOTES

Background

1. "Telegram F.A.Q." n.d. Telegram. Accessed February 1, 2019. https://telegram.org/faq.
2. *Ibid.*
3. *Ibid.*
4. *Ibid.*
5. *Ibid.*
6. No Telegram group or channel is searchable on the public web, only on Telegram.
7. "Telegram F.A.Q."
8. *Ibid.*
9. Fishman, Brian. 2019. "Crossroads: Counter-terrorism and the Internet," *Texas National Security Review*. April 2, 2019. https://tnsr.org/2019/04/crossroads-counter-terrorism-and-the-internet/#_ftnref1.
10. Alkhouri, Laith, and Alex Kassirer. 2016. "Tech for Jihad: Dissecting Jihadists' Digital Toolbox." Flashpoint. https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf.
11. *Ibid.*
12. *Ibid.*
13. Tan, Rebecca. 2017. "Terrorists' Love for Telegram, Explained." Vox. June 30, 2017. https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter.
14. Weimann, Gabriel. 2004. "www.terror.net: How Modern Terrorism Uses the Internet." USIP Special Report, 116. http://www.usip.org/publications/wwwterrornet-how-modern-terrorism-uses-the-internet
15. Weimann, Gabriel. 2010. "Terror on Facebook, Twitter, and Youtube." *The Brown Journal of World Affairs* 16 (2): 45–54; Conway, Maura. 2012. "From Al-Zarqawi to Al-Awlaki: The Emergence and Development of an Online Radical Milieu." CTX: *Combating Terrorism Exchange* 2: 12–22; Weimann, Gabriel. 2014. "New Terrorism and New Media." Wilson Center. http://www.academia.edu/download/36123842/STIP_140501_new_terrorism_F.pdf; Carter, Joseph, Peter Neumann, and Shiraz Maher. 2014. "#Greenbirds: Measuring Importance and Influence in Syrian Foreign Fighter Networks." International Centre for the Study of Radicalisation (ICSR). https://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf; Klausen, Jytte. 2015. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38 (1): 1–22. https://doi.org/10.1080/1057610X.2014.974948.
16. "Terrorists on Telegram." 2017. Counter Extremism Project. https://www.counterextremism.com/sites/default/files/Terrorists%20on%20Telegram_052417.pdf; Malik, Nikita. 2018. "Terror in the Dark: How Terrorists Use Encryption, the Darknet, and Cryptocurrencies." Centre for the Response To Radicalisation and Terrorism, Henry Jackson Society. http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf.
17. Graham, Robert. 2016. "How Terrorists Use Encryption." *CTC Sentinel* 9 (6). https://ctc.usma.edu/how-terrorists-use-encryption.
18. *Ibid.*
19. "Telegram F.A.Q."
20. Clary, Grayson. 2016. "The Flaw in ISIS's Favorite Messaging App." *The Atlantic*, January 4, 2016. https://www.theatlantic.com/technology/archive/2016/01/isiss-favorite-messaging-app-has-a-security-problem/422460; The Grugq. 2015. "Operational Telegram." November 18, 2015. https://medium.com/@thegrugq/operational-telegram-cbbaadb9013a. Cox, Joseph. 2015. "Encryption App Telegram Probably Isn't as Secure for Terrorists as ISIS Thinks." *Motherboard* (blog). November 18, 2015. https://motherboard.vice.com/en_us/article/mg7jq3/encryption-app-telegram-probably-isnt-as-secure-for-terrorists-as-isis-thinks.
21. From the early days of the IS's 2013-2014 reemergence in the Syrian conflict until 2016, Twitter was arguably the premier forum for IS' efforts online. Over time, Twitter's ToS enforcement, in combination with the growing popularity of Telegram, caused a major shift of online supporters of IS from Twitter to Telegram. A 2017 study by the Program on Extremism, which reviewed over 800,000 Tweets by 1,782 unique English-language, pro-IS accounts, found that the IS network on the platform experienced "digital decay" due to a combination of factors including "Twitter suspensions and IS' strategic shift from Twitter to messaging platforms that offer encryption services."See; Berger, J.M., and Jonathan Morgan. 2015. "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter." Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf; Berger, J.M., and Heather Perez. 2016. "The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters." Program on Extremism. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf; Alexander, Audrey. 2017. "Digital Decay? Tracing Change Over Time Among English-Language Islamic

State Sympathizers on Twitter." Program on Extremism. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DigitalDecayFinal_0.pdf.

22. Meleagrou-Hitchens, Alexander, and Seamus Hughes. 2017. "The Threat to the United States from the Islamic State's Virtual Entrepreneurs." *CTC Sentinel* 10 (3). https://ctc.usma.edu/the-threat-to-the-united-states-from-the-islamic-states-virtual-entrepreneurs/; Callimachi, Rukmini. 2017. "Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar." *The New York Times*, February 4, 2017, https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html; Moreng, Bridget. 2016. "ISIS' Virtual Puppeteers." *Foreign Affairs*, September 21, 2016. https://www.foreignaffairs.com/articles/2016-09-21/isis-virtual-puppeteers; Gartenstein-Ross, Daveed, and Madeleine Blackman. 2017. "ISIL's Virtual Planners: A Critical Terrorist Innovation." *War on the Rocks*. January 4, 2017. https://warontherocks.com/2017/01/isils-virtual-planners-a-critical-terrorist-innovation.

23. *Ibid.*

24. *Ibid.*

25. Smith, Laura. 2017. "Messaging App Telegram Centrepiece of IS Social Media Strategy." BBC Monitoring, June 5, 2017. https://www.bbc.com/news/technology-39743252.

26. According to IS, Amaq News Agency is technically not an official IS outlet, but instead an objective news agency (which, by happenstance, has frequent insider access to IS information). This degree of separation helps IS ignore unfactual reporting from Amaq, a useful media tool concerning attack claims. By letting Amaq claim attacks around the world before a connection to IS is discovered, Amaq piggybacks on the attack's media attention regardless of legitimate connection to the attacker, giving IS leadership more time to decide to release an official statement. Core content outlets like Nashir News Agency and Khilafah News also benefit from a degree of separation from IS media leadership, helping insulate traditional official outlets. See; Callimachi, Rukmini. 2016. "A News Agency With Scoops Directly From ISIS, and a Veneer of Objectivity." *The New York Times*. January 14, 2016. https://www.nytimes.com/2016/01/15/world/middleeast/a-news-agency-with-scoops-directly-from-isis-and-a-veneer-of-objectivity.html. Al-Tamimi, Aymenn. 2017. "Amaq News and Claims of Responsibility," (blog). October 2, 2017. http://www.aymennjawad.org/2017/10/amaq-news-and-claims-of-responsibility; Smith, "Messaging App Telegram Centerpiece of IS Social Media Strategy," 2017; Winter, Charlie and Parker, Jade. 2018. "Virtual Caliphate Rebooted: The Islamic State's Evolving Online Strategy." Lawfare. January 7, 2018. https://www.lawfareblog.com/virtual-caliphate-rebooted-islamic-states-evolving-online-strategy.

27. Smith, "Messaging App Telegram Centerpiece of IS Social Media Strategy," 2017.

28. Prucha, Nico. 2016. "IS and the Jihadist Information Highway – Projecting Influence and Religious Identity via Telegram." *Perspectives on Terrorism* 10 (6): 48–58.

29. *Ibid.*

30. *Ibid.*

31. Bindner, Laurence and Raphael Gluck. 2017. "Wilayat Internet: ISIS' Resilience across the Internet and Social Media." *Bellingcat*. September 1, 2017. https://www.bellingcat.com/news/mena/2017/09/01/wilayat-internet-isis-resilience-across-internet-social-media.

32. *Ibid.*

33. *Ibid.*; Lakomy, Miron. 2018. "Picturing the Islamic State's Online Propaganda: Vanishing or Resurfacing from the World Wide Web?" SSRN Scholarly Paper ID 3298932. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3298932.

34. Telegram post, December 9, 2015, referenced in "On Telegram, ISIS Supporters Are Instructed To Return To Twitter." 2015. The Cyber & Jihad Lab, MEMRI (blog). http://cjlab.memri.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/on-telegram-isis-supporters-are-instructed-to-return-to-twitter.

35. Hakim, Danny. 2014. "Once Celebrated in Russia, the Programmer Pavel Durov Chooses Exile." *The New York Times*, December 4, 2014,

36. *Ibid.*

37. *The New York Times*. n.d. "Attacks in Paris." https://www.nytimes.com/news-event/attacks-in-paris.

38. Tan, "Terrorists' Love for Telegram, Explained."; Shehabat, Ahmad, Teodor Mitew, and Yahia Alzoubi. 2017. "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West." *Journal of Strategic Security* 10 (3). https://doi.org/10.5038/1944-0472.10.3.1604; Vidino, Lorenzo, Francesco Marone, and Eva Entenmann. 2017. "Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West." ICCT-Program on Extremism-ISPI Report. https://icct.nl/wp-content/uploads/2017/06/FearThyNeighbor-RadicalizationandJihadistAttacksintheWest.pdf.

39. Warrick, Joby. 2016. "The 'App of Choice' for Jihadists: ISIS Seizes on Internet Tool to Promote Terror." *Washington Post*, December 23, 2016. https://www.washingtonpost.com/world/national-security/the-app-of-choice-for-jihadists-isis-seizes-on-internet-tool-to-promote-terror/2016/12/23/a8c348c0-c861-11e6-85b5-76616a33048d_story.html; Deutsche Welle. 2018. "Germany Searches for IS Member behind Anis Amri's Berlin Truck Attack," July 5, 2018. https://www.dw.com/en/germany-searches-for-is-member-behind-anis-amris-berlin-truck-attack/a-44547830; Yayla, Ahmet.

2017. "The Reina Nightclub Attack and the Islamic State Threat to Turkey." *CTC Sentinel* 10 (3), March 2017. https://ctc.usma.edu/the-reina-nightclub-attack-and-the-islamic-state-threat-to-turkey.

40. *Ibid.*

41. Engel, "One App Maker Has Shut down Almost 80 Channels."

42. *Ibid.*

43. "ISIS Watch." Telegram. https://telegram.me/ISISwatch.

44. *Ibid.*

45. Miller, Christopher. 2018. "Telegram CEO Defends New Privacy Policy, Says User Data Still Safe." RadioFreeEurope/RadioLiberty. August 28, 2018. https://www.rferl.org/a/telegram-ceo-defends-new-privacy-policy-says-user-data-still-safe/29458179.html.

46. "Telegram Privacy Policy." n.d. Telegram, accessed May 10, 2019. https://telegram.org/privacy#8-3-law-enforcement-authorities.

47. *Ibid.*

48. Tucker, Patrick. 2018. "Is Telegram Secure? French Terror Arrest Raises New Questions About Messaging App." *Defense One*. May 18, 2018. https://www.defenseone.com/technology/2018/05/telegram-secure-french-terror-arrest-raises-new-questions-about-messaging-app/148328.

49. "Analysis: Wave of Telegram Suspensions Hits Jihadist Accounts." 2018. *BBC Monitoring*. December 7, 2018. https://monitoring.bbc.co.uk/product/c200h0s4.

50. Bodo, Lorand. 2018. "Decentralised Terrorism: The Next Big Step for the so-Called Islamic State (IS)?" VOX - Pol (blog). December 12, 2018. https://www.voxpol.eu/decentralised-terrorism-the-next-big-step-for-the-so-called-islamic-state-is.

Methodology

1. Telegram's supergroup feature only allows members to see the date that the group was upgraded to a supergroup, not the date of creation of the original group. Researchers treated the date of upgrade as the date of creation for a supergroup.

2. In a few cases where channels or groups had a very large number of posts, scrolling back to the date of creation caused the computer to crash. For example, one group contained over 1,461 pages of PDF captured posts. Rather than lose this relevant data, authors included these channels or groups in the data set on a case by case basis, capturing data up until the crash point.

3. Alexander, "Digital Decay?" 2017.

4. Other languages observed in the collected groups and channels include Arabic, French, Russian, Turkish, Spanish, Bahasa Indonesia, Bahasa Melayu, Tagalog, Urdu, Bengali, Sindhi, Farsi, Pashto, Italian, German, Kazakh, and Tajik.

5. During data collection Telegram made notable advancements that would have benefited data collection, including chat download controls and releasing more information about their API. See; Telegram Team, "Chat Export Tool, Better Notifications and More." 2018. Telegram. August 27, 2018. https://telegram.org/blog/export-and-more

6. In the case of supergroups, which represent 10% of the sample, researchers gained access dating back to the date that administrators upgraded the group to a supergroup.

7. Milton, Daniel. 2016. "Communication Breakdown: Unraveling the Islamic State's Media Efforts." Combating Terrorism Center at West Point. https://ctc.usma.edu/app/uploads/2016/10/ISMedia_Online.pdf; Winter, Charlie. 2018. "Apocalypse, Later: A Longitudinal Study of the Islamic State Brand." *Critical Studies in Media Communication* 35 (1): 103–21. https://doi.org/10.1080/15295036.2017.1393094.

8. For more information about the Scholarly Technology Group, see https://library.gwu.edu/scholarly-technology.

9. https://euske.github.io/pdfminer/index.html

10. https://docs.python.org/3/library/re.html

11. https://docs.python.org/3/library/urllib.parse.html

12. https://doi.org/10.5281/zenodo.2558457; URIScrape is an open-source project available under the MIT license. Code and documentation are also available at https://github.com/gwu-libraries/uriscrape/tree/0.2.2

13. All hashtags, joinlinks, and external URLs are rendered as URLs in Telegram's code.

14. https://pandas.pydata.org.

15. Weirman, Samantha, and Audrey Alexander. 2018. "Hyperlinked Sympathizers: URLs and the Islamic State." *Studies in Conflict & Terrorism*: 1–19. https://doi.org/10.1080/1057610X.2018.1457204.

16. Fisher, Ali, and Nico Prucha. "How Well Established Is the Jihadist Movement on Telegram?" *Online Jihad: Monitoring Jihadist Online Communities* (blog), March 15, 2018. https://onlinejihad.net/2018/03/15/how-well-established-is-the-jihadist-movement-on-telegram.

17. Future studies seeking to measure activity on Telegram could analyze the number of unique users posting in pro-IS groups, though this indicator would also run into limitations concerning duplicate accounts.

Analysis

1. In January 2019, Telegram consolidated the features of supergroups and groups into a singular "groups" function, eliminating supergroups. See; The Telegram Team, "Group Permissions, Undo Delete and More," January 21, 2019. https://telegram.org/blog/permissions-groups-undo.
2. "What is a Telegram Group of Supergroup?" Telegram Guide. https://telegramguide.com/what-is-telegram-supergroup.
3. The Telegram Team, "Admins, Supergroups and More," Telegram. November 25, 2015. https://telegram.org/blog/supergroups.
4. The Telegram Team, "Supergroups 10,000: Admin Tools and More," Telegram. June 30, 2017. https://telegram.org/blog/admin-revolution.
5. The Telegram Team, "Group Permissions, Undo Delete and More," January 21, 2019. https://telegram.org/blog/permissions-groups-undo.
6. Berger and Perez, "The Islamic State's Diminishing Returns on Twitter," 2016.
7. Clifford, Bennett. 2018. "'Trucks, Knives, Bombs, Whatever:' Exploring Pro-Islamic State Instructional Material on Telegram." *CTC Sentinel* 11 (5). https://ctc.usma.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram.
8. *Ibid.*
9. Winter and Parker, "Virtual Caliphate Rebooted," 2018. Smith, "Messaging App Telegram Centerpiece of IS Social Media Strategy," 2017; Katz, Rita. 2019. "A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps." *Wired*. January 9, 2019. https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps.
10. "Telegram F.A.Q." n.d. Telegram. https://telegram.org/faq.
11. External joinlinks potentially include joinlinks to destinations that did not meet the selection criteria (lacking either pro-IS or English-language content), inaccessible joinlinks, or joinlinks missed during data collection.
12. Bindner and Gluck, "Wilayat Internet," 2017.
13. Alexander, "Digital Decay?" 2017.
14. The Telegram Team, "Shared Files and Fast Mute," Telegram. February 1, 2015. https://telegram.org/blog/shared-files.
15. "WhatsApp F.A.Q.: Why can't I send long videos in WhatsApp?" n.d. WhatsApp. Accessed February 1, 2019. https://faq.whatsapp.com/en/iphone/30060668.
16. "Twitter Help Center: Adding Content to Your Tweet" n.d. Twitter. Accessed February 1, 2019. https://help.twitter.com/en/using-twitter/twitter-videos.
17. Future analyses of content on Telegram can benefit from Telegram's new file download feature, which was nonexistent during data collection.
18. Vidino, Lorenzo. Hughes, Seamus. 2015. "ISIS in America: From Retweets to Raqqa," The Program on Extremism. December, 2015. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/ISIS%20in%20America%20-%20Full%20Report.pdf
19. Bindner and Gluck, "Wilayat Internet," 2017.
20. "Telegram F.A.Q."
21. Bindner and Gluck, "Wilayat Internet," 2017.
22. *Ibid.*
23. Kelion, Leo. "IS Propaganda 'Hidden on Internet Archive.'" BBC, May 15, 2018, sec. Technology. https://www.bbc.com/news/technology-44112431.
24. Fishwick, Carmen. "How a Polish Student's Website Became an Isis Propaganda Tool." *The Guardian*, August 15, 2014. https://www.theguardian.com/world/2014/aug/15/-sp-polish-man-website-isis-propaganda-tool.
25. Top4Top. https://up.top4top.net.
26. "More Support Needed for Smaller Technology Platforms to Counter Terrorist Content." Trends Alert. UN CTED, November 2018. https://www.un.org/sc/ctc/wp-content/uploads/2019/01/CTED-Trends-Alert-November-2018.pdf; "ISIS use of smaller platforms and the DWeb to share terrorist content," Tech Against Terrorism, April 29, 2019. https://www.techagainstterrorism.org/2019/04/29/analysis-isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content-april-2019.
27. This is a derogatory term for Shi'a Muslims. The hashtag is generally used to mark battles or attacks against Shi'a militia groups in Iraq and Syria.
28. "How the Battle for Mosul Unfolded." BBC, July 10, 2017, sec. Middle East. https://www.bbc.com/news/world-middle-east-37702442; Hassan, Hassan. 2017. "The Battle for Raqqa and the Challenges after Liberation." *CTC Sentinel 10* (6).
29. McKirdy, Euan, and Ivan Watson. "Bloodied and Broken: Rising Toll of Philippines' War with ISIS." CNN, August 24, 2017. https://www.cnn.com/2017/06/25/asia/philippines-marawi-isis/index.html.
30. Bindner and Gluck, "Wilayat Internet," 2017.
31. Bridge, Mark. "Isis Supporters Gloat over Manchester Carnage on Social Media." *The Times*, May 24, 2017, sec. News. https://www.thetimes.co.uk/article/isis-supporters-gloat-over-carnage-on-social-media-bq9fb59b0.
32. Beaumont, Peter. "Two Israeli Police and Three Gunmen Killed in Shootout at Holy Site." *The Guardian*, July 14, 2017. https://www.theguardian.com/world/2017/jul/14/

shooting-attack-jerusalem-temple-mount-friday-prayers.

33. Reinares, Fernando, and Carola Garcia-Calvo. 2018. "'Spaniards, You Are Going to Suffer:' The Inside Story of the August 2017 Attacks in Barcelona and Cambrils." *CTC Sentinel* 11 (1). https://ctc.usma.edu/spaniards-going-suffer-inside-story-august-2017-attacks-barcelona-cambrils.

34. "Parsons Green Bombing." BBC News. https://www.bbc.co.uk/news/topics/cwz4l24gel2t/parsons-green-bombing.

35. "Egypt Mosque Attackers Kill 235." BBC News, November 24, 2017, sec. Middle East. https://www.bbc.com/news/world-middle-east-42110223.

36. Breeden, Aurelien. "French Police Officer Wounded in Hostage Standoff Dies." *The New York Times*, March 26, 2018, sec. World. https://www.nytimes.com/2018/03/23/world/europe/france-trebes-attack.html.

37. Milton, "Communication Breakdown,"; Winter, "Apocalypse Later," 2018.

38. Alexander, "Digital Decay?" 2017.

39. Winter and Parker, "Virtual Caliphate Rebooted," 2018.

40. Alexander, Audrey. Powell, Helen. 2018. "Gray Media Under the Black and White Banner." *Lawfare*. May 6, 2018. https://www.lawfareblog.com/gray-media-under-black-and-white-banner.

41. Bloom, Mia, Hicham Tiflati, and John Horgan. 2017. "Navigating ISIS's Preferred Platform: Telegram." *Terrorism and Political Violence* 0 (0): 1–13. https://doi.org/10.1080/09546553.2017.1339695.

Case Studies

1. Caliwan, Christopher. 2017. "Woman inciting terror online nabbed in Taguig," Philippine News Agency, October 18, 2017. http://www.pna.gov.ph/articles/1013106

2. Mogato, Manuel. "Philippines arrests militant widow for trying to recruit fighters," Reuters, October 18, 2017. https://www.reuters.com/article/us-philippines-militants-arrest/philippines-arrests-militant-widow-for-trying-to-recruit-fighters-idUSKBN1CN0S0

3. Fonbuena, Carmela. 2017. "Counterterrorism: Why the death of AKP's Tokboy matters," *Rappler*, January 16, 2017. https://www.rappler.com/newsbreak/iq/157731-akp-ansar-khalifa-philippines-tokboy-death

4. "Charge Sheet." 2016. *State (NIA) v/s Mohamed Naser and Others*, NIA Patiala House Courts New Delhi. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Naser%20Charge%20Sheet%20%28NIA%29.pdf

5. *Ibid.*

6. *Ibid.*

7. "Supplementary Charge Sheet." 2016. *State (NIA) v/s Mohamed Naser and Others*, NIA Patiala House Courts New Delhi. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Naser%20Supplementary%20Charge%20Sheet%20%28NIA%29.pdf

8. Laskar, Rezaul. 2019. "Karnataka-born key Islamic State terrorist Shafi Armar killed, says group." *Hindustan Times*. March 23, 2019. https://www.hindustantimes.com/india-news/karnataka-man-and-is-recruiter-killed-in-syria/story-nbhia2dUsnTkCGiudHuVDP.html.

9. "Charge Sheet." 2016. *State (NIA) v/s Sheikh Azhar Ul Islam and Others*. NIA Court, New Delhi, 5. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Islam%20et%20al%20Charge%20Sheet%20%28NIA%29.pdf

10. *Ibid.*

11. Program on Extremism interview with U.S. government official, February 2019.

12. "Statement of Facts." 2018. USA v. Sean Duncan. *United States District Court for the Eastern District of Virginia*, 2. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/DuncanStatementofFacts.pdf

13. *Ibid.,* 3.

14. *Ibid.,* 3-4.

15. Singh, Vijaita. 2018. "Radicalised Filipina lured Indian men into IS web." *The Hindu*, May 6, 2018. https://www.thehindu.com/news/national/radicalised-filipina-lured-indian-men-into-is-web/article23790722.ece

16. See: Moore, Jack. 2017. "Philippines Arrests Top Female ISIS Recruiter of Foreign Fighters For Marawi Battle." *Newsweek*, October 18, 2017. https://www.newsweek.com/philippines-arrests-top-female-isis-recruiter-foreign-fighters-marawi-battle-687496. *Associated Press*. 2017. "Philippines says militant's widow recruited foreign fighters." October 18, 2017. https://apnews.com/bf0887e634b44ee69895c9a023483d01.

17. Dancel, Raul. 2017. "Philippines arrests top female ISIS recruiter." *The Straits Times*. October 18, 2017. https://www.straitstimes.com/asia/se-asia/philippines-arrest-top-female-isis-recruiter-ex-wife-of-radicalised-singaporean.

18. "Charge Sheet." 2016. *State (NIA) v/s Moahammed Sirajuddin*. NIA Court, Jaipur, Rajasthan. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sirajuddin%20Charge%20Sheet%20%28NIA%29.pdf

19. *Ibid.*

20. "Marawi, the "East Asia Wilayah" And Indonesia," 2017. Institute for Policy Analysis of Conflict, July 21, 2017, 16. http://file.understandingconflict.org/file/2017/07/

IPAC_Report_38.pdf

21. Bloom, Tiflati, and Horgan, "Navigating ISIS's Preferred Platform: Telegram," 2017.

22. Alexander, Audrey. 2019. "Perspectives on the Future of Women, Gender, & Violent Extremism," The Program on Extremism, February, 2019. 50-51. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Key%20Considerations-%20Forward%20Thinking%20About%20Women%2C%20Gender%2C%20and%20Violent%20Extremism.pdf

23. "Criminal Complaint." 2018. *U.S. v Ashraf Al Safoo*. United States District Court Northern District of Illinois Eastern Division. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Safoo%20Criminal%20Complaint.pdf.

24. "Chicago Man Charged with Conspiring to Support ISIS." 2018. Department of Justice Press Release. October 19, 2018. https://www.justice.gov/usao-ndil/pr/chicago-man-charged-conspiring-support-isis.

25. "Criminal Complaint." 2018. *U.S. v Ashraf Al Safoo*, 2.

26. *Ibid.*, 24.

27. Al Hayat Media Center. 2017. "Brothers in Marawi." October 12, 2017. Accessed via https://jihadology.net/2017/10/12/new-nashid-from-the-islamic-state-brothers-in-marawi.

28. "Criminal Complaint." 2018. *U.S. v Ashraf Al Safoo*, 25.

29. *Ibid.,* 11.

30. *Ibid.,* 22.

31. *Ibid.,* 21.

32. Prucha, "IS and the Jihadist Information Highway," 2016.

33. "Criminal Complaint." 2018. *U.S. v Ashraf Al Safoo*, 37.

34. *Ibid.*, 35.

35. *Ibid.*, 38.

36. *Ibid.*, 40

37. Alexander, Audrey, and William Braniff. 2018. "Marginalizing Violent Extremism Online." *Lawfare*. January 21, 2018. https://www.lawfareblog.com/marginalizing-violent-extremism-online.

38. "Criminal Complaint." 2018. *USA v. Ashraf Al Safoo,* 42-43.

39. Ashraf Al Safoo Linkedin Profile. Accessed February 1, 2019. https://www.linkedin.com/in/ashraf-al-safoo-b5b050b.

40. "Criminal Complaint." 2018. *USA v. Ashraf Al Safoo*.

41. Romo, Vanessa. 2019. "FBI Finds No Motive In Las Vegas Shooting, Closes Investigation." NPR. January 29, 2019. https://www.npr.org/2019/01/29/689821599/fbi-finds-no-motive-in-las-vegas-shooting-closes-investigation

42. "Criminal Complaint." 2018. *USA v. Ashraf Al Safoo*, 29.

43. *Ibid.,* 29-30.

44. *Ibid.,* 18.

45. *Ibid.,* 20.

46. *Ibid.,* 20.

47. Cowell, Alan. 2018. "The 'Lone Mujahid,' Who Threatened Prince George, Pleads Guilty." *The New York Times*, June 1, 2018, sec. World. https://www.nytimes.com/2018/05/31/world/europe/uk-terrorism-prince-george-husnain-rashid.html.

48. "Terror Accused 'Urged Prince George Attack.'" 2018. BBC, May 23, 2018, sec. Lancashire. https://www.bbc.com/news/uk-england-lancashire-44222753.

49. "Life Term for Prince George Attack Plotter," BBC, July 13, 2018, sec. Lancashire. https://www.bbc.com/news/uk-england-lancashire-44825047.

50. Posts in Telegram channel collected by the research team and reviewed by the authors, February 2019.

51. "Pro-IS Telegram Channel Lives on despite Jailing of Creator in UK." 2018. BBC Monitoring. https://monitoring.bbc.co.uk/product/c2003smw.

52. *Ibid.*

53. Gadher, Dipesh. 2015. "Manuals for 'Lone Wolf' Attacks Posted Online by UK Extremists." *The Sunday Times*, June 28, 2015. https://www.thetimes.co.uk/article/manuals-for-lone-wolf-attacks-posted-online-by-uk-extremists-pp5tpd9jm09.

54. Abu Kitaab al-Inkaltarra. *The Book of Terror*. 2015.

55. Posts in Telegram channels collected by research team and reviewed by the authors, February 2019.

56. *Ibid.*

57. *Ibid.*

58. Cowell, "The 'Lone Mujahid'," 2018.

59. *Ibid.*

60. *Ibid.*

61. "Pro-IS Telegram Channel Lives on despite Jailing of Creator in UK." 2018. BBC Monitoring. https://monitoring.bbc.co.uk/product/c2003smw.

62. *Ibid.*

Critcal Considerations

1. Clary, "The Flaw in ISIS's Favorite Messaging App," 2016; The Grugq, "Operational Telegram," 2015; Cox, "Encryption App Telegram Probably Isn't as Secure for Terrorists as ISIS Thinks," 2015.

2. Smith, Laura. 2017. "Islamic State Piggybacks Social Mega-Feed." BBC, June 12, 2017, sec. Technology. https://

www.bbc.com/news/technology-40246763.

3. *Ibid.*
4. *Ibid.*
5. BBC Monitoring. 2018. “Islamic State Media Turn to Rocket.Chat for Messaging,” December 20, 2018. https://monitoring.bbc.co.uk/product/c200i1fj#section21.
6. *Ibid.*
7. Bodo, “Decentralised Terrorism.” 2018.
8. Alexander, “Digital Decay?” 2017.
9. Brachman and Levine, “You Too Can Be Awlaki!” 2001.
10. BBC. 2018. “Germany to Enforce Hate Speech Law,” January 1, 2018, sec. Technology. https://www.bbc.com/news/technology-42510868.
11. Asthana, Anushka, and Sam Levin. 2017. “UK Urges Tech Giants to Do More to Prevent Spread of Extremism.” *The Guardian*, July 31, 2017, sec. Technology. https://www.theguardian.com/technology/2017/aug/01/uk-urges-tech-giants-to-do-more-to-prevent-spread-of-extremism.
12. Briggs, Rachel, and Sebastian Feve. 2014. “Policy Brief: Countering the Appeal of Extremism Online.” Institute for Strategic Dialogue. https://www.dhs.gov/sites/default/files/publications/Countering%20the%20Appeal%20of%20Extremism%20Online_1.pdf.
13. Alexander and Braniff, “Marginalizing Violent Extremism Online,” 2018.
14. *Ibid.*
15. *Ibid.*
16. Ingram, Haroro. 2017. “‘That Is What the Terrorists Want’: Media as Amplifier or Disrupter of Violent Extremist Propaganda.” presented at “The judicial response to terrorism and the charter of fundamental rights of the EU: Media treatment of terrorism cases,” European Commission, June 15. https://icct.nl/wp-content/uploads/2017/06/INGRAM-paris-speech.pdf.
17. *Ibid.*
18. *Ibid.*
19. *Ibid.*
20. Lakomy, “Cracks in the Online ‘Caliphate’,” 2017.
21. Graham, Robert. 2016. “How Terrorists Use Encryption.” *CTC Sentinel* 9: 6. https://ctc.usma.edu/how-terrorists-use-encryption.
22. “GIFCT.” n.d. Accessed March 9, 2019. http://www.gifct.org.
23. “Partners” n.d., GIFCT, Accessed March 9, 2019. https://www.gifct.org/partners.
24. “About Tech Against Terrorism.” n.d. Tech Against Terrorism. Accessed March 9, 2019. https://www.techagainstterrorism.org/about.
25. “Knowledge Sharing Platform.” n.d. Tech Against Terrorism. Accessed March 9, 2019. https://ksp.techagainstterrorism.org/.
26. Brantly, Aaron. 2017. “Banning Encryption to Stop Terrorists: A Worse than Futile Exercise.” *CTC Sentinel* 10 (7). https://ctc.usma.edu/banning-encryption-to-stop-terrorists-a-worse-than-futile-exercise/.
27. National Academies of Sciences. 2018. *Decrypting the Encryption Debate: A Framework for Decision Makers*. Consensus Study Report. https://doi.org/10.17226/25010.
28. Brantly, “Banning Encryption to Stop Terrorists: A Worse than Futile Exercise.”
29. *Ibid.*
30. *Ibid.*
31. *Ibid.*
32. *Ibid.*
33. Erdbrink, Thomas. 2018. “Iran, Like Russia Before It, Tries to Block Telegram App.” *The New York Times*, October 10, 2018, sec. World. https://www.nytimes.com/2018/05/01/world/middleeast/iran-telegram-app-russia.html.
34. *Ibid.*
35. “Closing of the Gates: Implications of Iran’s Ban on the Telegram Messaging App.” 2018. New York: Center for Human Rights in Iran. https://www.iranhumanrights.org/wp-content/uploads/Closing-the-gates-3-online.pdf.
36. Weselowsky, Tony. 2018. “In Russia, You Don’t Have To Be A Telegram User To Be Affected By The Ban.” RadioFreeEurope/RadioLiberty. April 17, 2018. https://www.rferl.org/a/in-russia-you-dont-have-to-be-a-telegram-user-to-be-affected-by-the-ban/29172774.html.

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

extremism.gwu.edu @gwpoe