Combating Terrorism Center
AT WEST POINT

ISD | Institute for Strategic Dialogue

الارشيف الاضخم للدولة الاسلامية

THE CLOUD CALIPHATE

ARCHIVING THE ISLAMIC STATE IN REAL-TIME

Moustafa Ayad, Amarnath Amarasingam, and Audrey Alexander | May 2021

The Cloud Caliphate:
Archiving the Islamic State in Real-Time

Moustafa Ayad
Amarnath Amarasingam
Audrey Alexander

Institute for Strategic Dialogue

ISD | Institute for Strategic Dialogue

Combating Terrorism Center at West Point

United States Military Academy

www.ctc.usma.edu

May 2021

Cover Photo: A cropped screenshot of a 2020 tweet by a pro-Islamic State account promoting access to the largest online archive for the Islamic State

CONTACT

Combating Terrorism Center

U.S. Military Academy

607 Cullum Road, Lincoln Hall

West Point, NY 10996

Phone: (845) 938-8495

Web: www.ctc.usma.edu

ACKNOWLEDGMENTS

The ISD-CTC team would like to thank their colleagues for their support of this project, particularly CTC Executive Director Brian Dodwell. Special thanks also to CTC Research Associate Muhammad al-`Ubaydi and Cadet Amir Udler at the United States Military Academy at West Point for their input on this report. CTC's Kristina Hummel provided us a fresh set of eyes and copyedits to help us cross the finish line and prepare the piece for publication.

About the Authors

Moustafa Ayad is the current Executive Director for Africa, the Middle East, and Asia at the Institute for Strategic Dialogue (ISD), overseeing more than 20 programs globally, and has more than a decade's worth of experience designing, developing, and deploying multi-faceted P/CVE, elections, and gender projects in conflict and post-conflict environments across the Middle East and Africa. He has experience in Iraq, Afghanistan, Yemen, Syria, Lebanon, Jordan, Kenya, and Senegal, with a range of government and non-governmental partners on violent extremism, conflict resolution, and strategic communications. He also has experience working across these regions with community organizations, media outlets, and regional/global production hubs on the creation of multi-platform media content aimed at empowering youth, supporting civil society, and strengthening national and local stakeholder capacity. His research on the use of social media platforms by extremist groups and their supporters has been featured in the BBC, *The Times*, VICE, CNN, NPR, *Wired*, and The Daily Beast.

Amarnath Amarasingam is an Assistant Professor in the School of Religion, and is cross-appointed to the Department of Political Studies, at Queen's University in Ontario, Canada. He is also a Senior Research Fellow at the Institute for Strategic Dialogue (ISD), an Associate Fellow at the International Centre for the Study of Radicalisation, and an Associate Fellow at the Global Network on Extremism and Technology. His research interests are in terrorism, radicalization and extremism, diaspora politics, post-war reconstruction, and the sociology of religion. He is the author of *Pain, Pride, and Politics: Sri Lankan Tamil Activism in Canada* (2015), and the co-editor of *Sri Lanka: The Struggle for Peace in the Aftermath of War* (2016). He has also written several peer-reviewed articles and book chapters, has presented papers at over 100 national and international conferences, and has written for *The New York Times*, The Monkey Cage, *The Washington Post*, CNN, Politico, *The Atlantic*, and *Foreign Affairs*. He has been interviewed on CNN, PBS Newshour, CBC, BBC, and a variety of other media outlets. He tweets at @AmarAmarasingam

Audrey Alexander is a researcher and instructor at West Point's Combating Terrorism Center. In that role, she studies terrorist exploitation of technology and investigates the nexus of gender and violent extremism. Before joining the Center, Alexander served as a senior research fellow at the George Washington University's Program on Extremism and worked at the International Centre for the Study of Radicalization. She is also an Associate Fellow at the Global Network on Extremism and Technology. Alexander holds a master's degree in Terrorism, Security & Society from the War Studies Department at King's College London.

TABLE OF CONTENTS

Executive Summary

This report offers a preliminary survey and analysis of one of the largest known online repositories of Islamic State materials in order to increase understanding of how violent extremist groups and their supporters manage, preserve, and protect information relevant to their cause. Seemingly managed by sympathizers of the Islamic State, the large cache of digital files, here nicknamed the "Cloud Caliphate," can offer researchers, policymakers, and counterterrorism practitioners additional insights on how and why groups and their adherents maintain archives of such material. From a sociological standpoint, caches like the "Cloud Caliphate" serve to curate a shared history of the movement. At the operational and tactical level, digital repositories help the online contingents of the group rally in the face of setbacks, particularly when adherents promote such resources across numerous information and communications platforms. Initially identified, accessed, and documented by the Institute for Strategic Dialogue (ISD), research partners at the Combating Terrorism Center (CTC) at the United States Military Academy at West Point supported the analysis. Ultimately, given the size of the "Cloud Caliphate" and the scope of its contents, no single research method is suitable for an initial survey of this resource. Instead, the authors of this report used a mixed-methods approach to explore different aspects of the cache, highlighting how digital archives like the "Cloud Caliphate" might inform researchers, practitioners, and policymakers in the future. The core analysis breaks into seven different parts. After reviewing the likely origins of the repository, the first section describes its composition, and the second discusses evidence concerning cyber support from other online actors. Then, sections three through six explore specific folders within the archive, which pertain to matters concerning the Islamic State's organizational predecessors and a range of notable leaders, ideologues, and scholars. Section seven of the report highlights a real-world case involving the use of the "Cloud Caliphate" archive by an Islamic State supporter.

The report concludes with a reflective discussion that notes potential policy considerations for those tasked with confronting the Islamic State's exploitation of information and communications technologies. First, it argues relevant stakeholders must look for opportunities to identify, document, and study accessible repositories and take stock of the methods used to build, promote, and maintain such resources. Second, while respecting human rights and the rule of law, relevant stakeholders should look for opportunities to identify and disrupt individuals creating, administering, supporting, or using the resources for criminal, terrorism-related activities. Third, stakeholders concerned with violent extremist exploitation of website services to develop repositories like the "Cloud Caliphate" must remember this problem is not new, and it brushes up against big questions involving internet governance. Fourth, relevant stakeholders, including service providers and organizations like the Global Internet Forum to Counter Terrorism and Tech Against Terrorism, should continue exploring ways to marginalize the influence of sources like the "Cloud Caliphate" by focusing on the networks and tools that enable them to reach new users. Ultimately, the counterterrorism community must recognize the role digital archives play in fostering a shared sense of identity in a global movement. Realizing the potential of repositories like the "Cloud Caliphate," for better or worse, should inform the development of mitigation tools.

Introduction

While the Islamic State may be a shell of itself in Iraq and Syria, it still conducts attacks with relative frequency in both countries.[1] Beyond Iraq and Syria, news reports indicate that the Islamic State has also stepped up attacks through its affiliates across Africa in places like Mozambique, Mali, Nigeria, and Egypt.[2] Contrary to claims of the Islamic State's defeat,[3] the enduring prevalence of the movement, both online and offline, indicates that the fight against the Islamic State and its global base of supporters is not over. On the contrary, the organization's ability to remain and expand continues to adapt to new pressures. Although the Islamic State's adaptation has taken place in different ways, its efforts to preserve and continue to disseminate information are of critical research importance. Consequently, this report focuses on Islamic State-affiliated content stored on digital archives, and the method of creating hubs of information to preserve such materials. Such research reveals one small part of the movement's ongoing efforts to document its path to stay relevant in the future.

Despite the group's territorial ebbs and flows, its virtual presence is far from "obliterated."[4] The decentralized nature of the Islamic State's online community makes it so that claims of victory—especially in an expansive and fluid operational theater such as the internet—are generally modest and short-lived. While pushing Islamic State sympathizers off select social media platforms may temporarily give governments or technology companies a sense of progress, pockets of sympathizers will continue to endure, regardless of countermeasures. For better or worse, decentralization is a feature of the internet and a defining characteristic of the Islamic State's web presence. In day-to-day life online, some adherents strive to unite disparate supporters under one banner and rely on information-sharing methods to project a unified narrative in the face of setbacks. While relatively specific, this report shows that somewhat-centralized online repositories housing content is one way Islamic State supporters rally in the face of setbacks. Since other terrorist organizations and violent extremist groups may use similar modes of operation, it is beneficial to examine such efforts and discuss policy considerations for managing such activities.

To better understand this aspect of the Islamic State's online ecosystem, this report explores the largest known online repository containing content aligned with the Islamic State or supportive of its worldviews. Nicknamed the "Cloud Caliphate" for this project, the large, formerly password-protected platform was accessed, archived, and analyzed by researchers at the Institute for Strategic Dialogue (ISD) in partnership with the Combating Terrorism Center at the United States Military Academy at West Point. Given sensitivities concerning the inadvertent promotion or glorification of terrorist material in pursuit of research, the authors chose to use the pseudonym "Cloud Caliphate" for the repository rather than broadcast the domain name.

Before delving into a discussion about the contents of the "Cloud Caliphate," this report will offer some background and context on violent extremists' use of repositories, exploring why such resources matter to groups like the Islamic State from a sociological perspective. With that foundation, the report will focus on the "Cloud Caliphate" itself, discussing how researchers accessed, documented, and evaluated

1 In a policy paper, Elizabeth Dent notes: "While U.S. policy in Iraq has remained laser-focused on Iran and winding down its military presence, ISIS has quietly reconstituted. In the first quarter of 2020 alone, 566 ISIS attacks were reported in Iraq." Elizabeth Dent, "US Policy and the resurgence of ISIS in Iraq and Syria," Middle East Institute, October 21, 2020. See also "Operation Inherent Resolve, Lead Inspector General Report to the United States Congress, July 1, 2020- September 30, 2020," released November 3, 2020.

2 Frank Gardner, "Is Africa overtaking the Middle East as the new jihadist battleground?" BBC, December 3, 2020.

3 Eric Schmitt and Adam Goldman, "The head of the Pentagon's Defeat ISIS Task Force was ousted and his office disbanded," *New York Times*, December 1, 2020; "President Trump: We have defeated ISIS," official Facebook page for The White House, August 21, 2020; Donald J. Trump, "Remarks by President Trump on the death of ISIS leader Abu Bakr al-Baghdadi," The White House, October 27, 2019; Paolo Zialcita, "Islamic State 'not present on the internet anymore' following European operation," National Public Radio, November 25, 2019.

4 "Europol disrupts Islamic State propaganda machine," BBC Monitoring, November 25, 2019.

the archive. Due to its size and scope, researchers decided that a mixed-method approach exploring seven different aspects of the repository offered value by demonstrating how the counterterrorism community might leverage such resources. Consequently, the core analysis breaks into seven different parts. After reviewing the repository's likely origins, the first section describes its composition, and the second discusses evidence concerning cyber support. Then, sections three through six explore specific folders within the archive. Section seven of the report delves into a real-world case of an Islamic State supporter who appeared to have access to the "Cloud Caliphate." This report will conclude with a reflective discussion that raises policy considerations for managing online contingents of movements like the Islamic State and explores methods for disrupting the creation and management of resources like the "Cloud Caliphate."

Background and Context

Over the past few years, research on the Islamic State's exploitation of information and communications technologies has worked to keep pace with the movement's ever-changing ecosystem of online adherents.[5] To the credit of researchers and analysts around the world, many aspects of the Islamic State's online behavior are documented and examined. Even so, old and new problems continue to create opportunities for subsequent analysis, like the enduring issue of URL sharing by violent extremists.[6] Some contemporary studies strive to chart the Islamic State's forays onto emerging platforms, such as text-based applications supplementing the movement's use of other messengers like Telegram and Kik and broad-based social media like Facebook and Twitter.[7] Other research has focused on the countermeasures Islamic State supporters use to overcome the challenges of online content moderation with tactics such as leveraging link-shorteners, using bots, hijacking hashtags, or using compromised and expendable accounts.[8] Some long-standing efforts by violent extremists to keep digital content accessible online, including rudimentary practices like making collections of content accessible with websites, forums, and other file-sharing tools, still warrant attention.[9] Today, there seems to be a modern twist on these old-school techniques as pro-Islamic State sympathizers use new tactics and platforms to seed links to longer-running collections of material. To better understand this phenomenon and its impacts, this report discusses the existence, contents, and promotion of the "Cloud Caliphate," the largest known repository aligned with the Islamic State and its predecessors. Before articulating how researchers accessed and studied the cache, it is helpful to highlight the roles of digital archives in fostering a shared sense of identity within an amorphous online community.

5 Deven Parekh, Amarnath Amarasingam, Lorne Dawson, and Derek Ruths, "Studying Jihadists on Social Media: A Critiques of Data Collection Methodologies," *Perspectives on Terrorism* 12:3 (2018); Amarnath Amarasingam, "What Twitter Really Means for Islamic State Supporters," War on the Rocks, December 30, 2015.

6 Moustafa Ayad, "'The Baghdadi Net': How a network of ISIL-supporting accounts spread across Twitter," Institute for Strategic Dialogue (ISD), November 2019; Samantha Weirman and Audrey Alexander, "Hyperlinked Sympathizers: URLs and the Islamic State," *Studies in Conflict and Terrorism* 43:3 (2018).

7 Bennett Clifford, "Migration Moments: Extremist Adoption of Text-Based Instant Messaging Applications," Global Network on Extremism and Technology (GNET), 2020; Ali Fisher, Nico Prucha, and Emily Winterbotham, "Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability," RUSI, Global Research Network on Terrorism and Technology, July 2019; Amarnath Amarasingam, "Telegram Deplatforming ISIS Has Given Them Something to Fight For," Vice, December 5, 2019; Amarnath Amarasingam, Shiraz Maher, and Charlie Winter, "How Telegram Disruption Impacts Jihadist Platform Migration," CREST, January 8, 2021.

8 Stuart Macdonald, Daniel Grinnell, Anina Kinzel, and Nuria Lorenzo-Dus, "A Study of Outlines Contained in Tweets mentioning Rumiyah," RUSI, Global Research Network on Terrorism and Technology, Paper No. 2; Ayad, "'The Baghdadi Net': How a network of ISIL-supporting accounts spread across Twitter;" Weirman and Alexander.

9 Brian Fishman, *The Master Plan: ISIS, al-Qaeda, and the Jihadi Strategy for Final Victory* (New Haven, CT: Yale University Press, 2016): pp. 56-57. See also Akil Awan and Mina Al-Lami, "Al-Qa'ida's Virtual Crisis," *RUSI Journal* 154:1 (2009); Aaron Zelin, "The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis," New America Foundation, January 2013; Aaron Brantly, "Innovation and Adaptation in Jihadist Digital Security," *Survival* 59:1 (2017); Craig Whiteside, "Lighting the Path: The Evolution of the Islamic State Media Enterprise (2003-2016)," The International Centre for Counter-Terrorism – The Hague (ICCT), November 2016.

The Will to Remember: The Islamic State's Imagined Community

From a sociological standpoint, whether used by extremist groups or non-violent movements, digital archives can help foster real and imagined identities. Wolfgang Ernst, the German media theorist, wrote that "the Internet extends the classical space of the archive, library, and museum by an extra dimension."[10] That extra dimension is where groups often create meaning out of loss. Following the devastating 9/11 attacks, historians designed and developed the *September 11 Digital Archive* to "create a permanent record of the events of September 11, 2001." The archive partnered with the Library of Congress a year later, the first digital acquisition by the Library of Congress, and it now represents one of the largest, most comprehensive digital archives of the terrorist attack to date. It contains some 150,000 pieces of digital content, about 40,000 emails, 40,000 first-hand stories, and 15,000 images.[11] Archives, in this sense, help preserve the collective sensory memory of the most spectacular terrorist attack of the past two decades and serve to fortify national identity.

Arjun Appadurai contends that archiving, in any form, functions as part of a collective project, suggesting "the archive is itself an aspiration rather than a recollection."[12] He suggests the archive represents a "collective will to remember" rather than a benign collection of the extant traces of history.[13] The desire to remember and archive thus reveals the desires of those seeking to record and document the past. For Islamic State supporters, the creation and curation of the online cache is a process of delineating the ideological and territorial parameters of what it means to be a supporter or member of the Islamic State. As this report demonstrates in its analytical discussion of the "Cloud Caliphate" repository, the ideologues, scholars, and territories they choose to include are not incidental but, like any national archive anywhere, can demarcate what is important to the group.

With the birth of digital archives, "the archive is gradually freed of the orbit of the state and its official networks" and "returns to its more general status of being a deliberate site for the production of anticipated memories by intentional communities."[14] This style of imagining a community—the imagined community of the nation—figures centrally in the aforementioned assessments of the modern archive. For Mike Featherstone, "archives along with museums, libraries, public monuments and memorials became instruments for the forging of the nation into the people — into an imagined community."[15] Case studies of particular modern archives have also borne out these claims about the "will to archive," and its support of emergent imagined communities, from Julie Biando Edwards and Stephen P. Edwards' analysis of the Iraq National Library and Archive to Sophia Milosevic Bijleveld's exploration of the Jihad Museum in Herat, Afghanistan.[16] In both case studies, the archive offers a site for the consolidation of what Anderson calls the "national biography," a coherent narrative "for ordering events of the past in light of the nation."[17] The "Cloud Caliphate" arguably serves the same function for Islamic State supporters: it is an ever-evolving repository of cultural productions that communicate what the Islamic State is about and who champions its ideas and narratives, and the

10 Wolfgang Ernst, *Digital Memory and the Archive* (Minneapolis: University of Minnesota Press, 2013), p. 84.

11 "The September 11 Digital Archive," American Social History Project, Center for Media and Learning, accessed on August 10, 2020.

12 Arjun Appadurai, "Archive and Aspiration," in Joke Brouwer and Arjen Mulder eds. *Information is Alive: Art and Theory on Archiving and Retrieving Data* (Rotterdam, Netherlands: NAI Publishers, 2003): p. 16.

13 Ibid., p. 17.

14 Ibid., p. 17.

15 Mike Featherstone, "Archive," *Theory, Culture & Society* 23:2-3 (2006): p. 592.

16 Sophia Milosevic Bijleveld, "Afghanistan: Re-imagining the nation through the museum - the Jihad Museum in Herat," *Studies in Ethnicity and Nationalism* 6:2 (2006): pp. 105-124; Julie Biando Edwards and Stephan Edwards, "Culture and the New Iraq: The Iraq National Library and Archive, 'Imagined Community,' and the Future of the Iraqi Nation," *Libraries & the Cultural Record* 43:3 (2008): pp. 327-342.

17 Benedict Anderson, *Imagined Community: Reflections on the Origin and Spread of Nationalism* (New York City, NY: Verso, 2006): p. 206.

archive separates the group's enemies from its adherents.

In 2006, long before the announcement of the "caliphate" and the proliferation of Islamic State accounts and websites across the open web, researchers were already concerned with "the size and scope of the web resources being developed by jihadist sympathizers" and the "key nodes" and "mother sites" of "jihadist groups, and of key jihadist clerics and ideologues."[18] At the time, researchers posited that by understanding one website within these online networks of jihadis, they could better understand the functionality, centrality, and importance of others in the same network.

Researchers at the University of Wollongong delved into the use of "anonymous sharing platforms and [Islamic State] content" in 2018. They aimed to provide "countermeasures against online propaganda operations," and to do that effectively, the research would have to go beyond the Telegram channels and dive into "anonymous sharing portals acting as black boxes for [Islamic State]-related propaganda." At the time, the research effort was focused on file-sharing sites like Justpaste.it, Sendvid.com, and Dump.to, specifically because Islamic State "networks seem to have reacted to the degradation of their capabilities on popular social media networks and rapidly migrated to new anonymous portals."[19] Predecessors and competitors of the Islamic State have used file-sharing sites like those mentioned above over the years, but mounting pressures from increasingly stringent content moderation efforts online have probably motivated increased use of these tools by Islamic State supporters.[20]

This dynamic, in which certain platforms force terrorist groups and supporters off and necessitate their expedient migration to others, was also at play when EUROPOL targeted Islamic State Telegram channels and groups in late 2019.[21] Such actions resulted in a ballooning of Islamic State channels and groups on TamTam and Hoop Messenger.[22] This dynamic is not unique to the Islamic State; as countries and service providers leverage the same mechanisms against white supremacist groups on social media platforms, similar shifts among sympathizers occur.[23] Ultimately, as this report argues, repositories containing archived material appear to be one way that the Islamic State (and potentially other groups) shifts between platforms and maintains a constant stream of information. While the research community has studied the production, themes, and dissemination of Islamic State-related content, whether produced by the group or its supporters, it dedicates less attention to the role of contemporary digital archives.[24] This report attempts to address that gap, as the authors believe violent extremists' efforts to build, protect, and maintain caches of information could remain a common practice in the years ahead. Particularly as the Islamic State grapples with its future on the ground,

18 One scholar notes: "The key to understanding online jihadism is to decipher the roles that an individual website plays in this interactive and highly dynamic infrastructure." Brynjar Lia, "Al-Qaeda online: understanding jihadist internet infrastructure," *Jane's Intelligence Review*, January 2006.

19 Ahmad Shehabat and Teodor Mitew, "Black-boxing the Black Flag: Anonymous sharing platforms and ISIS content distribution," *Perspectives on Terrorism* 12:1 (2018): pp. 81-99.

20 Awan and Al-Lami; Laurence Binder and Raphael Gluck, "Trends in the Islamic State's Online Propaganda: Shorter Longevity, Wider Dissemination of Content," International Centre for Counter-Terrorism (ICCT), December 5, 2018; "ISIS use of smaller platforms and the D-Web to share Terrorist Content," Tech Against Terrorism, April 29, 2019.

21 Amarnath Amarasingam, "A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit," *CTC Sentinel* 13:2 (2020).

22 Jeff Stone, "Islamic State propaganda efforts struggle after Telegram takedowns, report says," CyberScoop, July 28, 2020; Amarasingam, Maher, and Winter.

23 Ryan Greer, "Weighing the Value and Risks of Deplatforming," Global Network on Extremism and Technology (GNET), May 11, 2020.

24 There has been little focus within the research community on the use of archives across a range of extremist groups as well as their supporters. The al-Qa`ida-linked Global Islamic Media Front (GIMF) uses a "proprietary file-sharing application," which is branded the Epic Drive and once held digital territory on a .com top-level domain, and now on a site top-level domain, using Nextcloud. "Gnews," another GIMF archive, also uses Nextcloud. Al-Shabaab has a similar drive, which is dubbed the Kataib Drive and similarly uses Nextcloud. Then, there is the al-Shahab Archive, the official al-Qa`ida media outlet, which is also using a decentralized open-source file hosting service similar to Nextcloud called Owncloud. With the addition of the "Cloud Caliphate," there are five key drives that are commanded by affiliates and outlets of al-Qa`ida and Islamic State supporters. Four out of the five use the Nextcloud software to support their existence, and only one is currently accessible in full to the researchers: the "Cloud Caliphate."

historical archives like those stored online in the "Cloud Caliphate" will likely be critical to forging a shared identity for supporters, much like any archive.

Methodology: Finding and Leveraging the "Cloud Caliphate"

Focusing on the cache at hand, which is nicknamed the "Cloud Caliphate" for this project, it is vital to explain how researchers identified, accessed, documented, and studied this formerly password-protected, digital collection of materials aligned with the Islamic State and its worldviews. First, the choice to use the "Cloud Caliphate" pseudonym instead of the repository's domain name stems from reservations about the inadvertent promotion or glorification of terrorist material in pursuit of research. Though views on this decision may vary, the authors sincerely aim to offer a productive survey of the cache's contents without amplifying the site and encourage continued discourse on best practices for researchers studying materials associated with violent extremist groups. On a different note, although it is the largest cache of this type known to the authors, Islamic State adherents across numerous platforms appear invested in archiving content and amassing libraries of resources, which suggests the existence of other repositories. The cache features more than seven different languages. The primary languages are Arabic, French, German, and English. The secondary languages, which are less common, include Russian, Turkish, Farsi, Bangla, and Uyghur. Consequently, the analysis provided in this report, which subsequent publications will also explore, assesses the "Cloud Caliphate" as one part of a broader trend.

Before delving into granular details about the "Cloud Caliphate," it helps to understand how researchers identified and accessed the cache in the first place. In 2019, in the midst of an earlier project tracking Islamic State sympathizers' online responses to the death of Islamic State leader Abu Bakr al-Baghdadi,[25] researchers at ISD noticed some interesting link-sharing patterns on Twitter. Curious about this activity, researchers probed further, assessing the type of accounts and tactics used to disseminate a suite of different URLs that lead to the same domain. Further analysis of Islamic State support groups and clusters across numerous platforms, motivated by ISD researchers' initial observations, highlighted an interconnected network of users linked to a continually shifting cache of 1.3 terabytes (now 2.2 terabytes) of Islamic State content. In accessing the site, researchers noted how meticulously someone stored and sorted content using an open-source file hosting service called NextCloud.[26] NextCloud acts as a private file hosting application, with functionalities and user experiences akin to Dropbox and Google Drive. Utilizing a mix of open-source and paid services, NextCloud and Cloudflare—the web server notorious for hosting 8Chan—supporters have created a makeshift online warehouse that stores thousands of pieces of content and doubles as a website.

Supporters of the Islamic State have adapted adeptly to the rapid development of numerous encrypted platforms and open-source technologies to avoid detection. NextCloud is, in fact, the application of choice for The Electronic Horizons Foundation, dubbed the "ISIS Help Desk," to disseminate and store its content to aid supporters in evading authorities and detection online.[27] The tactical tools shared by both the cache's creator(s) and the Electronic Horizons Foundation to build their respective archives are similar, and sympathizers often tout both sites as means to access information when accounts or websites are taken down. This supporter-to-supporter learning is key to understanding how the Islamic State and its various support arms have evolved online. The two drives even share traits such as links to Telegram bots developed for their specific archives at the bottom of the page when they are accessed. Similar designs and tactical measures suggest that supporters learn from each other's

25 Ayad, "'The Baghdadi Net': How a network of ISIL-supporting accounts spread across Twitter."

26 The cache has since grown to 2.2 terabytes from 1.3 terabytes after June 2019, shifting its top-level domain in the process. Researchers are once again scraping its content to understand where content changes have occurred over time.

27 Cory Bennett, "New ISIS 'help desk' to aid hiding from authorities," Hill, February 10, 2016.

methods and possibly even coordinate activities, to develop and distribute archives across various Islamic State support groups with different propaganda supply-chain objectives.

NextCloud is the brainchild of the German open-source software developer Frank Karlitschek, who delivered a "User Data Manifesto" in 2012 that had a goal of giving "users the control over their own data back and to avoid centralized data silos."[28] Free speech advocates applauded the effort because, as Karlitschek put it, it would define "freedoms and rights that users have over their data and not just over their software."[29] This liberation from data restrictions not only plays to a global audience concerned with the overreach of technology companies mining their user databases for information, but also to an audience of Islamic State supporters looking for a safe haven from technology companies' restrictions on content. This nexus—on one side, the movement underpinning the rights of individual users to their data on the open web—converges well with the goals of the digital caliphate, which is to command and expand territory online. This dynamic is arguably under-researched, and media attention often focuses on the exploitation of single platforms rather than examining how Islamic State supporters leverage the open-source movement and decentralized tools to expand their operations online.

From the fall of 2019 through the spring of 2021, researchers analyzing the cache watched the drive grow to 2.2 terabytes through expansion and reorganization. It is also now on a different top-level domain. Evidence suggests that the creator(s) of the cache likely began uploading content to the repository in 2017,[30] and utilized the service to host the contents of a private server on a .com top-level domain they purchased from Tucows Inc. on August 18, 2017.[31] Tucows Inc. is a publicly traded Canadian company that provides wholesale domain registration.[32] According to public website registry records, the drive was hosted on seven different internet hosting services, and has had six unique name changes over the past three years.[33] Public records also suggest that its IP history continually shifted, featuring roughly six IP addresses over the same period of three years. In October 2020, after the cache's .com was disrupted, it reappeared as the same primary URL only on a .co top-level domain, registered through the French company NETIM. As of February 2021, the cache is supported by Cloudflare Inc. hosting services. Research suggests that the "Cloud Caliphate's" administrators are not necessarily unique in their approach to creating websites; the use and abuse of multi-party website service providers for domain registration and hosting is something other violent extremists do, too.[34]

Researchers believe sympathizers promoted non-password-protected links to the cache on popular social media platforms like Twitter, Facebook, and YouTube after al-Baghdadi's death. Before that timeline, users shared the link more exclusively on encrypted peer-to-peer platforms, like Telegram, Hoop, or TamTam, and select pro-Islamic State websites and forums. Likely in an attempt to usurp and disrupt the news cycle around the death of the Islamic State leader, supporters seemed to make a concerted effort to honor the legacy of al-Baghdadi through content posted on primary platforms like Facebook and Twitter and remind supporters of the history, breadth, and depth of the "digital caliphate." Researchers were initially skeptical of the cache's sudden availability, wondering if it was a ruse by intelligence services to draw users into a digital dragnet. However, the authors concluded this

28 Frank Karlitschek, "The user data manifesto," personal blog of Frank Karlitschek, February 10, 2019.

29 Ibid.

30 This is supported by time stamps of when materials were first uploaded in the cache.

31 Researchers used https://whois.domaintools.com/ to access the registry information affiliated with the cache between October 2019 and February 2021.

32 Tucows Inc. has previously been found to have registered al-Qa`ida in the Indian Subcontinent and Tehrik-i-Taliban Pakistan (TTP). Steward Bell, "How the Toronto-registered websites of al-Qaeda and the Pakistani Taliban were taken down," Global News, August 13, 2020.

33 See also "Why Tucows Doesn't Take Down Domains for Website Content Issues," Tucows Blog, December 5, 2017.

34 Bell. See also Jytte Klausen, Eliane Tschaen Barbieri, Aaron Reichlin-Melnick, and Aaron Zelin, "The YouTube Jihadists: A Social Network Analysis of Al-Muhajiroun's Propaganda Campaign," *Perspectives on Terrorism* 6:1 (2012), and "The use of the Internet for terrorist purposes," UNODC, September 2012.

was unlikely because authorities would not be inclined to disseminate some of the drive's contents, such as numerous explosive material instructions, information about creating chloroform, and illustrated guides on surveilling, stabbing, and kidnapping.

The format for delivering access to the links was also elaborate, involving hijacked Twitter accounts that shared links to the repository in their bios. In fact, researchers noted that the links to the cache also appeared on the pro-Islamic State website "Muslim News" in the comments sections of the site.[35] Tracing the Twitter cohort of Islamic State accounts allowed researchers to study a cluster of Islamic State websites, their interconnectedness, and their links to other sympathetic accounts on platforms like Twitter and Facebook. These linkages between Islamic State supporters on Twitter and Facebook also stretched into encrypted platforms like Telegram, Hoop, and TamTam. Islamic State supporters are not the only violent extremists promoting links to archives on social media with hijacked accounts, latching onto popular hashtags, or masking content with link-shorteners. ISD researchers, for example, are currently tracking al-Qa`ida and specifically al-Shabaab archives that are likely of comparable size, and these groups may utilize similar tactics to promote and disseminate links on social media.

At least anecdotally, the cluster of pro-Islamic State accounts that led to the discovery of the "Cloud Caliphate" was aided by the 'TweetItBot' on Telegram, which allowed users to share links directly from Telegram to Twitter.[36] Researchers found numerous 'TweetItBot' tags on the Islamic State Twitter accounts collected around the time of al-Baghdadi's death. Accounts were similarly connected, as noted above, by their use of short-links in account bios. It is unclear to researchers why these accounts used this sharing tactic, placing central links to this pro-Islamic State website ecosystem in "sockpuppet" account bios. However, the practice seems to mimic techniques news outlets like Vice News use on Instagram, which promotes breaking or emerging news stories by featuring URLs in the account bio.

Using the initial links to a non-password-protected version of the cache promoted by the abovementioned pro-Islamic State accounts on Twitter, researchers gained access to what seemed to be the full extent of the 2.2 terabytes "Cloud Caliphate" repository. Researchers would periodically lose and regain access when supporters affiliated with the drive updated the numerical section of the short link used to direct audiences to the cache. From June 2020 through October 2020, ISD researchers created an automated program to scrape the cache, downloading and collecting the primary data and corresponding metadata on more than 90,000 pieces of content stored in the drive. While some of the data was readily accessible files, researchers also found thousands of zip and disk image files. Using the system designed to scrape the site, researchers opened these files and found that beyond the primary data found in the folders were secondary sets of data in zipped files of previously taken down websites, old Islamic State Arabic learning applications, and other tools. Drawing on files, metadata, and content from the cache, researchers began piecing together the story around its development, maintenance, and place in the online ecosystem of Islamic State supporters. Though the broader research initiative into the cache is ongoing, this product offers an analysis that speaks to the archive between October 2019 and February 2021.

Given the size of the "Cloud Caliphate" and the sheer scope of its contents, no one research method is suitable for preliminary analysis on this resource. Consequently, the authors opted to use a mixed-methods approach to explore different aspects of the cache while demonstrating some of the ways digital archives might inform researchers, practitioners, and policymakers in the future. The following section offers a multi-part analysis on the "Cloud Caliphate."

35 "Muslim News" has had a long-standing duel with takedowns since 2016, and its creator(s) have subsequently learned to buttress its existence online by using multi-top-level domain copycat sites that can be activated once the site is booted off one service.

36 The 'TweetItBot' on Telegram supported the direct sharing of content from Telegram to Twitter.

Analysis of the "Cloud Caliphate"

The "Cloud Caliphate" sits centrally amongst a set of Islamic State websites ISD researchers have tracked on the open web over the past three years. Functioning as the archive of choice for a series of Islamic State websites built by the same support organization, it serves as a means to keep the memory of the "caliphate" alive. Even though password-protected, researchers were able to gain access to the cache's full content through a series of links shared through a phalanx of "sockpuppet" social media accounts promoting it as the "largest Islamic State archive."

Since October 2019, researchers have analyzed the content and monitored the cache's traffic, distribution, and connections to networks of Islamic State support groups clawing their way back onto Telegram while settling into new climes on platforms like Hoop Messenger. There appears to be a decentralized network of accounts sharing links to the cache, however, the site's administrators seem to be a relatively centralized hub of supporters, building new pro-Islamic State websites, uploading and organizing content, and promoting the resource across an array of platforms. Researchers are still working to determine whether the repository's administrators have operational connections to the Islamic State and its media apparatus. The original title of the "Cloud Caliphate" suggests that the repository is supporter-driven, but that alone does not prove or disprove formal ties to the Islamic State. In any case, this matter receives more attention in subsequent parts of the analysis.

Since at least 2017, the Islamic State supporters maintaining the resource have curated and stored the "Cloud Caliphate," which contains more than one terabyte of video and audio content from various Islamic State media outlets. For context, that is roughly around the same amount of content as streaming 400 hours of high-definition video on Netflix—into a cloud-based storage drive.[37] The cache appears to be more extensive than other Islamic State online repositories—for years, Islamic State supporters have been using Google Drive, Dropbox, JustPaste.It, and Archive.org as means to store and share propaganda—it is central to a series of standalone pro-Islamic State websites, Hoop and Telegram channels, and is possibly fueling a resurgence of support for the group on social media platforms such as Facebook and Twitter.[38]

1. Describing the Composition of the "Cloud Caliphate"

The cache's content is vast: On June 30, 2020, for instance, the cache held 97,706 folders and files. To put this in context, that amounts to nearly three times as many pieces of content disrupted in the EUROPOL anti-Islamic State campaign on Google, Twitter, Instagram, and Telegram in November 2019.[39] During the time Islamic State supporters and outlets were reeling from the EUROPOL disruption, the cache was unaffected, and was, in fact, growing in size. Another way to understand the cache's size is to compare it to other virtual or physical drives. The "Cloud Caliphate" repository holds about 75 percent more data than all the devices seized during the May 2011 raid on Usama bin Ladin's compound, including five computers, multiple mobile phones, 100 USB drives, DVDs, and CDs.[40]

So far, the content researchers have analyzed provides an understanding of the cache's curation, types of content hosted on the site within its folders, the top-level metadata contained within the content,

37 Researchers are obfuscating and withholding the name of the storage drive in order to avoid driving traffic to the site.

38 Researchers have tracked the "Cloud Caliphate" to Hoop and Telegram channels, and have found it linked on key Islamic State support websites on the open web. The cache's connections to Facebook and Twitter have been tracked by researchers to Islamic State-supporting social media accounts on both platforms. This was further corroborated by website analysis tools that provided some indication of referrals from social media platforms such as YouTube, Facebook, and Twitter. Researchers have found links to the cache on Facebook and Twitter, yet have been unable to find the links on YouTube.

39 Amarasingam, "A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit."

40 "National Geographic Announces In-Depth Analysis of Osama Bin Laden's Newly Declassified Personal Files in BIN LADEN'S HARD DRIVE Special," Business Wire, August 3, 2020.

and the primary languages of the content in the cache. For 10 months, there were 24 primary folders within the cache: *Recent Content*, *Archives of the Genesis of the Islamic State*, *Archives of the Emirs of Jihad*, *Archives of the Chants of the Caliphate*, *Archives of al-Bayan Radio*, *Archives of al-Furqan Media*, *Archives of the Old States*, *Archives of al-Amaq Bulletins*, *Archives of Military Sciences*, *Archives of the Wills of the Martyrs*, *Archives of al-Nabaa Newsletter*, *Archives of the Scholars of Jihad*, *Archives of the Fatwas over the Airwaves*, *Archives of Himmah Library*, *Content of the Caliphate's States*, *Photo Stories*, *Quran for the Mujahideen*, *Supporter Groups*, *The Islamic State Curriculum*, *Non-Arabic Content*, *Single Pieces of Content*, *Sarh al Khalifah*, *Content for the Holy Month of Ramadan*, and *Various Content*. In November 2020, administrators added three new folders: a backup folder for the Anfal radio website, a folder dedicated to the adjustments of the Islamic State-linked media outlet Itisam, and a conspicuous folder dubbed "*specific to Abu Muhammad*."

Within these primary folders are 58,898 image files, 10,092 video files, 9,038 applications (such as the infamous mortar-firing Arabic learning app for Islamic State children, and a turn-of-the-millennium al-Qa`ida website), 8,963 audio files, 7,728 files of unknown and outdated formats, and 2,972 text files. This content stretches back to Abu Musab al-Zarqawi's leadership when the group was called al-Qa`ida in the Land of the Two Rivers, also known as al-Qa`ida in Iraq (AQI), which became part of the Mujahideen Shura Council of Iraq. Such content has been shared previously on encrypted platforms like Telegram, but after al-Baghdadi's death, supporters disseminated the cache on more mainstream social media platforms. Before finding the link to the open cache, researchers could access some content in the archive, but not the full extent of the drive. By cracking the numerical code provided through the short links, researchers could access the drive as it changed, grew, and ultimately shifted its presence to a new URL. By providing top-line data from the annals of this Islamic State digital archive, which seems to be the most expansive to date, researchers gleaned several important takeaways from how supporters perceive the group's founding, its ideology, its primary ideologues and those in their ambit, as well as the group's support network and its territories prior to 2017, and now. In other words, like with the study of any archive, examining this cache provides a window into the kinds of content Islamic State supporters thought were worth saving for future generations and the types of content that constitute what it means to be part of the in-group.

2. Discussing Evidence Concerning Cyber Support

Researchers believe the cache is tied to a digital support group named Sarh al-Khilafah, the *Tower of the Caliphate*. The group's name is likely derived from a 2016 Islamic State al-Furqan media release by the same name, which was a detailed 15-minute video outlining the Islamic State's territories at the time, as well as its administrative and organizational structures.[41] The administrator(s) for Sarh al-Khilafah appear to operate a Telegram bot, which disseminates portions of the cache folder-by-folder, and a now-defunct Hoop channel of 1,474 members, which was created in April 2020 and removed by the site in September 2020. Researchers found numerous .txt files titled "readme" in several of the folders in the cache that seemed to link the drive to the Sarh al-Khalifah group. Conventionally, .txt files are non-defined text files that can be accessed and opened using a range of different file editors, such as Microsoft Word or WordPad. Sarh al-Khalifah's site usage has a similar platform use pattern as The Electronic Horizons Foundation: at the time of writing this report, both groups used NextCloud and the druager.de messaging application. It is unclear, however, if the connections go beyond the use of the same platforms and a suite of similar applications to support their online presence.

What is evident, however, is Sarh al-Khalifah's linkages to a recently redesigned al-Bayan radio website, which provides live streaming services of Islamic State radio content, and links to the group's Hoop and Telegram channels in its "about us" section. Al-Bayan was rebranded last year as al-Anfal

41 Enab Baladi, "Sarh al-Khalifah… 'the Islamic state' explains its states' and organizational structure," Enab Baladi, accessed on July 7, 2016.

Radio, but it still carries the URL associated with al-Bayan. The site directly links to all but one of the primary folders available in the cache. Sarh al-Khalifah has similar connections to another site, "The Punishment," a pro-Islamic State supporter website that has transitioned its top-level domains eight times during eight months in 2020. A fake Netflix account on Twitter advertised "The Punishment" site on March 24, 2020, as a means to "watch realistic and enthusiastic films" to "show who will rule the world after this corona COVID19." The site's navigation bar has a drop-down menu under the heading "plus+" that allows users to visit a page on the site called "important links." The page has a similar format as the Al-Anfal website and links to nearly every primary folder of the cache, leaving out the URL to only one folder. The drop-down menu similarly links to the Hoop and Telegram channels previously manned by Sarh al-Khalifah.

These standalone platforms are primary referral nodes to the cache. Researchers have been monitoring the sites since finding the "Cloud Caliphate." The investigation into these standalone websites, such as "The Punishment," al-Bayan radio, and "Muslim News," shows that they function as funnels for users to access the cache. This constellation of websites, which on the surface seem like separate propaganda projects by disparate Islamic State supporters, are part of an intricate ecosystem of Islamic State support on the open web. The sites link or feed into one another in different ways, but they all seem to provide differing functions. While "The Punishment" is a virtual video bank of Islamic State content, "Muslim News" functions as an aggregator and archive for news bulletins and beyond. The al-Bayan and al-Anfal radio sites are distinct in their audio offerings and are perhaps the most sophisticated because they have a streaming service with downloadable audio playlists curated by Islamic State. The cache takes this one step further, functioning as an Islamic State archive—much like a virtual Library of Congress—it allows users to access the continually updated content curated by supporters to keep official Islamic State media in continuous circulation online. It sits dead center in this constellation of sites. (See Figure 1.)

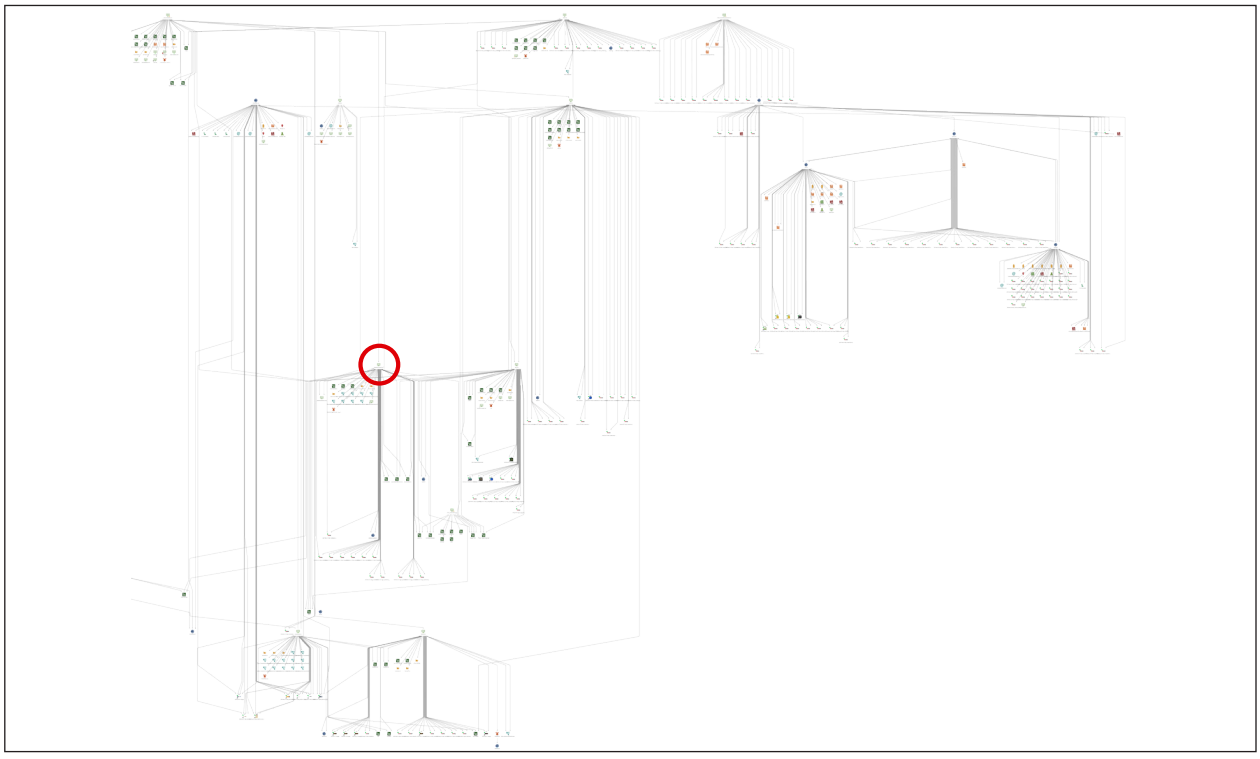

Figure 1: The circled part of this graphic highlights the position of the "Cloud Caliphate" cache amidst a broader constellation of notable Islamic State sites.

Utilizing SimilarWeb,[42] a proprietary website analysis service that provides traffic, social media engagement, and referral metrics data, researchers found that the top-three referring websites to the cache were al-Bayan, "Muslim News," and "The Punishment." These sites accounted for 46 percent, or 5,514 visits, of all referral traffic into the cache from May through July 2020. While "Muslim News" is not directly linked to Sarh al-Khalifah, across hundreds of separate pages on the site that date back to August 23, 2014, links to the cache are peppered into the comments sections on those individual pieces of content. ISD research has previously evaluated the site traffic and its persistent presence on a Malian top-level domain since 2014.[43] "Muslim News" experienced a significant traffic boom during the start of the global pandemic lockdown period from March to May 2020, receiving on average 181,840 site visits per month, and accumulating 543,500 visits over those three months.[44]

These three standalone platforms show the interconnected nature of Islamic State support groups on the open web. They also showcase the centrality of the "Cloud Caliphate" cache and Sarh al-Khalifah as aggregators for legacy and current Islamic State content online. Understanding what the repository holds, beyond its connections to support groups and sister websites, required researchers to delve further into its content. Since identifying the resources, researchers have set up digital monitors and scraped the site's content to gather more granular data about its stores. While content analysis is ongoing, this series of notable findings provide the national security community and terrorism researchers insight into the use of archives as central features of violent extremists' online activity.

3. Exploring the Genesis Files

The archive's folder on the *Genesis of the Islamic State* splits into two sub-primary folders, one called Jama'at al-Tawhid wal-Jihad (JTJ, or the Society for Monotheism and Jihad) and the Mujahideen Shura Council of Iraq.[45] Abu Musab al-Zarqawi founded JTJ, and the group was subsumed by al-Qa`ida in Iraq in 2004 under the official name Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn. The Mujahideen Shura Council of Iraq was the umbrella organization that hosted the al-Qa`ida group, and it "was designed to put an Iraqi face on al-Qa'ida's efforts in the insurgency."[46] These two folders contain 60 videos from both organizations, all of which are primarily of hostages, attacks on various Iraqi, American, and British civilians and forces, as well as JTJ's announcement of al-Zarqawi's and other ideologues' deaths.

The folders represent a minuscule portion of the overall breadth and depth of the cache but indicate the importance of tracing the origins of the Islamic State to these two groups. They also show how much content currently exists online in relation to the two groups and their video media outputs, much of which was previously limited to legacy salafi-jihadi message boards and websites. Research into the Islamic State's central media department's development has delved into the rudimentary nature of the media apparatus used by JTJ and the Mujahideen Shura Council at their birth.[47] The hour-long "Winds of Victory" video, for example, features a montage of attacks, opening with blowing wind sound effects and graphics of a breeze, followed by the bombing of Iraq during the "shock and

42 SimilarWeb is a proprietary service and hence does not provide detailed information on how it culls traffic to websites. The service claims to be General Data Protection Regulation (GDPR) compliant.

43 Moustafa Ayad, "Pilgrimage to the platform: The repeat audience for 'Muslim News,'" Global Network on Extremism & Technology, March 9, 2020.

44 Ibid.

45 "Image commemorating Jama'at al-Tawhid wal-Jihad fighters," Militant Imagery Project, Combating Terrorism Center, United States Military Academy at West Point.

46 Joseph Felter and Brian Fishman, *Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records* (West Point, NY: Combating Terrorism Center, December 2007).

47 Whiteside.

awe" campaign overlaid with bold red text saying "democracy."[48] Shoddily captured footage of suicide bombers follows, including the reading of their wills. At its core, the content does represent a critical starting point for how the Islamic State would frame its messaging, primarily around attacks and gruesome executions that highlight their core socio-political grievances. While the *Genesis of the Islamic State* folder corresponds with the modern-day historical reading of the Islamic State's rise, much of the group's media warrants further analysis. As compared to the cache's initial 1.3 terabytes of content, these two groups make up a little more than .15 percent of its overall content.

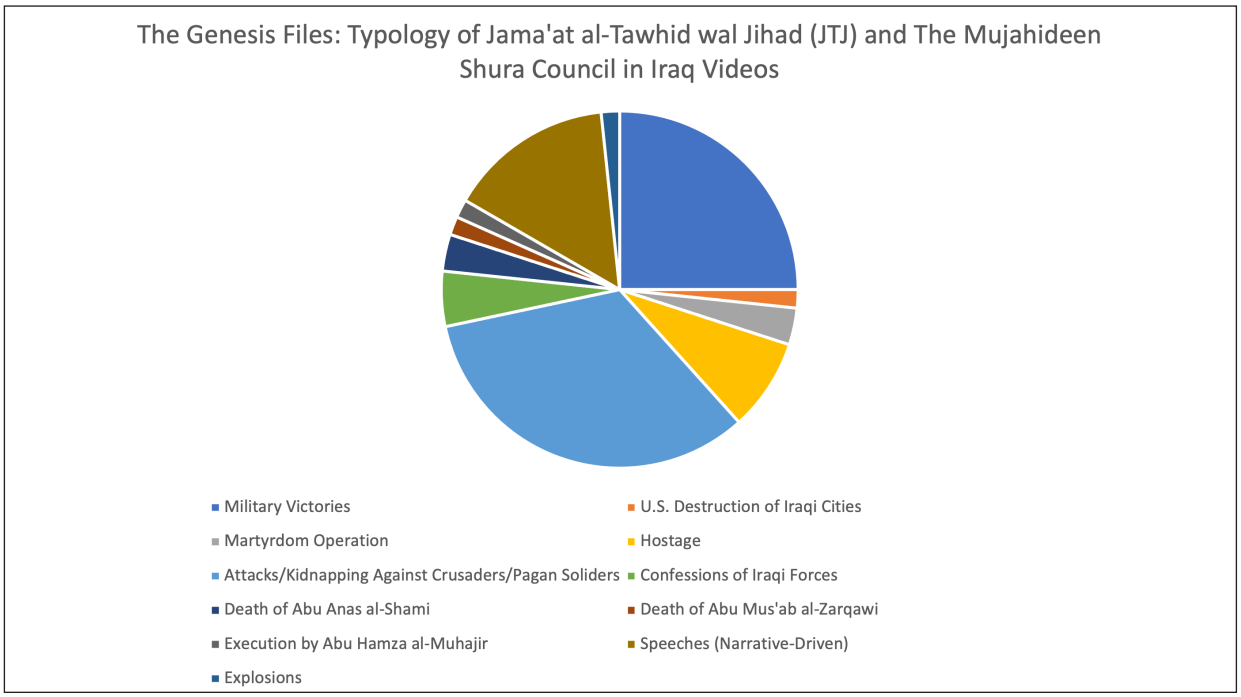

Figure 2: This chart shows the breakdown of themes highlighted withing the 'Genesis of the Islamic State' folder.

4. Exploring the Ideologues Files

Pivoting to the *Ideologues Files*, it is important to note the subject of acceptability of several al-Qa`ida figures in the cache, specifically Ayman al-Zawahiri and Usama bin Ladin. However, in the same vein, it is similarly vital to mention the disdain for the group's current leadership found in the content, and the schism that erupted between the two factions appears to have affected the developers of the cache. The version accessed by researchers over the past 10 months has featured a folder, innocuously named *New Folder*, which houses a virtual treasure trove of slanderous material meant to discredit al-Qa`ida, its affiliates, and the group's leadership, specifically al-Zawahiri. This *New Folder* contains 472 video and image files, 76 PDFs, and a single Word document. The PDFs consist of the case against al-Qa`ida and al-Zawahiri. According to file timestamps recorded by the file-hosting software, the drive has a meticulously curated folder of 272 social media posts that date back to 2015. Eight PDFs and three pieces of audio content specifically use al-Zawahiri's name in the title. Of those files, most are response documents from former Islamic State spokesmen: Abu Muhammad al-Adnani and one by

48 Please note, researchers accessed the "Winds of Victory" during their analysis of the drive's content.

Abu Maysarah al-Shami,[49] also known as Ahmad Abousamra,[50] the Syrian-American editor-in-chief of the Islamic State magazine Dabiq.

The *New Folder* contains crude, ready-made responses to notable salafi-jihadis on social media, such as Shaykh Hani al-Sibai, the controversial Egyptian cleric in Britain who was on U.S., E.U., and U.K. sanctions lists for links to al-Qa`ida.[51] One piece of content is a Twitter reply to an al-Sibai post from September 2015, when he posted, "there is no mujahid university/movement that have a state or Caliphate. Al-Baghdadi has claimed a Caliphate but he should have at least freed Jerusalem." The response to al-Sibai on Twitter at the time was "the greatest Caliph was Abu Bakr al-Siddiq and he didn't liberate Jerusalem." This salafi-jihadi schism highlighted on a micro-level in the al-Sibai Twitter post and response is repeated in the numerous curated posts attacking al-Qa`ida-linked ideologues, affiliates, and their statements. Al-Sibai was added to a 35-person kill list by an Islamic State support group called al-Battar.[52]

5. Exploring the Scholars of Jihad Files

Abu Muhammad al-Maqdisi has been one of the more notable salafi-jihadi scholars for several years. Numerous academic articles and books have noted al-Maqdisi's outsized influence on a community of jihadi thinkers and ideologues that have either been his pupils or were influenced by his writings. Recently, however, a range of salafi-jihadi groups in Syria and Iraq have challenged and refuted al-Maqdisi's influence.[53] One researcher noted that al-Maqdisi, "like many al Qa'ida-allied thinkers, objects to the Islamic State, especially its uncompromising approach to power politics within the jihadist world."[54] In the same vein, other scholars have stated, "although there is no one who has likely eclipsed al-Maqdisi's influence, it does not make sense anymore to say that al-Maqdisi is the most important jihadi ideologue in the world today when two of three jihadi poles are against him."[55] That is clear from the content contained within the folder demarcated as the *Scholars of Jihad* in the cache. (See Figure 3.) Understandably, al-Maqdisi has a lackluster showing amongst the *Scholars of Jihad* as curated by Islamic State supporters. Well-known salafi-jihadi scholars like al-Maqdisi, at least those who generally receive attention and commentary from like-minded violent extremists, are in the lower 10 slots of content attributed to them in this cache.

49 "Most wanted terrorist: Ahmad Abousamra," Federal Bureau of Investigation, U.S. Department of Justice.

50 Paul Cruickshank, "ISIS lifts veil on American at heart of its propaganda machine," CNN, April 7, 2017.

51 Rachel Bryson, "How six Islamist ideologues shaped jihadi activity in Britain," Tony Blair Institute for Global Change, October 3, 2017.

52 "ISIS launches campaign calling to kill prominent Islamic clerics such as Yousuf al-Qaradawi, Saudi Mufti 'Abd Al'Aziz Aal Al-Sheikh, former Egyptian Chief Mufti 'Ali Gum'a," Middle East Media Research Institute (MEMRI), February 14, 2017.

53 Aaron Zelin, "Living long enough to see yourself become the villain: The case of Abu Muhammad al-Maqdisi," Washington Institute for Near East Policy, September 9, 2020.

54 Thomas Joscelyn, "Al-Qaeda uses ISIS to try to present itself as respectable, even moderate," Foundation for the Defense of Democracies, February 13, 2015.

55 Zelin, "Living long enough to see yourself become the villain: The case of Abu Muhammad al-Maqdisi."

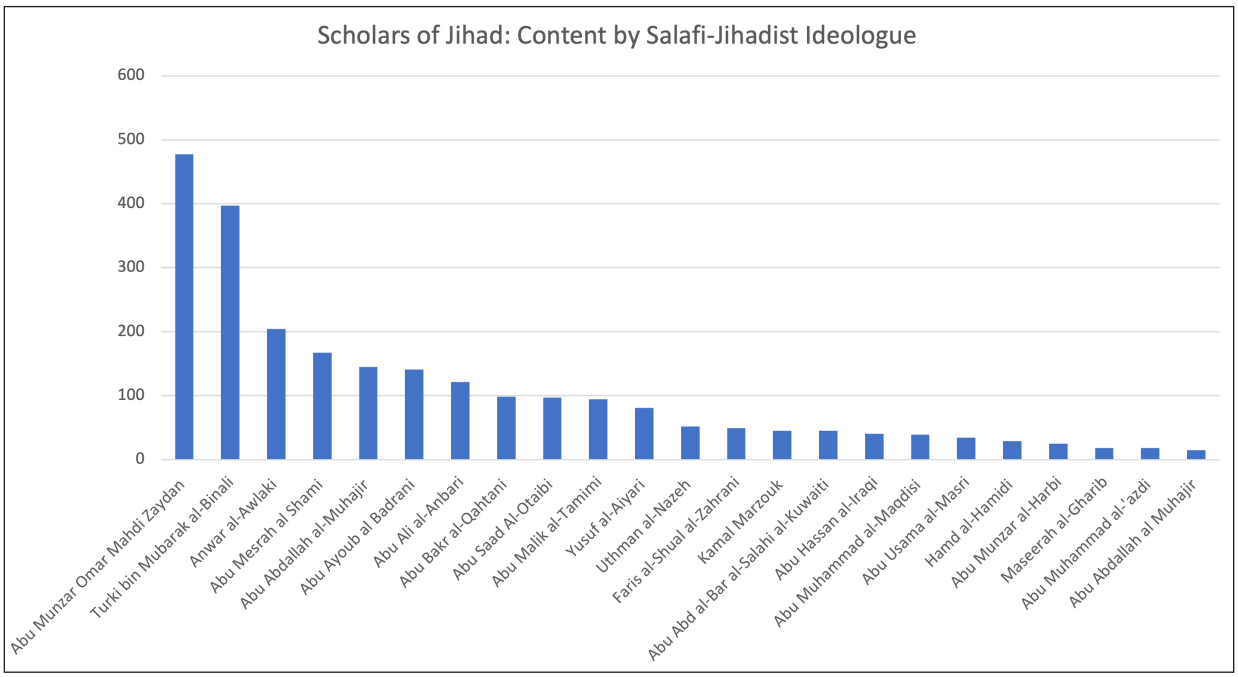

Figure 3: This graph shows the amount of content per ideologue sub-folder in the 'Scholars of Jihad' folder.

The late 'Umar Mahdi al-Zaydan, a Jordanian and former colleague of al-Maqdisi, finds himself in the frontrunner position in terms of the content attributed to him and stored in the cache.[56] Little is written on the Irbid native's works, other than his siding with the al-Zarqawi wing of salafi-jihadis in Jordan and joining the Islamic State's ranks. For a time, he was supposedly a potential spokesperson replacement for Abu Muhammad al-Adnani after al-Adnani was killed. Al-Zaydan was reportedly killed in 2017 in Mosul, and beyond the fractious relationship with his peer al-Maqdisi, researchers know relatively little about the man.[57] Understanding al-Zaydan's life, ideology, and impact on the salafi-jihadi movement is arguably key to understanding the schism between ideological counterparts-turned-rivals. Content tied to al-Zaydan, Turki bin Mubarak al-Binali, and Anwar al-Awlaki make up 31 percent of the *Scholars of Jihad* folder. Al-Binali, a Bahraini who reportedly served as the head of the Islamic State's scholarly research body, was believed to be relatively close to al-Baghdadi, though al-Binali and his associates had tense relations with other Islamic State members due to ideological differences.[58] Al-Awlaki, meanwhile, is regarded as "al-Qa'ida's most effective English-language recruiter."[59] Though al-Binali and al-Awlaki are different figures in many ways, both are known in terrorism studies circles and media because of their influence on their respective movements.[60]

56 Joas Wagemakers, "The concept of bay'a in the Islamic State's ideology," *Perspectives on Terrorism* 9:4 (2015).

57 Joas Wagemakers, "Jihadi-Salafism in Jordan and the Syrian conflict: Divisions overcome unity," *Studies in Conflict & Terrorism* 41:3 (2017).

58 Cole Bunzel, "Ideological Infighting and the Islamic State," Perspectives on Terrorism 13:2 (2019); Cole Bunzel, "The Islamic State's Mufti on Trial: The Saga of the 'Silsila 'Ilmiyya,'" CTC Sentinel 11:9 (2018).

59 Scott Shane, "The enduring influence of Anwar al-Awlaki in the Age of the Islamic State," *CTC Sentinel* 9:7 (2016).

60 "Who tells ISIS fighter's they are doing God's work?" CBS News, January 28, 2015; Shane.

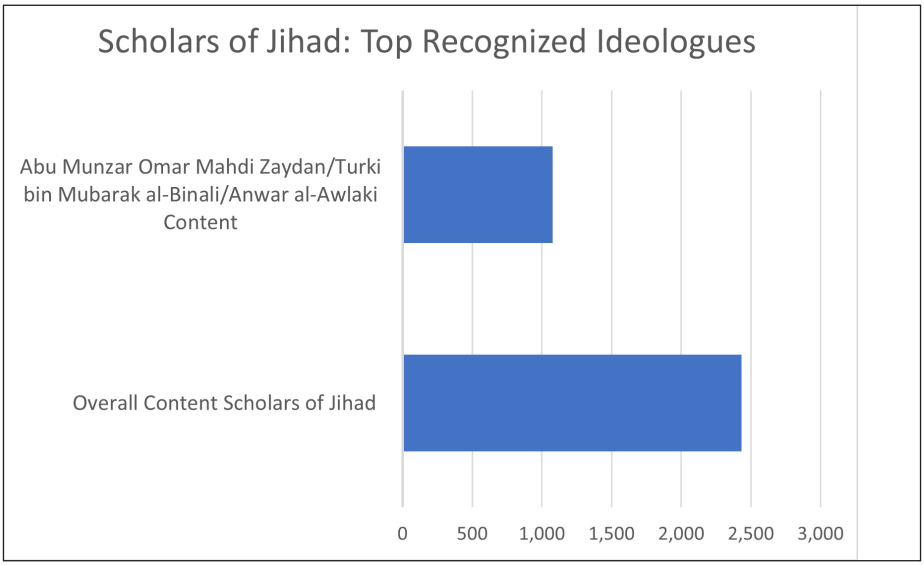

Figure 4: This graph shows the amount of content attributable to Abu Munzar Omar Mahdi Zaydan, Turki bin Mubarak al-Binali, and Anwar al-Awlaki (1,078 pieces of written, audio, and video content) in comparison to all of the content attributable to all of the ideologues in the 'Scholars of Jihad' folder.

6. Exploring the Emirs of Jihad Files

By creating a distinction between scholars of jihad and emirs of jihad, the creator(s) of the cache have disaggregated leadership from salafi-jihadi scholar influence. The folders for Usama bin Ladin, Abu Musab al-Zarqawi, and Abu Muhammad al-Adnani are by far the most flush with content within the cache. However, the ability to understand the Islamic State from its origins requires an understanding of its leaders and their visions that set the tone for its eventual rise in 2014, such as Abu Abdallah al-Jabouri and Abu Anas al-Shami. Scholars have recently delved into the past of the movement around the Islamic State, citing some of the most notable speeches and content produced by its predecessor groups.[61] Biographical data of some of these predecessor ideologues, however, has been limited. Within the cache, each of these ideologue folders contains a *seerah*, or "prophetic biography," sub-folder, demonstrating the level of organization and curation within this part of the drive. Unlike the *Scholars of Jihad* folder, the biographical accounts of these ideologues were deliberately curated with video *seerahs*. These *seerahs* were produced by the Islamic State-linked media outlet al-Battar, named after a sword wielded by the Prophet Mohammad.[62] Only three of the emirs do not have video *seerahs*: Abu Muhammad al-Adnani, Usama bin Ladin, and Hamza al-Qurayshi.

61 For more context, see Haroro Ingram, Craig Whiteside, and Charlie Winter, *The ISIS Reader: Milestone Texts of the Islamic State Movement* (New York, NY: Oxford University Press, 2020), and also Fishman.

62 The al-Battar sword is an often used as a reference by salafi-jihadis. The sword is erroneously ascribed to having a potential role in defeating the coming of the Antichrist.

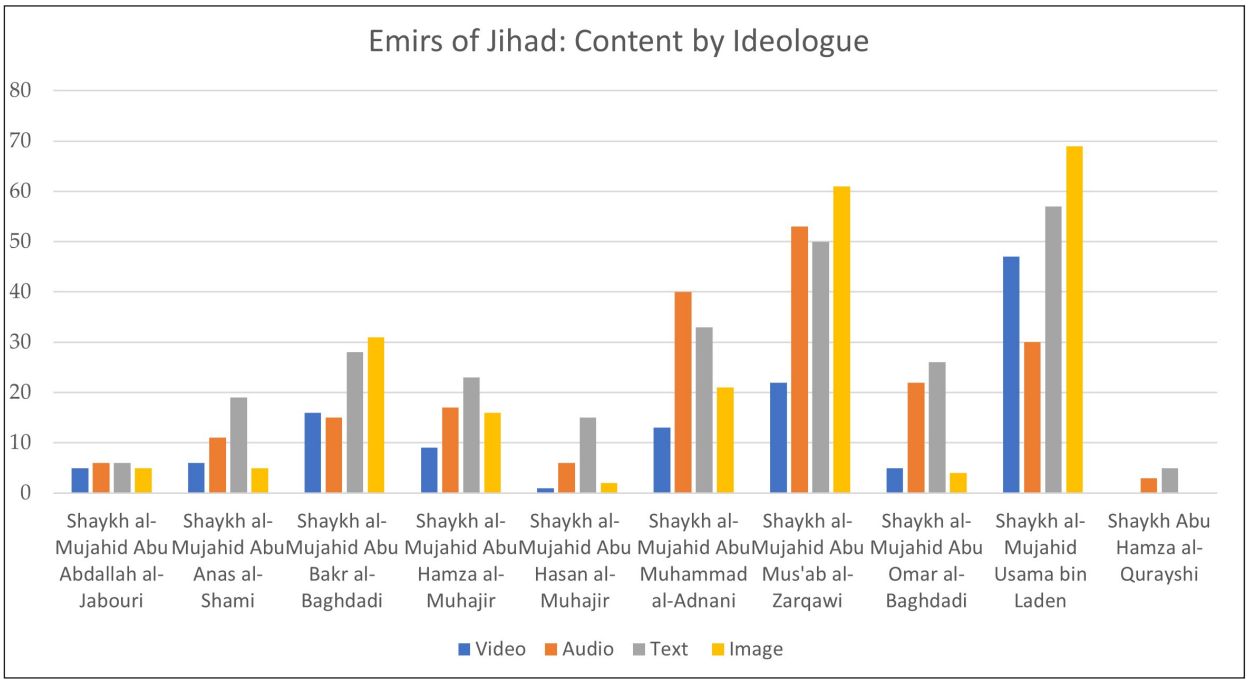

Figure 5: This graph shows the amount of content attributable to each 'Emir of Jihad' in the sub-folders contained in the 'Emirs of Jihad' folder.

Both al-Jabouri's and al-Shami's *seerahs* speak to an era where there was a focus on building consensus among jihadis in Iraq to fight the invasion, as well as a concentrated effort to present them as Ba'ath dissidents that were both religious scholars and intellectually strong.

Born in a farming town in Salah el-Din Province, al-Jabouri grew up salafi, and dismissive of the "perversions" that were rampant in society. He majored in law at Saddam University, later rebranded as the University of the Two Rivers, and led an "uprising" against the Ba'athists, establishing a mosque on the campus. He, the *seerah* goes, had lots of followers and students, and while working on his Ph.D. was harassed and threatened by the Ba'ath party, later imprisoned and tortured in the process. Released from prison, he began amassing weapons and men, forming a jihadi group called Sarayat al-Jihad al-Islamiyya. He never pledged allegiance to a specific group, preferring to state "he was a servant to the jihad and mujahideen."[63] Al-Jabouri was key to establishing the Mujahideen Shura Council (MSC) of Iraq, and became the official spokesperson of the Islamic State of Iraq (ISI), one of several predecessors of the Islamic State movement. He was later killed in a bombing campaign in 2007.

63 "The seerah of Abu Abdallah al-Jabouri," as accessed by researchers in the drive (video).

Figure 6: A stylized graphic of Abu Abdallah al-Jabouri from his video* seerah*, contained in the cache.

Al-Shami was a Palestinian who grew up in Kuwait. He was trained in classic Arabic at the age of 14. According to his *seerah*, al-Shami was known for having patience and leniency with those who had been previously led astray and considered outcasts of society. He, like many before him, had been a part of the Afghanistan mujahideen core, the "Arab-Afghans" as they were called, and trained at Farouk Camp for three months before traveling to Jordan, Bosnia, and then eventually back to Jordan, where he was arrested while working for a religious center in Marka, East Amman. Upon his release, he went to Saudi Arabia for *umrah*, where he was connected with members of JTJ, and eventually traveled to Iraq to fight alongside al-Zarqawi. He would become the head of the Shura Council, and as his *seerah* states, a "confidant and advisor" to al-Zarqawi. Like al-Zarqawi, al-Shami was killed in a missile attack by coalition forces.[64]

64 "The seerah of Abu Anas al-Shami," as accessed by researchers in the drive (video).

Figure 7: A screenshot of Abu Anas al-Shami from his video* seerah *contained in the cache.

Both *seerahs* tell researchers that it is not just the biographical sketches of the key ideologues or noted "emirs," but rather, some of the forgotten stories and integral personalities that laid the ideological and operational groundwork for the self-proclaimed caliphate.

7. Highlighting Linkages to a Real-World Case

While understanding the design, development, and dissemination of the cache throughout the period of analysis is important to researchers, it is also useful to touch on the cache's connections to real-world Islamic State cases. According to website analysis tools, thousands of people accessed the website each month: that population might include administrators, Islamic State supporters, researchers, journalists, and possibly law enforcement and intelligence personnel. Reviewing the case of one individual Islamic State sympathizer might offer some insight into how people accessed and possibly used the "Cloud Caliphate."

The case of Muhammed al-Azhari, a 23-year-old American in Tampa, Florida, charged with attempting to provide material support to the Islamic State in May 2020, offers an interesting example.[65] Leading up to his arrest in the United States, al-Azhari was reportedly working to acquire weapons and

65 "Tampa Man Charged with Attempting to Provide Material Support to ISIS," U.S. Department of Justice, May 27, 2020; "Indictment," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-cr-00206-TPB-AEP), June 23, 2020.

interested in plotting an Omar Mateen-style shooting.[66] Tracing back to 2015, while living in Saudi Arabia, al-Azhari was allegedly convicted "of possession of extremist propaganda, holding extremist views, and attempting to join a terrorist organization, namely, Jaysh al-Islam."[67] Court documents explain that al-Azhari eventually returned to the United States, and after some time in California, he settled in Tampa, Florida, in 2019 and worked at a Home Depot.[68] During al-Azhari's time in Tampa, the Federal Bureau of Investigation (FBI) became aware that al-Azhari acquired at least three firearms; additionally, he allegedly attempted to modify those weapons and unlawfully acquire others to carry out a mass shooting.[69] Court filings indicate that the FBI discovered al-Azhari's access to the "Cloud Caliphate" repository in 2020 while conducting a court-authorized search of al-Azhari's electronic devices.[70] According to court documents, prosecutors provided evidence that al-Azhari accessed the cache and "consumed [Islamic State] propaganda and news, and made a video on his phone playacting a terrorist scene."[71] Although the court filings do not explain how else al-Azhari might have used the archive, the "Cloud Caliphate" does not appear to have played a definitive role in al-Azhari's radicalization process. Even still, it is possible that al-Azhari accessed ideological material or content in the military science folder, which offers tactical instruction. ISD researchers are still reviewing publicly available court documents in the United States to check if other cases reference the archive. Ultimately, the al-Azhari case and his use of the "Cloud Caliphate" is consistent with scholarship suggesting that the internet does not serve as a "virtual training camp" so much as a compilation of "resource-banks maintained and accessed largely by self-radicalized sympathizers."[72]

Concluding Comments and Policy Considerations

In short, this report explored the potential origins of the largest storage drive of Islamic State content known to researchers at ISD and the CTC, and tracked its promotion across social media platforms through influential pro-Islamic State accounts and websites, highlighting the "Cloud Caliphate's"

66 A news article notes, "In his free time, [al-Azhari] surfed Islamic State chatrooms that offered training on making suicide belts and bombs. He looked up details of Omar Mateen's 2016 shooting attack on Orlando's Pulse nightclub and googled 'Bayshore Boulevard' and 'busy beach.' One day, he drove out to Honeymoon Island in Dunedin, then turned around and drove straight back to Tampa." Kavitha Surana, "Tampa Islamic State supporter rehearsed attach, tried to by gun before arrest, FBI says," *Tampa Bay Times*, May 29, 2020; "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, May 26, 2020, (Case 8:20-mj-01518-AEP).

67 "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), May 26, 2020; "Order of Detention Pending Trial," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), June 2, 2020; "Objection to magistrate judge's preliminary hearing decision," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 15, 2020. For more on Jaysh al-Islam, the following article explains, "On Sept. 29, at least 50 groups operating mainly around Damascus merged into Jaish al-Islam ('the Army of Islam'), thus undermining the FSA's dominance in a part of the country where it had long been considered the strongest rebel force." Hassan Hassan, "The Army of Islam is winning in Syria," *Foreign Policy*, October 1, 2013.

68 "Order of Detention Pending Trial," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), June 2, 2020; "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), May 26, 2020.

69 "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), May 26, 2020; "Government's response to motion to revoke detention order and release the defendant from custody," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 2020.

70 "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), May 26, 2020; "Order of Detention Pending Trial," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), June 2, 2020; "Objection to magistrate judge's preliminary hearing decision," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 15, 2020; "Government's response to motion to revoke detention order and release the defendant from custody," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 2020.

71 "Criminal Complaint and Affidavit," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), May 26, 2020; "Order of Detention Pending Trial," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-AEP), June 2, 2020; "Objection to magistrate judge's preliminary hearing decision," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 15, 2020; "Government's response to motion to revoke detention order and release the defendant from custody," *USA v. Muhammed Momtaz Al-Azhari*, (Case 8:20-mj-01518-TPB-AEP), June 2020.

72 In a journal article, one researcher notes: "As of today, the Internet is best viewed as a resource bank for self-radicalized and autonomous cells, which is used alongside more traditional ways of training and preparing. In many cases, jihadi Internet manuals may function as a preparation for real-life training, rather than a substitute for it." Anne Stenersen, "The internet: A virtual training camp?" *Terrorism and Political Violence* 2 (2008).

centrality to the ever-evolving and expanding ecosystem of Islamic State sympathizers online. After situating this research within broader efforts to study pro-Islamic State online activity, this report reflected on the role of digital archives in online communities and highlighted how contemporary violent extremists can benefit from such resources. Then the report described how researchers found, identified, and accessed the repository and worked to document and study its maintenance and contents. The core analysis was divided into seven parts to examine various aspects of the "Cloud Caliphate." After touching on the repository's origins, the first section described its composition, and the second discussed evidence concerning cyber support from other online actors. Then, sections three through six explored specific folders within the archive that pertain to matters concerning the Islamic State's organizational predecessors, and a range of notable leaders, ideologues, and scholars. Section seven delved into a real-world case study involving the archive. To conclude the report, this segment summarizes thoughts on the future of pro-Islamic State repositories like the "Cloud Caliphate" and raises policy considerations for stakeholders concerned by the proliferation of digital archives sympathetic to violent extremist groups.

Historically, terrorism researchers have struggled with a lack of data in the field; the groups they studied were naturally secretive and closed off. This largely shifted in the years leading up to the declaration of the Islamic State's caliphate in June 2014.[73] As social media platforms matured, a new generation of jihadis traveled to fight in countries like Somalia, Iraq, and Syria, sympathizers offered online support from afar, and the slow drip of propaganda from previous conflicts turned into a veritable flood.[74] Islamic State supporters were active across countless social media platforms, posting photos and videos of their breakfasts and their battles, touting praise for the cause, and sharing graphic video releases. This tempo gave terrorism researchers a new problem: an overwhelming amount of data that takes time and other resources to evaluate and determine which topics require more attention. In short order, research products explored many aspects of Islamic State propaganda and connections to the group's global base of supporters. English-language content and users received disproportionate attention. Knowledge gaps remain, however, and this report strives to address one such opening: pro-Islamic State digital repositories like the "Cloud Caliphate." Particularly in the face of continued efforts to combat the group online, digital archives appear to play an increasingly common role in preserving materials while sympathizers shuffle around different messengers and social media platforms. Researchers, practitioners, and policymakers alike must remain vigilant about the resurgence of this old-school but effective mode of operating. Since Islamic State supporters promote links to such archives with newer tactics that optimize content dissemination online, repositories like the "Cloud Caliphate" may be more accessible and influential than earlier digital libraries. This trend has notable implications for the future of the Islamic State's propaganda efforts.

In light of the aforementioned theoretical frame on archives and imagined communities, two features of this pro-Islamic State archive require further comment. As one reflection, the "Cloud Caliphate" repository is digital and accessible to a decentralized network, though it appears to have some type of vetting in place for administrators since the ability to curate files within the archive is limited to a few pro-Islamic State users. In other words, the structure and administrative access to the cache seem centralized, but the process of distrusting and promoting the resource is not. The use of the "Cloud Caliphate" by Islamic State supporters to expediently share and back up content recalls Mike Featherstone's suggestion that electronic archives represent a shift toward a site "facilitating immediate

73 JM Berger and Jonathon Morgan, "The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter," Brookings Project on U.S. Relations with the Islamic World, No. 20, March 2015.

74 Zelin, "The State of Global Jihad Online: A Qualitative, Quantitative, and Cross-Lingual Analysis;" Charlie Winter, "The virtual 'Caliphate': Understanding Islamic State's propaganda strategy," Quilliam Foundation, 2015; Lorne L. Dawson and Amarnath Amarasingam, "Talking to Foreign Fighters: Insights into the Motivations for Hijrah to Syria and Iraq," *Studies in Conflict & Terrorism* 40:3 (2017).

transfer" of information between countless online users, in contrast to the physical archive.[75] Moreover, unlike physical archives, the terrain of the digital archive constantly shifts as files are added, removed, and reorganized with ease, a fact noted by the researchers in the case of this particular repository.[76] In the sense that the archive seems to be controlled and curated by a few Islamic State sympathizers, not the Islamic State's official media apparatus, Appadurai's claim that "the archive is gradually freed of the orbit of the state and its official networks" with its digitization rings partially true. Even so, researchers believe the "Cloud Caliphate" may retain at least some connection with the Islamic State media operations structure because the archive's creator(s) have linkages to some websites that play more central roles in the Islamic State's surface web ecosystem. Consequently, this digital, more horizontally-produced archive still serves explicitly national ends by collectively remembering and imagining a shared national community.

As another reflection, the "Cloud Caliphate" blends the transnational capacities of social media with nationalist claims to a particular territory, and in doing so, contributes to an imagined community. As scholars Barbato, Hantscher, and Lederer claim, this imagined community blends secular/national and religious/transnational discourses.[77] The aggressive and sophisticated use of digital platforms for communication with Islamic State supporters around the globe inculcates transnational imaginings of its national unity. To clarify, the archive described here is not the only strategy supporters use to produce an imagined community: social media communication and 'pilgrimages' (in Anderson's terms) to Syria also represent critical strategies for imagining the Islamic State.[78] The archive itself is not solely used for national ends either. It contains instructional content for hijacking planes, for example, which offers tactical guidance rather than cultivating a sense of comradeship. The inclusion of a significant amount of content regarding Islamic State ideology, influential leaders, and theologians, however, alongside content representing daily life as a member of the (imagined) Islamic State, all point toward an attempt to produce a sense of national identity within a global, imagined network of supporters. In the case of the pro-Islamic State "Cloud Caliphate," the "will to archive" signifies supporters' attempts to produce a national conscience as well as a "national biography" to interpret events past and future in light of the establishment of the caliphate.

In light of these reflections, it is useful to raise some policy considerations geared toward marginalizing the influence of repositories like the "Cloud Caliphate." As a starting point, stakeholders, including policymakers, practitioners, and researchers, must understand that violent extremists' efforts to collect and share content they deem meaningful will persist and evolve in response to measures that governments or service providers impose. The expulsion of violent extremist archives and users who support or maintain them is neither possible nor necessary. However, several courses of action may progressively weaken the influence of digital repositories like the "Cloud Caliphate," minimizing their potential effects on the pro-Islamic State community. Motivated by the strategy of "marginalizing" violent extremism online, the following considerations emphasize proportionality, pragmatism, and respect for human rights and the rule of law.[79] First, relevant stakeholders must look for opportunities to identify, document, and study accessible repositories and take stock of the methods used to build, promote, and maintain such resources. In doing so, investigating parties must assume responsibility

75 Featherstone, p. 592.

76 Carl Miller, "Inside the secret plan to reboot ISIS from a huge digital backup," Wired UK, September 4, 2020.

77 Mariano Barbato, Sinja Hantscher, and Markus Lederer, "Imagining Jihad," *Global Affairs* 2:4 (2016): pp. 419-429.

78 See Benedict Anderson, *Imagined Communities: Reflections on the Origin and Spread of Nationalism* (New York: Verso, 2006), Chapter 4 on the functions of pilgrimage in imagining the nation. It is also worthwhile noting that the Islamic State's use of an archive is not altogether unprecedented. See Anderson. As a note, al-Qa`ida has also compiled similar information into archives online. See Martin Rudner, "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism: Terrorist Online Propaganda and Radicalization* 40:1 (2017): p. 13.

79 Audrey Alexander and Bill Braniff, "Marginalizing Violent Extremism Online," Lawfare, January 21, 2018; Audrey Alexander, "A Plan for Preventing and Countering Terrorist and Violent Extremist Exploitation of Information and Communications Technology in America," George Washington University's Program on Extremism, September 2019.

for protecting that data, transparency about how it was acquired, and establishing appropriate ethical parameters for the work. While researching digital archives associated with violent extremism, notable observations might offer speculation about whether a repository has command-and-control-related ties to an organization, insights on the actions of administrative versus supportive users, the structure and content stored on the archive, and the tactics used to promote access to the resource on other information and communications technology platforms.

Second, while respecting the rule of law and human rights, including freedom of expression, relevant stakeholders should look for opportunities to identify and disrupt individuals creating, administering, supporting, or using the resources for criminal, terrorism-related activities. Mirroring the tactics used by the bot-like network that was sharing the link to the cache, a Chicago native named Thomas Osadzinski programmed his computer to make Islamic State propaganda easily accessed and disseminated by other social media users.[80] Osadzinski's script was allegedly designed to "automatically copy and preserve" Islamic State media in an organized fashion. Federal authorities arrested Osadzinski in November 2019 and found more than 700 gigabytes of Islamic State material, including magazines, speeches, and videos on his computer.[81] Osadzinski's tactics mirror some of the "Cloud Caliphate" administrators' methods, though the "Cloud Caliphate" is more than 800 gigabytes larger than Osadzinski's repository. In short, the Islamic State supporters behind the "Cloud Caliphate" are also using a mix of automation and proprietary tools to disseminate links and terrorist content.

Third, stakeholders concerned with violent extremist exploitation of website services to develop repositories like the "Cloud Caliphate" must remember this problem is not new, and it brushes up against matters involving speech, internet governance, and broader criminal abuse of the Domain Name System. Without getting into the weeds, it is crucial to recognize that there are many different players involved in the affordances of the internet abused by violent extremists.[82] Registrars and registries, among other actors in the process, seem to be more reticent about making content-related decisions, at least partly because they are not involved with the publication of content and do not make determinations about what users see like some social media providers.[83] Although it is fair to ask companies to enforce their terms of service and advocate for companies to take a stance against the promotion of terrorism, many companies do not want to act as arbiters of speech.[84] Political pressure for social media platforms to take such actions, however, is much greater. At least anecdotally, violent extremists use web services because it is a relatively safe and cost-effective way to operate without the same level of interference, but they are still vulnerable to actions by law enforcement and are not untouchable.[85] Ultimately, if stakeholders do advocate for the seizure or closure of sites, they should also emphasize the documentation of such material because it may have utility to members of the counterterrorism community as a data source for researchers, evidence for law enforcement, or reference for intelligence practitioners. Human rights advocates may also find such materials useful when repositories contain evidence documenting abuse. To the extent possible, providing customers and users opportunities to appeal decisions might also be an important option for technology providers to contemplate if they take a more aggressive posture against terrorist exploitation of their services.

Fourth, relevant stakeholders, including service providers and organizations like the Global Internet Forum to Counter Terrorism, should continue exploring ways to marginalize the influence of sources

80 Jason Meisner, "DePaul student wrote computer code to help spread ISIS propaganda online, feds charge," *Chicago Tribune*, November 2019.

81 "Chicago Man Charged with Attempting to Provide Material Support to ISIS," U.S. Department of Justice, November 19, 2019.

82 For a list of examples, see Matthew Prince, "Why We Terminated Daily Stormer," Cloudflare, August 2017.

83 "Why Tucows Doesn't Take Down Domains for Website Content Issues;" Daphne Keller, "The Daily Stormer, Online Speech, and Internet Registrars," Center for Internet and Society, August 15, 2017.

84 "Why Tucows Doesn't Take Down Domains for Website Content Issues."

85 Keller.

like the "Cloud Caliphate" by focusing on the networks and tools that enable them to reach new users. As detailed in this report, researchers initially found links to the repository within the tweets and bios of Islamic State sympathizers promoting the cache after Abu Bakr al-Baghdadi's death. URLs, including those siphoned through link-shorteners and bots, are users' pathways to the "Cloud Caliphate." Arguably more than the folders, videos, and PDFs the folder contains, it is the links that flow across social media platforms and messengers with relative ease. Consequently, finding ways for these service providers to detect and curb the dissemination of problematic URLs, particularly after rallying events that might draw more uses to access specific content (like notable speeches or a eulogy), may help reduce the number of accounts navigating to repositories like the "Cloud Caliphate" in the first place.[86] In designing, piloting, implementing, and evaluating counter-extremism measures concerning moderating content and leveraging URLs, transparency and input from civil society groups and free speech advocates is essential.[87]

Building on the last recommendation, policymakers, practitioners, and researchers, including service providers and organizations that support service providers, must find and support collaboration opportunities to undercut the broader ecosystem of communications exploited by Islamic State sympathizers online. Beyond more tactical-level information-sharing partnerships, which draw a healthy amount of skepticism, there is still tremendous utility in collaborating to conduct research, facilitate training, share practices, identify challenges, and promote transparency amidst such efforts. Tech Against Terrorism and the Global Internet Forum to Counter Terrorism, for example, are currently hosting a free webinar series for tech professionals, researchers, and government and law enforcements officials covering topics such as 'Transparency Reporting for Smaller Companies,' 'Technical Approaches to Countering Terrorist Use of the Internet,' and 'Countering Terrorist Use of Emerging Technologies.' In this way, inter- and intra-sector engagements can help equip more players to marginalize violent extremist exploitation of digital platforms while inviting additional opportunities for accountability.

In sum, the "Cloud Caliphate" examined in this report is notable because of its size, accessibility, and contents, but ultimately, this repository is only one part of a complex and dynamic pro-Islamic State online ecosystem. By conducting a preliminary survey of the "Cloud Caliphate" and its contents, the authors of this report have reflected on the role digital archives play in fostering a shared identity among disparate supporters. While limited in scope, this analysis highlights observations about the organization, maintenance, and promotion of archives that curate the Islamic State's legacy and work to make that content accessible to wider audiences. As the virtual environment affords new opportunities for violent extremist groups like the Islamic State, similar recordkeeping practices will likely continue. Although stakeholders within the counterterrorism community may have differing views on how to respond to such resources, there should be some recognition that these resources are important to violent extremist groups online and offer numerous opportunities for policymakers, practitioners, and researchers.

86 To offer one example, the Terrorist Content Analytics Platform (TCAP), which Tech Against Terrorism developed with support from Public Safety Canada, helps identify and verify URLs containing terrorist content, then it alerts the companies using the TCAP about said URLs.

87 For more on these considerations and others, see Tech Against Terrorism, "The Terrorist Content Analytics Program and Transparency by Design," VoxPol, November 11, 2020.

Combating Terrorism Center

AT WEST POINT

ISD | Institute for Strategic Dialogue