www.eictp.eu

EXPERT PAPER

Dr. Ali Fisher | Dr. Nico Prucha

The Salafi-Jihadi online ecosystem in 2022

Swarmcast 2.0

July 2022

E·I·C·T·P

IMPRINT

The European Institute for Counter Terrorism and Conflict Prevention (EICTP) is a research association operating worldwide and with its headquarters in Vienna, Austria. As a non-profit institution the focus of EICTP is on key topics around security policy-related issues. It carries out projects with renowned partners in Austria and abroad, maintains close relationships with high-level research organizations and a network of prominent experts and scholars, offers profound sets of actions, consultations and strategies related to counter-terrorism, hybrid conflicts, and de-radicalization measures and aims at creating policy-related recommendations based on research and expert assessments for decision-makers.

Address:

European Institute for Counter Terrorism and Conflict Prevention (EICTP)

Esslinggasse 17/5, AT-1010 Vienna

www.eictp.eu

Media owner, editor, producer: EICTP

Place of publication: Esslinggasse 17/5, 1010 Wien

Proof-reading and formal editing: EICTP

Graphic Design: Citypress GmbH

Print: Citypress GmbH

Contents

Summary

In 2022 the Media Mujahidin - the media operatives who work on and offline in support of Salafi-Jihadi groups – have continued to maintain a persistent presence online and conduct influence operations amongst their primary, Arabic speaking, target audience.

This contrasts significantly with the dominant narrative which has been presented by both the transatlantic orthodoxy of Terrorism Studies and the trade associations backed by big social media platforms. That 'success' narrative claims Salafi-Jihadi groups, such as IS and AQ, have successfully been forced to use smaller or fringe platforms. These small and micro-platforms are targeted – so the narrative goes – because they lack the capacity of large tech platforms to build and maintain automated content moderation algorithms, and instead have to rely on slower human moderated systems.

However, as this article demonstrates, the Salafi-Jihadi movement has continued to exploit many of the biggest social media platforms, including WhatsApp with a userbase of around two billion accounts. In addition, the Media Mujahidin have continued to expand their reach by adopting a multiplatform communication paradigm, giving potential sympathisers many avenues with which to engage with their content.

Media Mujahidin have achieved a persistent presence despite the ongoing efforts to disrupt their communication, due to the speed, agility and resilience of their networks coupled with the willingness to embrace emergent behaviours and web3 technology. This is the Swarmcast2.0.

As technology continues to develop, the modus operandi of the Media Mujahidin evolves with it. A Web3-enabled Swarmcast2.0 has arrived. Swarmcast2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than the original version which emerged by 2014.

If Terrorism Studies and policy makers continue to buy into the 'success narrative', rather than grasp the increasing complex constant evolution of the Swarmcast2.0 there is an increasing risk that disruption efforts will be using Web 2.0 approaches in a Web3 world.

Key Findings

The relationship of Web 1.0 to the Web of tomorrow is roughly the equivalence of Pong to The Matrix

Darcy DiNucci, 1999

This paper adopts the progressive approach to Terrorism Studies, which focuses on an evidence-based analysis, in this case examining the purpose, strategy and tactics of the Media Mujahidin. It examines the recent evolution of the Salafi-Jihadi information ecosystem including the adoption of Web3 and the emergence of the Salafi-Jihadi Swarmcast2.0.

The paper demonstrates:

1. **The emergence of Web3 significantly (if not completely) undermines the current approaches to disrupt the online activity of the Salafi-Jihadi movement.**

    - The Salafi-Jihadi movement and specifically al-Dawlat al-Islamiyah (IS) have already adopted Web3 technologies.
    - The Web3 technology currently in use already represents a significant circumvention of existing tactics and techniques intended to disrupt their online activity. From EthLink and IPFS pinning, to the integration of onion links which underpin the strategy to deliver a resilient surface web distribution infrastructure, Web3 is already in use.
    - With the advent of Web3, the current approaches to content removal may be a necessary clean-up of Web2.0, but no longer represent a viable strategy to disrupt the activity of the Media Mujahidin.

2. **The multiplatform communication paradigm (MCP) adopted as part of the Salafi-Jihadi Swarmcast2.0 has created a network of significant resilience, vastly outstripping that which existed during the short period of time when the multilingual Salafi-Jihadi movement was heavily reliant on Twitter.**

    - Social media users on average use 7 platforms each month. Adopting a multiplatform strategy provides the Salafi-Jihadi movement with multiple entry points to reach their target audience.
    - While the core of the Salafi-Jihadi movement communicates through Telegram, the existence of multiple platforms mitigates against the disruption on any single platform, as users can redirect their attention elsewhere.
    - Platforms which act as the primary ‘beacons’ within the Swarmcast2.0 are Telegram, Rocket, and Matrix, while many second-tier networks exist that belong to the so-called tech giants and comparative newcomers.

3. **The current ‘success narrative’ produced by the transatlantic orthodoxy of Terrorism Studies (OTS) has overstated the effectiveness of contemporary disruption efforts.**

- The OTS refrain that accessing Salafi-Jihadi content requires having access to Telegram or an old Jihadi forum, is not supported by the available evidence.
- An evidence-based approach contradicts the claims that Salafi-Jihadi groups have been forced off tech giants such as Facebook and Twitter onto smaller platforms.
    - Despite the significant resource and effort expended by larger platforms, Salafi-Jihadi networks and content are easily identifiable on all four of the biggest social media platforms, i.e., Facebook, Instagram, YouTube and WhatsApp.
    - Twitter has strong name recognition amongst policymakers and OTS researchers. However, due to the changes in the tech landscape, some of the so-called ‘smaller’ or ‘niche’ platforms used by the Salafi-Jihadi movement now have significantly bigger userbases than Twitter.

Conclusion

- A Web3-enabled Swarmcast2.0 has arrived. Swarmcast2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than the original version which emerged by 2014.
- Swarmcast2.0 circumvents or renders obsolete many of the current tactics intended to disrupt the online activity of the Media Mujahidin.
- The need for a strategic level approach to disruption, and collaborative strategies, are increasingly pressing and can no longer be held back by the comfort and reassuring rhetoric of the OTS ‘success narrative’.
- The future of disruption efforts requires a Web3 strategy. The risk posed by relying on Web 2.0 disruption approaches in an increasingly Web3 world, approaches the equivalence, to lean on Darcy DiNucci’s analogy, of planning to play Pong but finding yourself in *The Matrix*.

Introduction

The Salafi-Jihadi movement has to date maintained a persistent presence for its networks and content despite the pressure from governmental organisations, the efforts of the tech sector and active attacks from other online groups including cyber-divisions of Shia militia groups.[1] The Salafi-Jihadi movement has achieved the persistent presence because "the movement can leverage collective behaviours across multiple platforms to maintain a persistent presence for their content".[2] This is the Swarmcast, which combines the speed of dissemination, the agility of users and the resilience of network structures. In many ways the Media Mujahidin and supporters of Salafi-Jihadi groups more broadly have been early adopters of technologies and platforms within their multiplatform communication paradigm (MCP) which have enabled them to remain many steps ahead of disruption efforts.[3]

For over 20 years, the activity of the Media Mujahidin has been in a state of constant evolution as their multiplatform zeitgeist has continued to reconfigure.[4] Having been pioneers in using electronic communication, the Media Mujahidin are an established side of any real-life conflict and became of greater importance with the wars in Afghanistan 2001 and Iraq 2003. As of now, Salafi-Jihadi groups have already fully embraced many of the characteristics of Web3, including decentralisation, in a self-governing distributed and robust multi-server, and multiplatform network.

While the Media Mujahidin have been forging ahead, exploiting new technologies and approaches, many researchers and 'embedded academics' in the transatlantic orthodoxy of Terrorism Studies have perpetuated a 'success narrative' about the online efforts against Salafi-Jihadi groups.[5] This 'success narrative' in many ways echoes elements of the wider War on Terror since 2014, in which attempts to demonstrate policy success and announcing the decline, collapse, defeat, and demise of Salafi-Jihadi groups have taken centre stage. Unfortunately, the extent to which the transatlantic orthodoxy of Terrorism Studies has defined these groups as defeated has little to do with their continued ability, willingness, and theological drivers to wage their particular form of Jihad.[6] Salafi-Jihadi groups remain undeterred by the Western claims of success against them.[7]

While the digital environment has gone through significant changes, much of OTS research has focused on the same old places from the early Web 2.0 era, with any change in tactics made by the Media Mujahidin being ascribed to the success of Western pressure. One will often hear OTS pundits and researchers use a version of the supposed truism that IS presence 'is not like it used to be', implying or explicitly claiming success of disruption. And indeed, it is not like it used to be. However, this is primarily because the tech landscape has changed significantly, including the usability and accessibility of platforms, and the Media Mujahidin have evolved their tactics to maximise the impact of their efforts in this changing tech landscape.

In an OTS context, the phrase is often used as part of the success narrative to hark back to a short-lived era when the Media Mujahidin heavily relied on Twitter, with the implication, in the OTS mindset, that the situation is much better now. Some OTS researchers have even

claimed that accessing Salafi-Jihadi material is limited to Telegram or an old Jihadi forum. However, the contemporary reality is that the Swarmcast2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than it was in 2014. It is also using platforms with a much greater reach than those of 2014. Ultimately, like almost everything about the way we use technology and access the web in 2022, it is not like it used to be. That change, however, is not necessarily the result of Western success against Salafi-Jihadi groups, nor has it become harder for the Media Mujahidin to operate in any strategically meaningful sense.

The paper is divided in four parts.

- Part 1 tests the orthodox success narrative about Salafi-Jihadi groups being driven onto smaller platforms.
- Part 2 introduces the conceptual underpinning of Swarmcast2.0, both through the Swarm metaphor and the concept of Web3.
- Part 3 examines how Swarmcast2.0 thrives in practice by examining the contemporary digital environment and the three contemporary distribution pillars which contribute to the multiplatform zeitgeist.
- Part 4 provides concrete evidence of the steps the Media Mujahidin have taken with Web3.

Part 1. Reassuring rhetoric

In recent years the transatlantic orthodoxy of Terrorism Studies has produced a slew of reassuring research looking at what individual platforms have done and has purported to show ever greater success against the Salafi-Jihadi movement online. In the ever-changing digital landscape, the shift of primary 'beacon' platform from Twitter to Telegram has frequently been described as a success and subsequently interpreted as forcing Salafi-Jihadi groups to use 'smaller' platforms. As Tech Against Terrorism director Adam Hadley said, "smaller platforms and social media services are where extremists moved to after being shut down by giants like Facebook and Twitter".[8] Amongst the transatlantic orthodoxy, it has become the dominant narrative now that Salafi-Jihadi groups rely on smaller, niche, or fringe platforms; for example, a recent report concluded that "broad improvements in the detection and removal of terrorist content on mainstream social media platforms has pushed such actors onto smaller online spaces".[9] These small and micro-platforms are targeted – so the narrative goes – because they lack the capacity of large tech platforms to build and maintain automated content moderation algorithms, and instead have to rely on slower human moderated systems.[10]

There are two interconnected problems with the 'success narrative' as presented by the transatlantic orthodoxy. First, the ability to deny Salafi-Jihadi groups access to platforms run by tech giants such as Facebook and Twitter, as we show below, has been frequently overstated. Second, the landscape occupied by the tech giants of 2014 is not the same as it is today. The Media Mujahidin and supporters of Salafi-Jihadi groups more broadly have been early adopters of platforms and technologies (including Web3) within their multiplatform communication paradigm (MCP).[11] That early adoption of new platforms is currently paying dividends twice over, in the form of both potential audience numbers and greater resilience of their networks.[12]

Deplatforming

Within the 'success narrative' the argument that Salafi-Jihadi groups have been deplatformed has two significant problems. First, there has been a tendency to imply that because OTS researchers could not locate branded content from Salafi-Jihadi groups on a specific platform, those groups, their supporters and aligned users were not on the platform. Second, some OTS researchers have sought to "whittle away" reference to theology to "uncloak", in their words, the real purpose of the movement.[13] As a result, material framed in theological terms is dismissed as irrelevant, even functionless, within the Salafi-Jihadi movement. Instead, many OTS accounts of the movement focus on elements such as crime, kittens, gamification, Nutella, or a jihadi utopia.

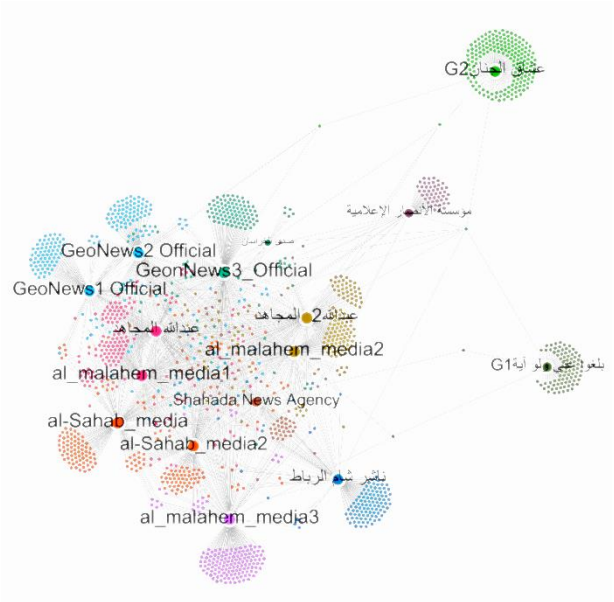
However, while theology is undervalued or overlooked in many OTS accounts of the movement, the shared understanding of theological reference points between producer and primary target audience enables the clear expression of religious concepts – concepts that are obvious in Arabic, and apparent to anyone familiar with the theological content, but which may be impenetrable code to the uninitiated viewing material from a Western habitus. It is

exactly the shared understanding of theological references between producers and audiences that the Media Mujahidin use to convey their messages, communicate complex theological concepts in a few keywords or an image, and identify potential supporters – across numerous languages, with Arabic primary among them.[14]

In addition to delivering a caricature of the Salafi-Jihadi movement, the tendency to deemphasise theology has led many OTS researchers to focus on seeking out 'official' or 'branded' material, often relying on formal logos, flags, or a narrow range of search terms. Where this approach fails to yield results, OTS has frequently concluded the Salafi-Jihadi movement's networks have been degraded or the group has been 'deplatformed'.[15] When integrated into the 'success narrative', this approach has resulted in a distorted view of the Media Mujahidin and the online presence of the Salafi-Jihadi movement.[16]

The contemporary success narrative began around 2014, when J.M. Berger believed "that Twitter suspensions have seriously degraded IS ability to game hashtags and distribute content."[17] Furthermore, while it was possible to produce claims about high levels of disruption,[18] and later the so-called 'deplatforming' of 'daesh', from an evidence-based perspective, there has not been an appreciable decrease in the ability of the Media Mujahidin to operate and fulfil their strategic theologically inspired purpose. In fact, exactly at the time when there was talk of IS suffering high levels of disruption, one third of all known traffic to IS content was still coming from Twitter.[19] The traffic data demonstrated that while researchers were unable to find them, supporters were using Twitter to share links. As such, the published conclusions that purported to have shown success in disrupting IS communications reflected the competence of the researchers in locating relevant material rather than the lack of that material, nor the difficulty the intended audience had in finding it.

Subsequent research has also shown IS videos posted on Twitter receiving tens of thousands of views.[20] The continued ease with which Salafi-Jihadi material can be located on larger platforms in 2022 should further test the success narrative, despite its wide acceptance within OTS, and the notion that current approaches have "pushed" Salafi-Jihadi groups "onto smaller online spaces". Below are a series of examples from platforms, each with over one billion users, including the world's favourite social platform WhatsApp, other Meta-owned platforms Instagram and Facebook, along with Google-owned YouTube. These platforms essentially define what it is to be an Internet Giant, yet as shown below they are all being exploited by Salafi-Jihadi groups.



WhatsApp

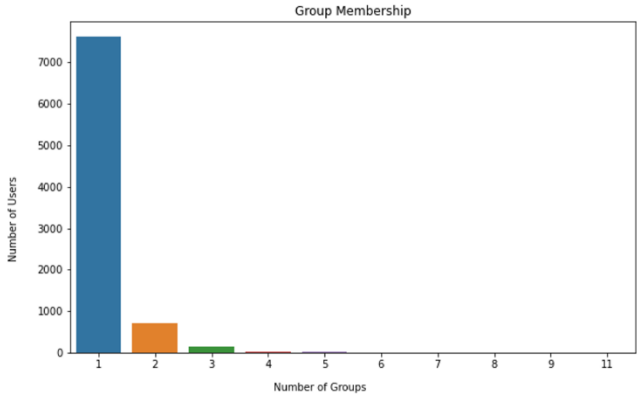
More than 2 billion people in over 180 countries use WhatsApp. It was the third most used social platform and fourth most downloaded mobile app globally in Q3 2021.[21] In January 2022 Hootsuite reported it was the world's favourite social

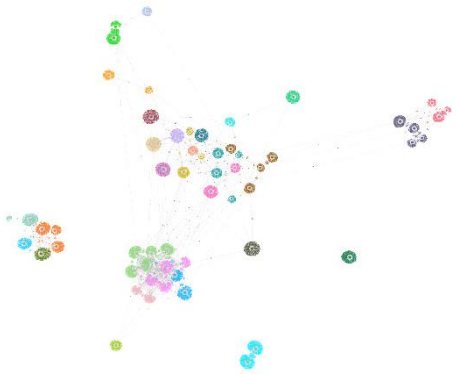
platform.[22] IS, AQ and the Taliban have all made use of Meta-owned WhatsApp. For IS and AQ WhatsApp is a second-tier network compared with other platforms, in part due to security concerns highlighted in the Electronic Horizon Foundation (EHF) discussed in a subsequent section, and due to limited group size.

WhatsApp started as an alternative to SMS; it now supports sending and receiving a variety of media: text, photos, videos, documents, and location, as well as voice calls, and provides in-app end-to-end encryption.

The network (above right), observed in 2021, features 1500 WhatsApp users following AQ WhatsApp groups such as al-Malahem (Yemen), as-Sahab (AQ Central), Shahada News (HSM, Somalia) and GeoNews (GIMF, global remit). Many of these users also join more mainstream Salafi groups that are in theological proximity but do not promote the type of violence perpetrated by Salafi-Jihadi groups.

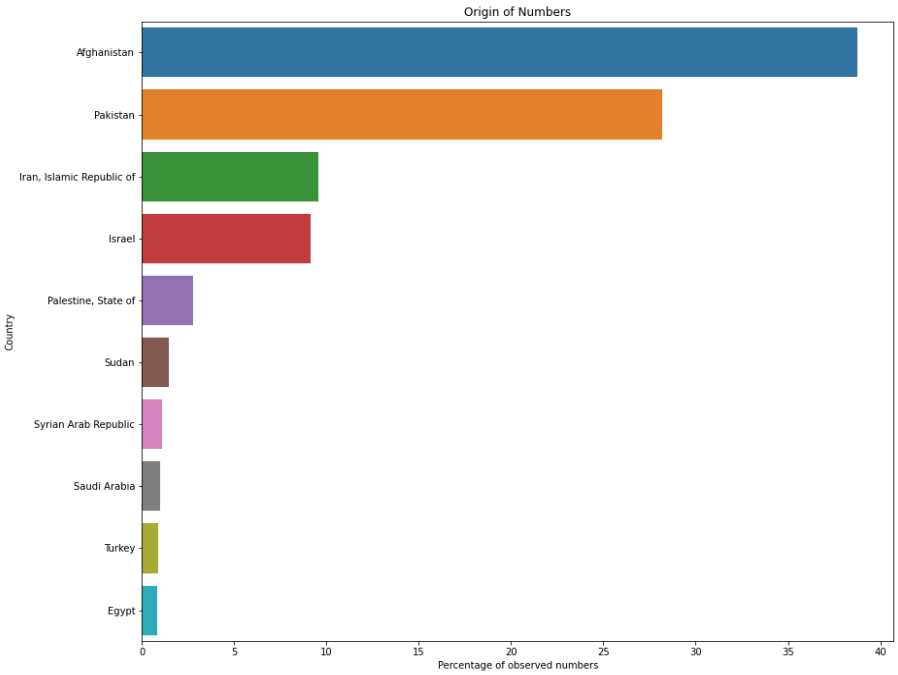
In contrast to the more subdued approach of IS and AQ, the Taliban have been heavily promoting WhatsApp chat links via their Telegram channels.





This network represents over 7000 accounts that have joined a range of Taliban promoted WhatsApp groups.[23] Each of these groups has a specific focus, from News and building Islamic apps to Taliban media output and learning languages. In this network most users have only joined one of the groups being examined.

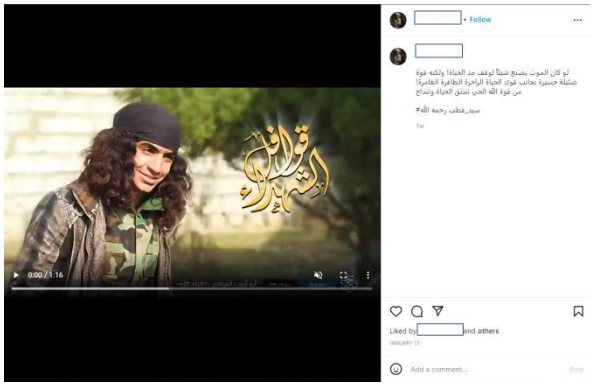
These groups not only focus on Afghanistan, but the graph below shows the users they reach are predominantly joining WhatsApp with numbers registered in Afghanistan and Pakistan.



Evidence that the world's favourite social platform, with 2 billion users, is being exploited by IS, AQ, and the Taliban should undermine confidence in the claims commonly accepted in OTS and some parts of the CVE industry that Salafi-Jihadi groups have been pushed from so-called tech giants onto smaller platforms.

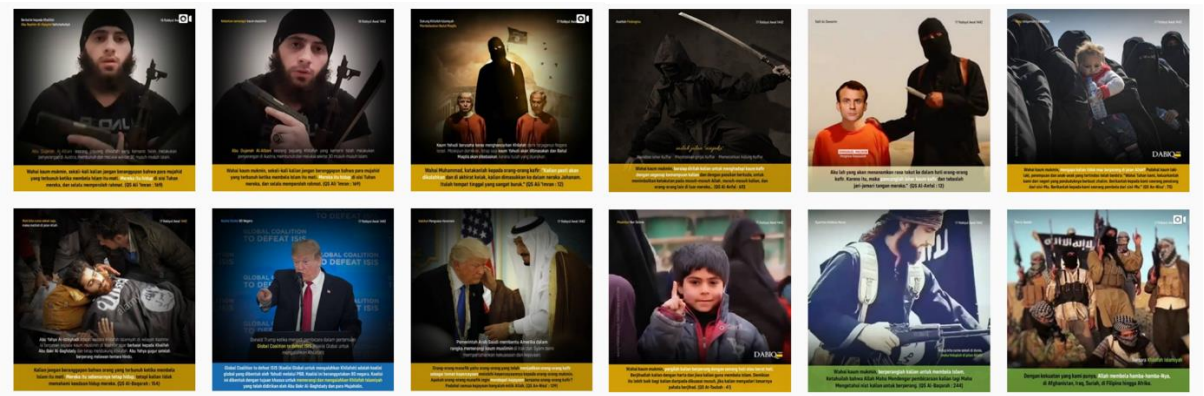
Instagram

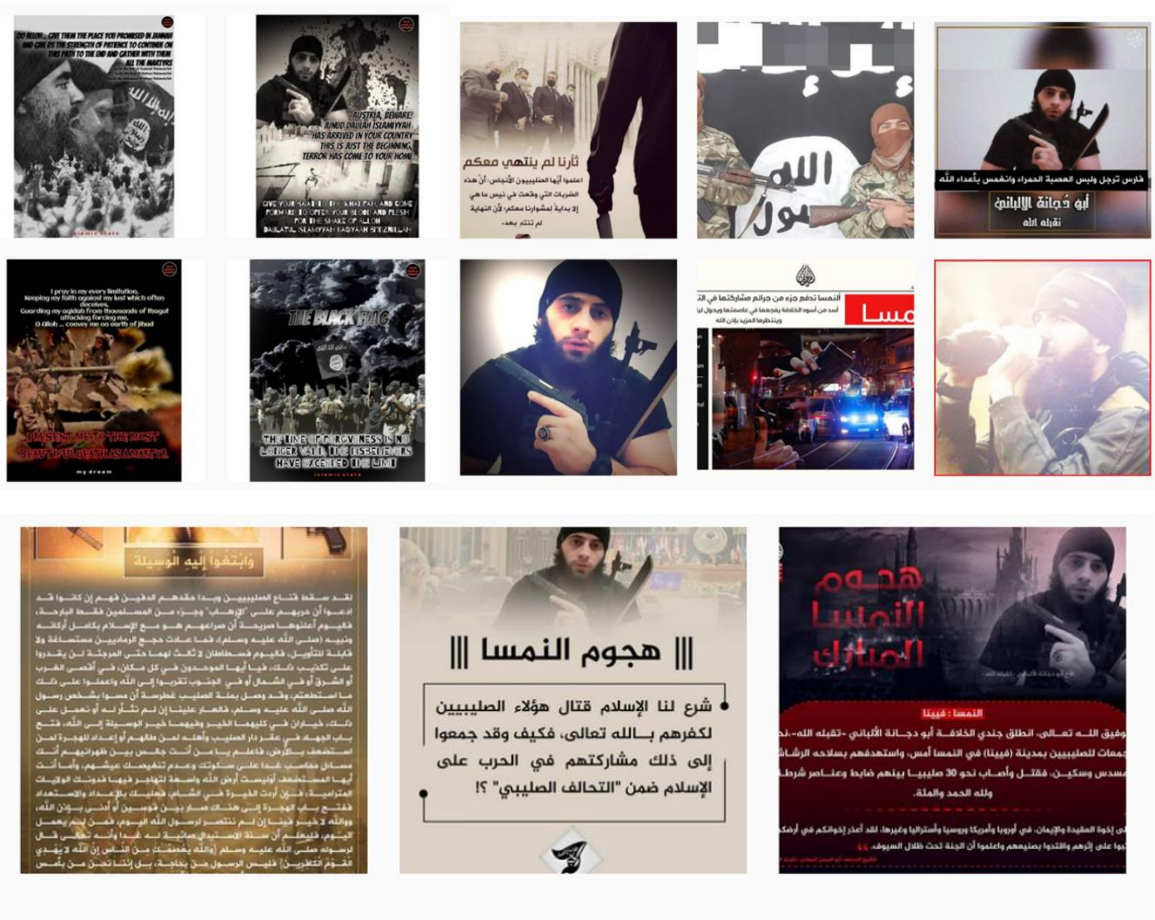
Instagram is built almost entirely around sharing images and videos. Meta-owned Instagram was the fourth most used social media platform in 2021, and the second most downloaded mobile app of the year.[24] The platform claims to have over 1.4 billion users, and networks of Salafi-Jihadi supporters are easily locatable. A simple search in January 2022 returned recognisable videos and images.



In addition to easily findable branded media, there are networks of users on Instagram who share the theological positions of groups such as AQ and IS but express them through items which convey shared meaning rather than branded or so-called 'official' material. This makes the networks largely invisible to OTS research which has focused on the easily identifiable branded content. This type of network on Instagram could be termed a second-tier network, as it is not a formal part of the content delivery system developed by Salafi-Jihadi groups that have been formally designated terrorists. These second-tier networks fulfil the purpose of spreading Salafi-Jihadi theology, just as FTO seek to spread that theology through their activity.[25] As such, these second-tier networks form an important part of the Salafi-Jihadi movement, but are often overlooked or ignored in discussions about Salafi-Jihadi use of the Internet. However, second-tier networks occasionally share material that makes their alignment, if not allegiance, clear.

For example, following the attack in Vienna in November 2020, networks of users began sharing the image of the attacker on Instagram, some even briefly adopting it as their profile picture. This highlighted the ability of Salafi-Jihadi supporters to form networks in plain sight to make continued use of platforms run by so-called tech giants. The users had previously connected through identifiers of their shared theology and a shared understanding of specific images, rather than being focused or reliant on branded material from Salafi-Jihadi groups. The theological codes that are conveyed and understood function as identifiers to other members of the movement. When users wanted to share branded material, the network was available to facilitate distribution. A sample of the images shared using Instagram is shown below.



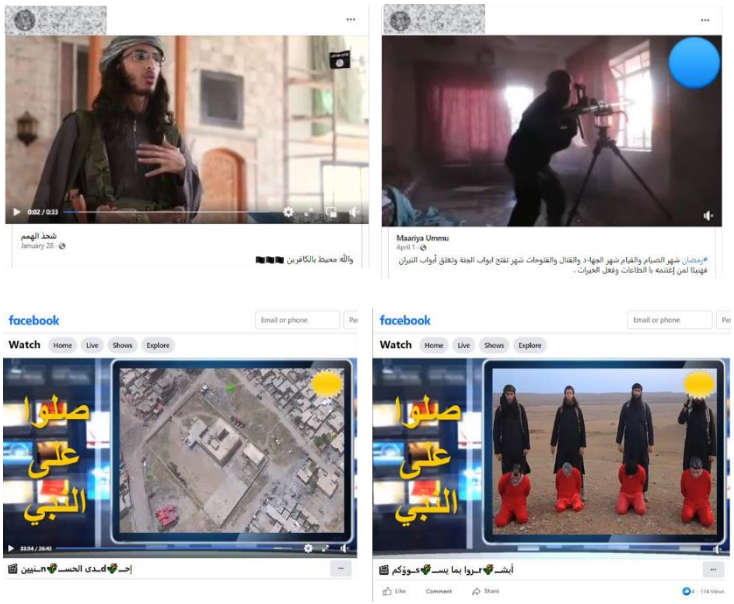


Images praising the attacker in Vienna had been shared alongside images relating to other contemporaneous events. For example, claims of suicide bombings in Afghanistan and images referencing the October 2020 beheading of a French school teacher in Paris, who was killed in revenge for having shown the Muhammad cartoons.

Facebook

Facebook is the most used social media platform, with over 2.9 billion users, and ranked third in Hootsuite's ranking of the most popular platforms.[26] However, "while Facebook continuously claims that they are investing in, and broadening, their approach to content moderation", recent research from the Institute for Strategic Dialogue (ISD) "identified many gaps in the hate speech reporting process".[27] Moustafa Ayad, Executive Director for Africa, the Middle East and Asia at ISD, said, "It's just too easy for me to find this stuff [Jihadi content] online, … What happens in real life happens in the Facebook world".[28]

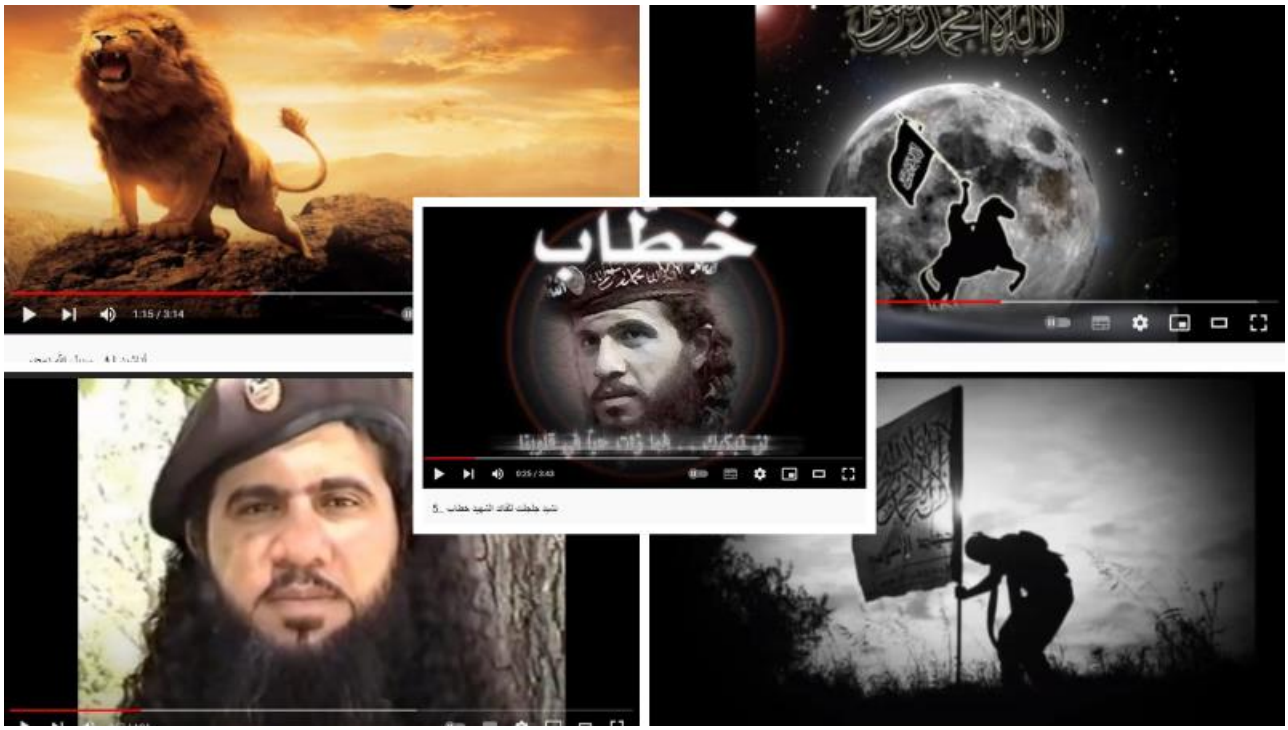
IS images from Ramadan (2022), could be easily located along with speeches and older video. Videos include individuals speaking to camera, drone footage of bombings and beheading.[29]



These examples and other content were posted by a range of users. While it is beyond the scope of this report to demonstrate the range of techniques used to evade automated detection, the above demonstrate a few common elements, including changing the aspect ratio, adding elements to cover logos, removing a portion of the image, or a combination of these techniques.

YouTube

YouTube, with 2.5 billion users, claims to be the world's most popular video sharing platform. Once the platform of choice for videos by IS and AQ, the YouTube URL is much less likely to appear in new releases.[30] However, Jihadi classics are still findable in 2022.



Videos shown were on YouTube in 2022, and were posted between February 2010 and November 2019, views range from 13,890, through 979,290 to 3,283,000. These examples represent AQ anashid and material relating to Chechnya. The comments sections make clear the alignment of many viewers with the theological perspective represented. This highlights again that while official and branded accounts might be difficult to locate, the Salafi-Jihadi movement and supporters are still active on YouTube.

That networks still exist to varying degrees on Facebook, YouTube, WhatsApp and Instagram means in 2022 material was easily findable on all four of the world's most used social platforms.[31] This is not to say these are the only platforms the Salafi-Jihadi movement uses. Nor should anybody doubt that these platforms have expended significant resources locating and removing that material. It is, however, clear that, despite the efforts of the four biggest platforms (by the number of users), that the Salafi-Jihadi movement continues to exploit them. This significantly tests the orthodox narrative about how hard operations have become for the Media Mujahidin, the extent to which they have been deplatformed, and the degree they are forced to use smaller or niche platforms. These findings significantly undermine confidence in the success narrative, even before we consider that the tech landscape is not as it was when the Media Mujahidin were briefly heavily reliant on Twitter.

Tech Landscape

The presence on the four largest platforms is not the only thing which tests the orthodox narrative; the idea that their ability to operate has been degraded and that they are being pushed to use smaller or niche platforms relies on a static view of those platforms during earlier iterations of the Salafi-Jihadi Swarmcast.

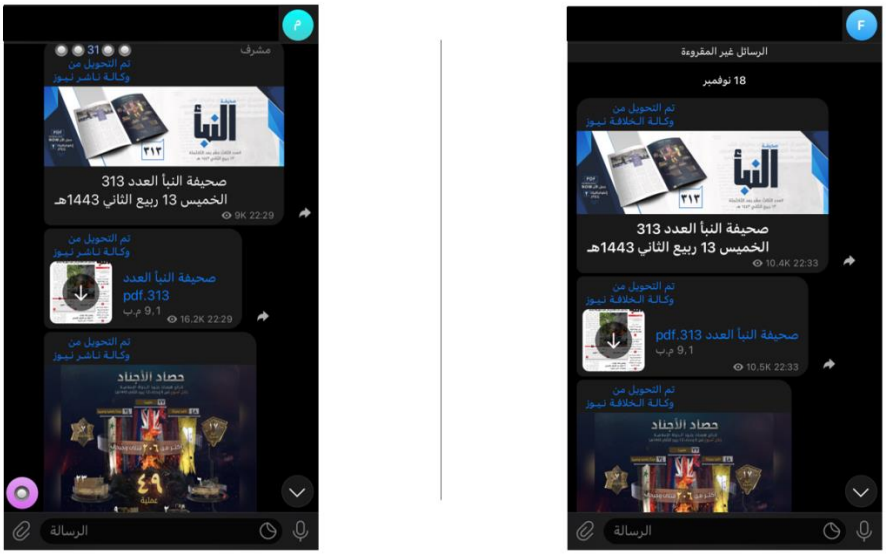
The Salafi-Jihadi movement has continued its da'wa efforts despite repeated claims of success against the movement. We are now seven years after the claims that content distribution had been degraded, six years after the "purported resilience" of Salafi-Jihadi online networks was derided by those in the orthodoxy of Terrorism Studies, and three years after the supposed "full-fledged collapse" of IS media.[32] In this time the tech landscape has changed, some of what are referred to as 'smaller' and 'niche' platforms have become new 'tech giants', a reality which poses a significant challenge to the orthodox notion of driving the movement to smaller platforms.

Telegram

Telegram has been the core of the Salafi-Jihadi information ecosystem for the last five years. Telegram claims to have over 100 million more users than Twitter.[33] Telegram was the 5th most downloaded mobile app worldwide in 2021 and the 13th most used social platform (Twitter did not feature in the top downloads and was 15th by user numbers).[34] Even if the deplatforming posited by the 'success narrative' were to be believed, the result is that Salafi-Jihadi groups have moved from reliance on Twitter to Telegram - a platform with a greater userbase and presence on mobile devices.[35]

One of the reasons for the importance of comparisons to the period when Salafi-Jihadi groups relied heavily on Twitter may also be a tendency to elevate the importance of Twitter, given its popularity amongst Western researchers and commentators.[36] Some researchers have spent the last few years tweeting large volumes of Salafi-Jihadi material, ostensibly for 'research' purposes, while also lamenting the trauma viewing the material may cause.[37] That it is the platform of choice for researchers sharing Salafi-Jihadi material does not mean it is the most important for the Salafi-Jihadi movement. Making a similar point, a Hootsuite blog post noted:"Given its fairly small user base, Twitter has impressive name recognition - 90% of Americans have heard of Twitter".[38] However, the strength of name recognition amongst Americans and terrorism researchers of the orthodox persuasion should not distract from the millions more users on the platforms Salafi-Jihadi currently favour.

Clearly, just having a large potential userbase is not the only issue; Salafi-Jihadi groups must also be able to deliver content. This is what they have continued to do. At the end of November 2021, two pdf versions of the same al-Naba (issue 313) alone were viewed over 16,000 and 10,000 times respectively on Telegram:



View statistics shown in two Telegram channels for al-Naba issue 313 released 18th November 2021

- Left: Banner 9,000 views – pdf 16,200 views.
- Right: Banner 10,400 views – pdf 10,500 views.[39]

The weekly newspaper is not an anomaly; the posts of an Amaq video showing the IS attack on a PKK-controlled prison gained more than 23,000 views in full HD and 36,700 views in reduced file format (right).[40] From these examples it is clear IS is still able get content to users.

TikTok

Shifting focus from Telegram to a relative newcomer, TikTok is another so-called 'smaller' platform on which extremist content is posted. Tiktok recently passed one billion users, which, while smaller than Facebook, is more than twice the size of the Twitter userbase.[41] Far from being deplatformed or driven to the fringes of the mainstream social media, Salafi-Jihadi groups, supporters and aligned networks are still very much a feature on many of the world's biggest and most popular platforms.

Despite the ease with which Salafi-Jihadi material can be found, much of the transatlantic orthodoxy has focused on 'problem solving' approaches and finding ways to measure and report success against the online efforts of the Salafi-Jihadi movement.[42] In doing so, as Mohammad-Mahmoud Ould Mohamedou put it, such research "knows only two directions,

that of rise or fall, victory or defeat, new or old. Who's-up-and-who's-down", best described as "scorekeeping accounts".[43] This approach has focused on making linear assessments and direct comparisons over time while researching a phenomenon which is continually evolving tactically and operating in an ever-changing technological landscape.

In 2021, the average social media user used 7 different platforms each month.[44] Salafi-Jihadi groups have adopted a multiplatform communication paradigm (MCP) which makes their presence more resilient and increases the opportunities for users to connect with their content.[45] By contrast, OTS approaches and the resultant 'success narrative', have consistently missed the meaning, strategy or tactics of the Salafi-jihadi movement and the purpose their online activity.

Starting 2022, the Media Mujahidin, through the Swarmcast2.0, have continued to maintain a persistent presence, distributing content to thousands of core supporters and operating on platforms with a larger potential audience than was available when the Media Mujahidin were heavily reliant on Twitter during the first iteration of the Swarmcast. The Twitter era is considered by OTS to be the heyday of IS, and Salafi-Jihadi Media Mujahidin more broadly, mainly because it was easy for those within the transatlantic orthodoxy to locate Jihadi material which was much more visible to non-Arabic speakers and non-initiated users, as it displayed openly Salafi-Jihadi avatars and images, often battlefield-related. This section has shown that despite the success narrative, Salafi-Jihadi communities flourish on the world's largest social platforms. Furthermore, users now have a much greater range of options through which to access Salafi-Jihadi material and connect with fellow supporters.

The following sections examine the nature of the Swarmcast in theory and practice, including how Web3 ethos and technology have been embraced by the Media Mujahidin.

Part 2. Arrival of Swarmcast2.0.

The term Swarmcast2.0 is coined to characterise the activity of the Media Mujahidin in their da'wa efforts on the changing digital terrain. It maintains the ecological metaphors of swarm and emergent behaviours, along with the speed, agility and resilience of their networks.[46] However, while the original Swarmcast was enabled largely by the increasing access to mobile technology, Swarmcast2.0 operates with the emergence of alternative distribution modalities including the growth in Web3 technologies, approaches, and ethos. This section reviews the Swarm, and the role of Web3 in theory. Part 3 examines how Swarmcast2.0 thrives in practice by examining the contemporary digital environment and the three contemporary distribution pillars which contribute to the multiplatform zeitgeist. Part 4 provides concrete evidence of the steps the Media Mujahidin have taken with Web3.

The Swarm

The Swarm is closely linked with the concept of Netwar. "Cyberwar and netwar are modes of conflict that are largely about 'knowledge' – about who knows what, when, where, and why, and about how secure a society, military, or other actor is regarding its knowledge of itself and its adversaries."[47]

According to Arquilla and Rondfeldt, networks are "very hard to deal with. …What all have in common is that they operate in small, dispersed units that can deploy nimbly - anywhere, anytime". In addition, successfully executing a netwar strategy requires that a group knows "how to swarm and disperse, penetrate and disrupt, as well as elude and evade." Organizations engaging in networked approaches are often diffuse, leaderless, and incredibly resilient.[48] For at least the last decade, the Media Mujahidin have successfully adopted this capacity to swarm and disperse using an approach to conflict closely aligned with the concept of shared purpose rather than shared organisational structure as outlined by Abu Mus'ab as-Suri. This has been observed in studies of the jihadist Swarmcast.[49]

The Swarmcast operates as an interconnected network which constantly reconfigures itself, much like the way a swarm of bees or flock of birds constantly reorganizes in mid-flight. This relies on users remaining attentive and being able to move with great speed and agility, just as the success of a flock of birds rests on the behaviour of individual birds, ensuring they do not fly into each other. This is a shift from the broadcast models of communication during conflict, which has presented new challenges for traditionally hierarchical organizations to counter, due to the great flexibility and non-linear nature of this type of organisation.[50]

Interpretations of swarming in a military setting often maintain a paradigm of centralised design, thereby contrasting hierarchies with networks as modes of operation.[51] However, swarms in nature occur without the centralised direction or design. Equally, in their most extreme incarnations, beyond those which Ronfeldt and Arquilla envisioned, the Media Mujahideen, and other dispersed networks, cease to depend on centralised direction, and instead adopt genuine swarming behaviours akin to those observed in nature. This extends the understanding of netwar and requires netwar to include the importance of emergent behaviour

and the impact of collective action in complex systems.[52] Specifically where there is potential for individual interactions to aggregate into system-wide behaviours in complex systems.[53]

As Jeffrey Goldstein put it, "emergent phenomena are conceptualized as occurring on the macro level, in contrast to the micro-level components and processes out of which they arise".[54] Emergence refers "….to the arising of novel and coherent structures, patterns, and properties during the process of self-organization in complex systems".[55]

> "Emergent properties of groups are not surprising in view of recent research on complexity demonstrating the ability of large populations of simple, identical units (for example, spin magnets) to self-organize, form patterns, store information, and reach 'collective decisions'."[56]

An authentic understanding of the Jihadist movement and the Media Mujahidin rests as much on the variation and creativity which results from the 'struggle for existence'. As in nature, where the swarm protects the individual by confusing the predator, so users disperse and regroup to maintain a persistent online presence.[57]

Pressures in the information ecosystem drive variations in tactics. Those that provide greater success for the Media Mujahidin are adopted by a greater proportion of the Swarmcast2.0. These variations, transmitted by the many interactions between individual participants, feed the further development of emergent behaviours in complex systems.

However, there is a downside, as swarming increases visibility. For example, "marine mammals use the tendency of their prey to be concentrated to facilitate successful attack".[58] Applied to the information ecosystem, when the Mujahidin Media and their supporters cluster in one place they are able to distribute information quickly but garner greater attention. Greater attention over the last few years has led to greater removal of accounts and content.

In this ecological metaphor external pressure drives variation in tactics and successful tactics spread throughout the ecosystem, augmenting the existing complex structures. Where they are successful, they become under greater pressure. Driven by the struggle for survival, the Media Mujahidin innovate, testing different technologies and platforms to find a solution with greater utility. These individual innovations thereby aggregate into system-wide behaviours, thereby reconfiguring the massively multiplatform distribution system without deliberate centralised direction.

The most successful new behaviours become formally sanctioned based on the potential impact and assessment of the challenge facing the Media Mujahidin, such as the shift from classical forums to using social media, and, two years later, the shift to Telegram. While major shifts have granted the Media Mujahidin access to the greater utility of chosen platforms, they have also known the potential limitations. As Cole Bunzel noted, quoting Abu Sa`d al-`Amili, one of the major objections raised within the Salafi-Jihadi movement about social media was that Jihadist groups were "only 'guests,' for these sites are run by 'our enemies.' Inevitably there will come a day when 'they shut their doors in our faces'."[59] Swarmcast2.0 has mitigated against this risk by operating across multiple

platforms, reducing the impact of disruption activity on a single platform, and embracing Web3 technology and ethos.

Web3

Web3, a term originally coined in 2014, refers to a third phase of evolution in the Internet, with the first era characterised by 1990s-style primarily static websites, "you can think of Web 1.0 as the read-only web".[60] "Then came Web 2.0, starting in the mid-2000s. Platforms like Google, Amazon, Facebook, and Twitter emerged to bring order to the Internet by making it easy to connect and transact online".[61] Web 2.0 is often seen as "the era of centralization, in which a huge share of communication and commerce takes place on closed platforms owned by a handful of super-powerful corporations".[62] Just as it was unclear to a Web1 world exactly how Web2.0 would develop when Darcy DiNucci envisaged the Fragmented Future of Web2.0, so the concrete form of Web3 has yet to emerge. Just as the original view of Web2.0 was very different to many of the elements which are commonplace today. Darci DiNucci wrote of the "first glimmerings of Web 2.0", noting that the Web1.0 that loaded "into a browser window in essentially static screenfuls, is only an embryo of the Web to come". "The process will be long and unpredictable, though – an organic system of mitosis, mutation, and natural selection that we can only regard with wonder". However, it will be, as Darcy DiNucci put it "the ether through which interactivity happens".[63]

In this sense, Web3 "is a vision of the future of the Internet in which people operate on decentralized, quasi-anonymous platforms, rather than depend on tech giants like Google, Facebook, and Twitter".[64] In one view, Web3 will be "a decentralized online ecosystem based on the blockchain. Platforms and apps built on Web3 won't be owned by a central gatekeeper, but rather by users, who will earn their ownership stake by helping to develop and maintain those services".[65] Molly Mackinlay argues we "want it to be hyper-distributed, replicated, resilient across many, many different parts throughout all of the galaxies that humans eventually colonize".[66] "There are a few fundamental differences between web2 and web3, but decentralization is at its core".[67] As Nader Dabit described it:

> "In web3, developers don't usually build and deploy applications that run on a single server or that store their data in a single database (usually hosted on and managed by a single cloud provider). Instead, web3 applications either run on blockchains, decentralized networks of many peer to peer nodes (servers), or a combination of the two…"[68]

From a user perspective, as Molly Mackinlay explains:

> "When you frame it from the lens of user agency, it's really about giving you control over your own experience browsing on the web. That implies permanence, because if you want to have a piece of content on your machine, you want to host it, you want to access it, that's your node's prerogative. But it doesn't necessarily mean that you can force someone else to store content on the internet that they don't want to. And it means that if you don't want to load content that some other node happens to be

> storing, you don't have to. It's really about giving you control over your own experience browsing on the web."[69]

Many of the approaches embraced by the Media Mujahidin follow an approach akin to the Web3 ethos. They are looking to control their experience of the web and the ability to create nodes in the network where they can host content. Giving them the ultimate advantage, their content is connected and interconnected to Salafi publications, enabling the Media Mujahidin to inject their created content into networks that share those books and publications that the Media Mujahidin also cite heavily in their own writings. They have already adopted the modus operandi where online activity of Salafi-Jihadi groups does not rely on a single server, single cloud provider or social media platform – they are not solely dependent on the tech giants. Instead, the media jihad exists as a multiplatform zeitgeist hyper-distributed and massively replicated on multiple servers simultaneously. The Media Mujahidin combine decentralized network forms on specific platforms with the decentralized peer-to-peer networks which mark the transition to Web3.

Part 3. The current pillars of Swarmcast2.0

The persistent presence produced by Swarmcast2.0 relies on being a multiplatform zeitgeist maintained by the speed, agility and resilience of its networks. The Media Mujahidin, and the Salafi-Jihadi movement more broadly, currently operate across a vast range of platforms which make up their multiplatform communication paradigm (MCP).[70] The current MCP and Swarmcast2.0 have emerged with a similar structure and ethos to much of current thought about Web3. Within the MCP, some platforms fulfil the role of beacons around which the movement can regroup should their activity be disrupted on a single specific platform. These beacons are the pillars of Swarmcast2.0, Telegram, Rocket.Chat, and Matrix. While the exploitation of each platform warrants significant research, too lengthy to present here, an overview of each and their relative characteristics are discussed below.[71]

Telegram functions as the core of the movement, where the entire Salafi-Jihadi ecosystem exists in one place. Since 2016, users have been able to access mainstream Salafi material alongside material from specific Salafi-Jihadi groups, including IS and AQ. All of this communication takes place via a mobile app which can facilitate communication in groups of over 100,000 users or encrypted one-to-one messaging.

Rocket.Chat servers have the role of a static 'citadel' or 'factory', similar to the original bulletin board and forum sites from the first decade of the 21st century. The role of these sites was described by Abu Sa`d al-`Amili in a piece where he lamented the shift of "major [jihadi] writers and analysts" to social media and the decline in participation in jihadist online forums. He issued a "Call (nida') to the Soldiers of the Jihad Media", demanding that they "return to their frontiers (thughur)", elevating their status as the driving force of the movement.[72] Rocket provides the modern version of these citadels, where access, participation, and publication are controlled by the server administrators loyal to AQ or IS.

Matrix operates as the final pillar, heavily promoted in online security briefings posted by groups aligned to IS. It is, from a technical perspective, the leading edge of the Salafi-Jihadi movement, already fully able to operate using Web3 approaches and ethos.

Telegram

What is Telegram

The Media Mujahidin have used Telegram to communicate since 2016.[73] According to Telegram developers, Telegram is a cloud-based instant messaging service, providing optional end-to-end encrypted messaging. Telegram lets users access their chats from multiple devices with messages that are heavily encrypted and can self-destruct. Telegram has no limits on the size of your media and chats, and groups can hold up to 200,000

members.[74] It is free and open, having an open API and protocol free for everyone, which has allowed users to build their own bots, and even their own clients to access Telegram.

Over the last five years Telegram has been the most important social media platform for jihadist media operatives to project influence, disseminate videos, text documents, pictures, audio and torrent files. Since its adoption, Telegram has customarily been the first point where Salafi-Jihadi content is released into the information ecosystem.

Much of the transatlantic 'success narrative' has presented the adoption of Telegram as the result of disruption on Twitter, forcing IS and AQ to use smaller platforms on the margins of the Internet. From the perspective of the Media Mujahidin. Telegram has had much greater utility for their efforts to communicate with supporters. The ability to use one app to have encrypted conversations, share large files, broadcast content to thousands of users, use large group text chat, now with the option to allow millions of users to chat live[75], along with one-to-one video, and automated features including bots[76] to moderate groups or interact with users to share content has been significant.

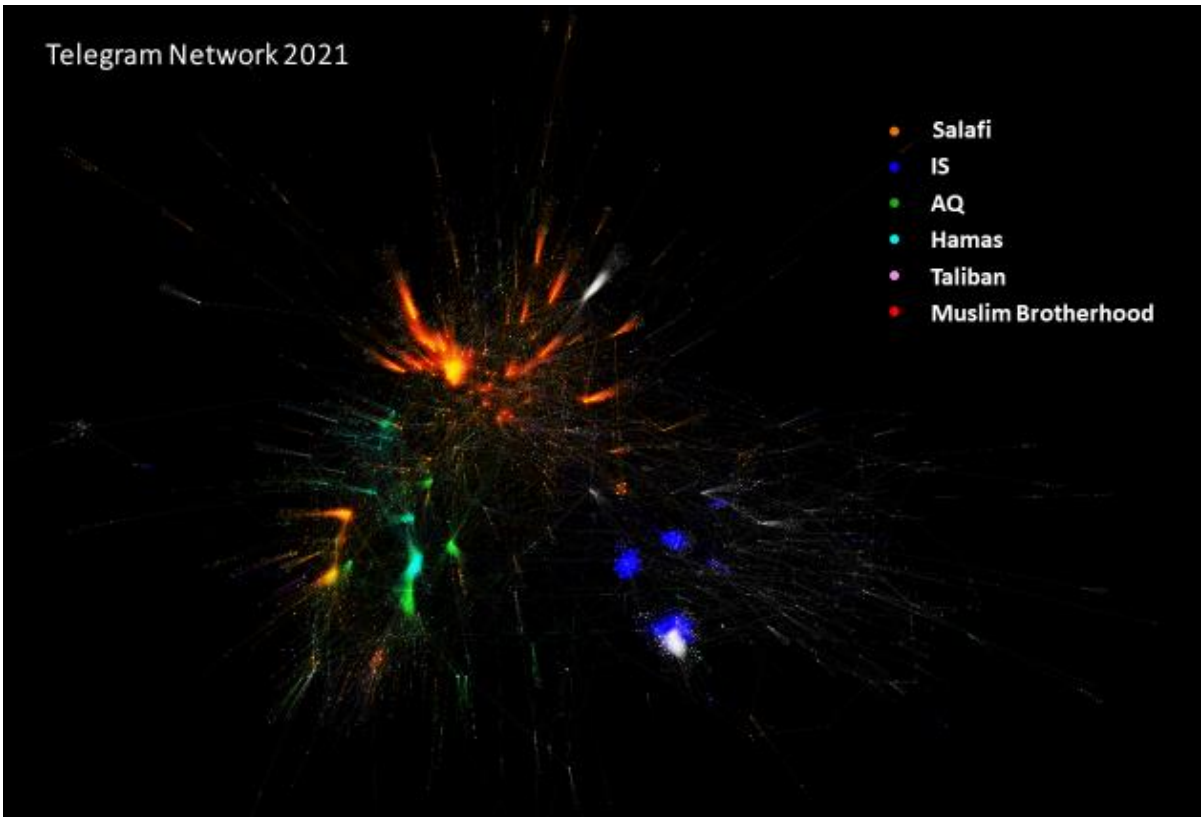
It is important to note, while the move to Telegram by the Media Mujahidin has been mythologized within the transatlantic orthodoxy of Terrorism Studies as the result of a 'successful' effort to drive them from Twitter, there is another perspective.

First, Telegram now has both a larger userbase than Twitter and a greater number of mobile downloads. As a previous study has highlighted, Telegram was the 5th most downloaded mobile app worldwide and the 13th most used social platform in 2021. In contrast, Twitter once hailed as the platform on which IS achieved mass reach, is now ranked 15th by user numbers, has approximately 100 million fewer users than Telegram and didn't feature in the top mobile downloads.[77]

Second, even when Salafi-Jihadi groups such as the Taliban are able to use Twitter openly, they have Telegram groups with tens of thousands of users. Third, Telegram enables users to engage with the full range of groups and content across both sides of the Salafi-Jihadi nexus.[78] Fourth, large Salafi networks are well established on Telegram. This is the primary target audience for Salafi-Jihadi groups to garner sympathizers and recruits, as important Salafi Telegram channels frequently shared links to channels which hosted Salafi-Jihadi FTO material.[79] The Media Mujahidin shares links to Salafi channels and re-shares Salafi content within Salafi-Jihadi channels. At the centre of this interaction stands a shared theology which, from a Salafi-Jihadi perspective, provides the understanding of and rationale for Jihad in theory and practice.[80]

Telegram Data

The full range of material of mainstream Salafi and Salafi-Jihad material is available on Telegram. The network of content sharing (one channel/group re-sharing messages from another channel/group) within the core of the movement shows a network of over 7600 channels. Which include IS, AQ, the Taliban, the Muslim Brotherhood, and Hamas.



As published in detail in a previous article, the network created by content sharing between channels during 2021 shows that just under 90% of channels connect into a single giant network which includes both Salafi and Salafi-Jihadi content.[81] IS, AQ, Hamas, the Taliban and the Muslim Brotherhood may therefore not connect directly to each other's channels, but they are all connected to the same network and draw on the same ecosystem of content and theological material. Despite the ongoing presence of this network, there have been those within the OTS and CVE industry who have been keen to talk up the impact of disruption efforts. For example, Winter and Amarasingam were quick to claim that EUROPOL action had "resolutely trashed the Islamic State's presence on Telegram".[82] As has become commonplace in elements of OTS, policy positive claims by commentators are not supported by evidence-based research. In this case, the data clearly shows that, rather than networks being trashed, the Media Mujahidin from IS and other Salafi-Jihadi groups have maintained a persistent presence, reconfiguring like birds in flight, reconnecting with primarily Salafi channels and have been able to continue to exploit the platform. In addition, the EUROPOL-backed attempt to remove IS from Telegram spurred the group to experiment with new(er) platforms while resettling their base on Telegram. IS, AQ and others now continue to operate networks of various sizes across other platforms, in addition to increasing numbers of spontaneous and sympathetic networks being created by supporters. This level of interconnectivity within the Multiplatform Communication Paradigm (MCP) adopted by the Salafi-Jihadi movement produces many levels of redundancy in a network and ensures a persistent presence for the movement. This approach makes the network much more resilient and enables users to reconnect quickly and conveniently.

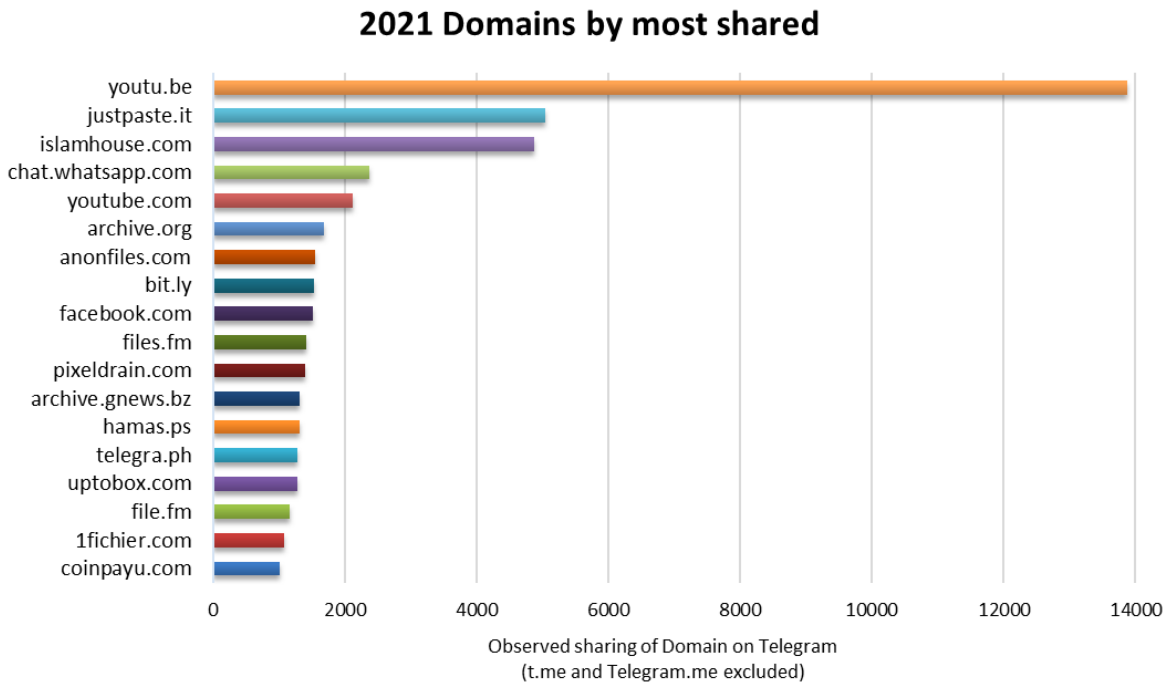
Furthermore, the evolution of a single giant network has occurred despite the various groups on both sides of the Salafi-Jihadi nexus being subject to very different pressures. Some groups are able to use Twitter openly, while others face concerted efforts to remove them. This challenges the orthodox assumption that IS was driven to use what is often referred to as the 'smaller' platform, Telegram. The claim is that IS and AQ use Telegram due to the difficulty of using Twitter. However, this pressure did not apply to the Taliban and many Salafi organisations, who, despite being free to use Twitter, have built large networks on Telegram as well. Clearly, for various Salafi and Jihadi groups, there is a large target audience and a rationale for using Telegram, other than not having access to Twitter.

In addition, as shown elsewhere, Salafi channels create a permissive environment in which Salafi-Jihadi groups can target their intended audience, and from which theologically aligned material to bolster the credibility of their theological position is shared.[83] Amongst orthodox interpretations promoting the success narrative, this point is almost never made, however. By contrast, the progressive, evidence-based approach to Terrorism Studies has shown the Telegram network is an online manifestation of the Salafi-Jihadi nexus.

As noted in a previous paper:

> "The Salafi materials are often quick and easy to find online - and in several languages. This enables jihadis to attain credibility as a religious movement fighting for ultraorthodox theological parameters while the networks online on the Salafi side of the nexus are rarely taken down or pushed offline. This reality strengthens Salafi-Jihadi networks online as it is one column, upon which they can rely to repopulate their content and continue to attract consumers of the Salafi world to their 'enhanced' world where religion is applied by force and based on theological constants and commandments that are explained in a soft-power fashion within the Salafi networks.[84]"

The finding of the network analysis is replicated in the analysis of domains most shared by accounts at the core of the Salafi-Jihadi information ecosystem on Telegram. The analysis demonstrates the ability of the Media Mujahidin to swarm and disperse, along with an increasing adoption of Web3 technologies.



The most shared domains on Telegram include platforms fulfilling the main roles within the multiplatform communication paradigm; 'beacon', 'content aggregator', and 'file store'. In addition to Telegram, WhatsApp chat links are shared frequently. Justpaste.it and Telegra.ph are the most frequently used aggregators of Salafi and Salafi-Jihadi content, with YouTube, archive.org, annonfiles being prominent content stores.

Three other particularly noteworthy domains are first, archive.gnews.bz is a subdomain from the former location of the AQ Rocket server, discussed in more detail below. Second, Coinpayu.com enables users to earn cryptocurrency and gives access to a number of cryptocurrency mining and exchange apps – cryptocurrency, NFT, and blockchain being prominent elements of current Web3 applications.[85] Third, Islamhouse.com describes itself as "The largest and the most authentic free reference to introduce Islam in the world languages on the internet".[86] That it is part of the Salafi-Jihadi nexus should not be surprising, given the theological nature of the movement and the tendency to use mainstream Salafi material alongside branded IS or AQ content.[87] Islamhouse.com offers mainly books in Arabic, and in another 120 languages, where selected Arabic writings are free to read online and download as translations. The site hosts the writings of Sunni Islamic scholars – hence the writings are all theological and offer a wide range of shared meaning within the Salafi-Jihadi movement, ranging from hatred against Shi'ites, anti-LGBTQ+ propaganda to historical books framing it a divine obligation for any Muslim to kill anyone accused of blasphemy, especially of insulting God or prophet Muhammad. These books are being re-shared within the networks after attacks to justify the killing of, for example, a French teacher who showed the Muhammad cartoons in Paris, October 2020. The books in question are of theological nature and can be easily obtained online without much effort, including translations on missionary sites such as Islamhouse.com.

In sum, through the Telegram app, with hundreds of millions of users (a significantly greater userbase than Twitter), Salafi-Jihadi groups are able to target their primary target audience through the concurrence of Salafi and Salafi-Jihadi material within a single interconnected online network.

Rocket

What is Rocket

The makers of Rocket.Chat describe it as "The communications platform you can fully control and trust". It is offered as either Software as a Service (SaaS) or as a "self-managed" install on an independent server. It is intended to "empower organizations to own their conversations by developing the world's most flexible and secure open-source communications platform".[88] Echoing the Web3 emphasis on decentralisation, Rocket.Chat is open source; the creators argue: "the future of communication is not on closed systems and will never be".[89] In fact, the Rocket.Chat code is hosted on Github, has over 31,000 stars (similar to Facebook 'likes') and has been forked[90] over 7,000 times.[91] Rocket.Chat offers integrations with a range of other communication methods, including WhatsApp, Facebook Messenger, Twitter, Telegram, Email and SMS. It also offers integration with chat bots and machine learning apps, including Amazon Lex, Algolia, IBM Watson, Azure Bot Service, Ilhasoft and Chatfuel.

Both IS and AQ have access to their own self-managed Rocket.Chat installation. In Web3 style, this means they have all the capabilities of a mature communications platform, but without the centralised administration of Web 2.0 platforms, like Facebook or Twitter, that can suspend or remove IS/AQ accounts when reported by users or governments.

Rocket Data

The AQ installation is primarily Arabic focused, with some other languages from multiple AQ groups. These include JNIM (Sahel), HSM (Somalia), AQAP (Yemen), as-Sahab (global) and additional media via Thabat and Zallaqa, GIMF and Shahada News.

The IS Rocket server has a range of multilingual channels sharing branded IS news and releases, along with a range of media foundations including al-Bayan, Ajnad, al-Taqwa, and Sunni Shield. There are also a series of groups on specific themes, from the lives of the martyrs and Jihadi Scholars to Coronavirus as a soldier of God.

		IS	AQ
Groups	Number of Groups	254	122
Membership	Mean	458.61	742.39
	Median	93	101
	Mode	103	12
	Highest	5,158	2,532
Messages	Mean	662.65	713.47
	Median	92	145
	Mode	7	1
	Highest	12,611	8,654
	Total Messages	168,313	87,043

On their Rocket.chat servers IS has approximately twice as many groups and twice as many total messages, and the largest group is approximately twice as large as the largest group on the AQ server. It is beyond the scope of this discussion to analyse the number of unique users on each server, but the largest group indicates there are at least this number of accounts on each server.

In addition to the updates on content releases and announcements available in the channels, both IS and AQ use other features which contribute to the multiplatform communication paradigm:

- Following a well established protocol, lists of URLs are shared to content stored on filesharing sites as well as lists of channels on other platforms, including Telegram, Matrix, and Whatsapp.
- The Rocket servers have an 'archive' subdomain, where content is stored. Links to content in the Rocket archives appear in the lists of URLs shared content releases and re-releases. These archives circumvent the content removal efforts, because even if all other links are removed, material is available via the Rocket archive link.
- The 'archive' subdomain provides integration with Nextcloud, free and open-source software which enables anyone to "install and operate it on their own private server".[92] Files can be transferred directly from the Rocket archive subdomain to an individual's self-hosted Nextcloud, links to which can then be shared. Nextcloud is a "open source file sync and share software for everyone from individuals operating the free Nextcloud Server in the privacy of their own home, to large enterprises and service providers supported by the Nextcloud Enterprise Subscription".[93] Links to Nextcloud Servers shared within the Salafi-Jihadi movement focus on specific groups or areas, including HSM material on an installation called "kataibdrive", or AQIM on "maghrebfiles" or in a specific language such as an installation known as "Banglafiles".[94] This combination of Rocket, an archive subdomain, and Nextcloud creates the dispersed storage which enables the Media Mujahidin to maintain a persistent presence as part of the Web3 approach to decentralisation.

Matrix

What is Matrix

Matrix is an open network for secure, decentralized communication (the Matrix open standard).[95] Through using the Matrix open standard it “is as simple to message or call anyone as it is to send them an email”. Users can “communicate without being forced to install the same app” and “can choose who hosts your communication”. In addition, “conversations are secured by E2E encryption”.[96]

Matrix is a network of interconnected 'federated homeservers’ – users initially register on a ‘homeserver’ and the matrix’ open standard enables communication between users on the same server and connects ‘homeservers’ to each other. Matrix is analogous to email servers like Google, Outlook, or Protonmail. Users can communicate across servers, but each server has its own specific nuances. They communicate with each other, but each gives the user a slightly different experience.

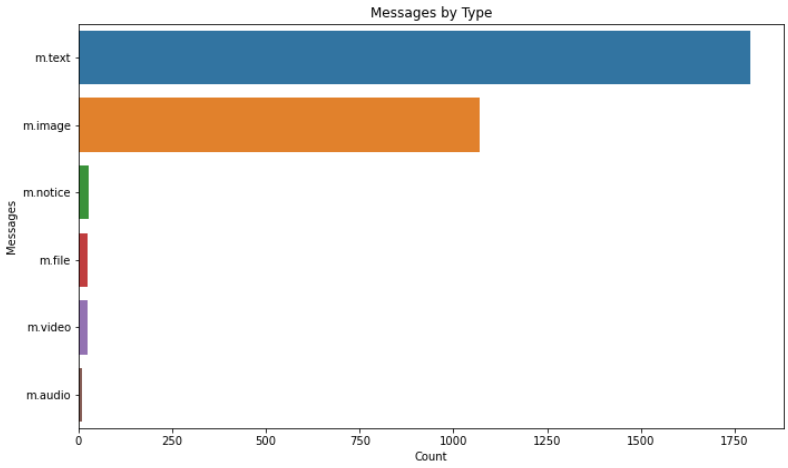
Matrix is heavily favoured in advice circulated within the Salafi-Jihadi movement due to its utility, security, and anonymity. It can be accessed through clients such as Element (previously Riot), Ditto Chat, FluffyChat, Hydrogen for mobile, and with Desktop clients, including Nheko, Fractal, NeoChat, Mirage, Seaglass and Spectral. Other options exist for Web, Terminal/Command Line, and even Nintendo 3DS.

The decentralised nature of Matrix makes it particularly useful to the Web3 enabled Swarmcast2.0 and Matrix users are likely the leading edge of the Salafi-Jihadi online movement. Both IS and AQ have created channels on the main Matrix.org homeserver, while IS has also created its own homeserver. That homeserver runs on a Nginx[97] web server, controlled by a pro-IS administrator. In the Web3 context, this gives IS the ability to provide content and to control the content on their server (using their 'node prerogative') in the decentralised network.[98] All channels which appear on this IS homeserver have the approval of the server admin, and currently have between 300 and 550 members.

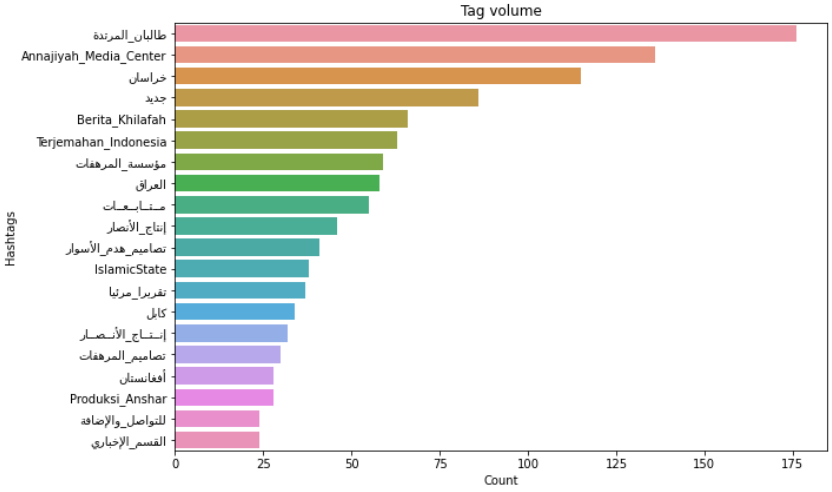
In addition to having their own node in the Matrix network, using their node prerogative to host the material they choose, the homeserver also utilises the Matrix 'bridge' function, where content can be imported from other platforms. In the IS case, they have bridges from Telegram, so the material which appears in their channels on Telegram also appears in their Matrix channels. This extends the distributed network which made the Salafi-Jihadi network on Telegram so resilient to the "hyper-distributed, replicated, [and] resilient" network imagined in the Web3 ethos and the multiplatform communication paradigm which underpins Swarmcast2.0.

Matrix Data

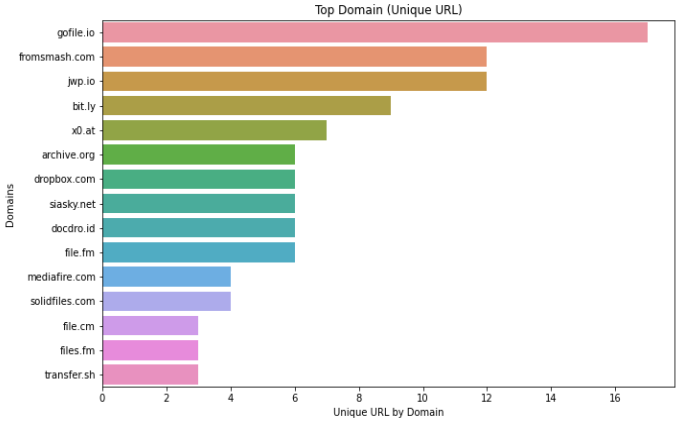
3000 messages archived from the IS Matrix homeserver in December 2021 demonstrate how the IS homeserver is used.[99]



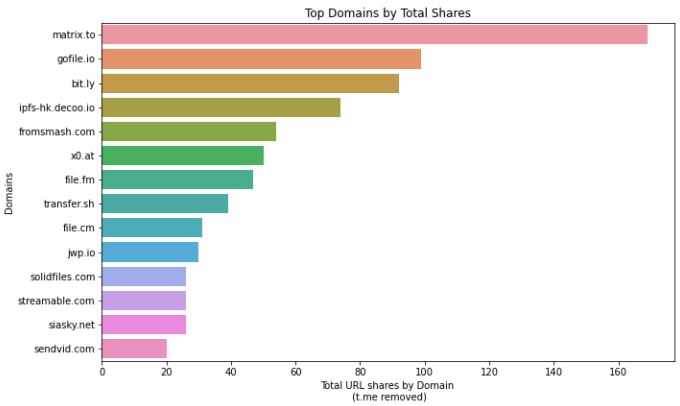
The majority of the messages are text which include URLs, but a third are images. The most commonly used hashtags in the messages highlights whether the material is in Arabic and Latin script and draws on material from a range of producers and locations.



The URL which appears in the text of messages also facilitates the multiplatform communication paradigm. The most commonly linked domain is Telegram, shared over 1750 times. This enables users to reconnect with the core of the Salafi-Jihadi network on Telegram and is also driven by the links contained in material posted via the Matrix Telegram Bridge.



The range of domains used highlights the different roles platforms fulfil in the MCP, including the ‘beacons’ such as Telegram and Matrix, with many of the others being filesharing sites in the role of ‘content stores’.[100] Most relevant to the emergence of Swarmcast2.0 is the adoption of decoo.io, which brands itself as the “Entrance to Web 3.0”.[101]



Part 4. Web3 in action

The Web3 technology currently in use already represents a significant circumvention of existing tactics and techniques intended to disrupt the Salafi-Jihadi movement´s online activity. From EthLink and IPFS pinning, to the integration of onion links which underpin the strategy to deliver a resilient surface web distribution infrastructure, Web3 is already in use. This final section provides evidence of specific Web3 approaches already in use by groups within the Salafi-Jihadi movement.

IPFS

IPFS, the InterPlanetary File System.[102] IPFS is a distributed system for storing and accessing files, websites, applications, and data.[103] IPFS makes "it possible to download a file from many locations that aren't managed by one organization", producing the decentralisation central to Web3 and the modus operandi of the Media Mujahidin.[104] IPFS not only "supports a resilient internet", "it makes it harder to censor content".[105] The IPFS provides greater resilience because:

> "files on IPFS can come from many places, it's harder for anyone (whether they're states, corporations, or someone else) to block things. We hope IPFS can help provide ways to circumvent actions like these when they happen".[106]

"IPFS is based on the ideas of possession and participation, where many people possess each other's files and participate in making them available", an approach which is very similar to both iterations of the Swarmcast where members of the Salafi-Jihadi movement contribute to maintaining the persistent presence of Salafi-Jihadi material.[107] Advocates of IPFS follow John Perry Barlow's argument that "The Internet treats censorship as a malfunction and routes around it". For example, following claims that the Turkish government had "issued a court order that permanently restricts access to the online encyclopedia Wikipedia", volunteers made a snapshot of the Turkish version via IPFS. The announcement stated, "We're alarmed by the erosion of civil liberties wherever it occurs, and we want to help people like the citizens of Turkey preserve freedom of information, even in the face of a tightening iron fist".[108] This example demonstrates how small groups of individuals can use Web3 technology to make material available in face of government attempts to block it. By making content available via IPFS links, the Media Mujahidin has likewise taken advantage of the additional resilience on offer.

Decoo

Decoo is a Web3.0 service provider established by DCF (Decentralized Cloud Foundation). Decoo focuses on IPFS Pinning & Hosting Service, Decentralized Cloud Storage, Node Service and API Service. Decoo aims to create an easy-to-use entrance infrastructure into

Web3.0 - real decentralized, distributed cloud, for worldwide users.[109] It is built on the experience of projects such as Git[110], BitTorrent[111], Kademlia[112] (which contributed to the development of Ethereum[113]), and Bitcoin[114].[115] Decoo and other similar services allow users predominantly accustomed to a web2.0 experience to use IPFS. The benefit for the Media Mujahidin is that their material can be distributed via IPFS but accessed via a web browser with which their target audience is already familiar.

One of the groups which takes advantage of IFPS services such as Decoo is IS. The screenshot above shows a recent video made available via IPFS playing in a chrome browser.[116] This means IS has adopted the technology to deliver a resilient surface web distribution infrastructure via Web3. As we have seen with many other developments, once the practical details have been established by one group within the movement, 'blue collar knowledge' rapidly spreads to other groups.[117] The screenshot above, a video release by the Islamic State province West Africa, documents the application of theology, citing a verse of the Quran defining the rule of God in dealing with thieves. This understanding of this particular verse (Quran 5:38) is not unique to the 2022 IS video. The same jurisprudence has been in place in the writings for decades, since the 1980s and 1990s.[118]

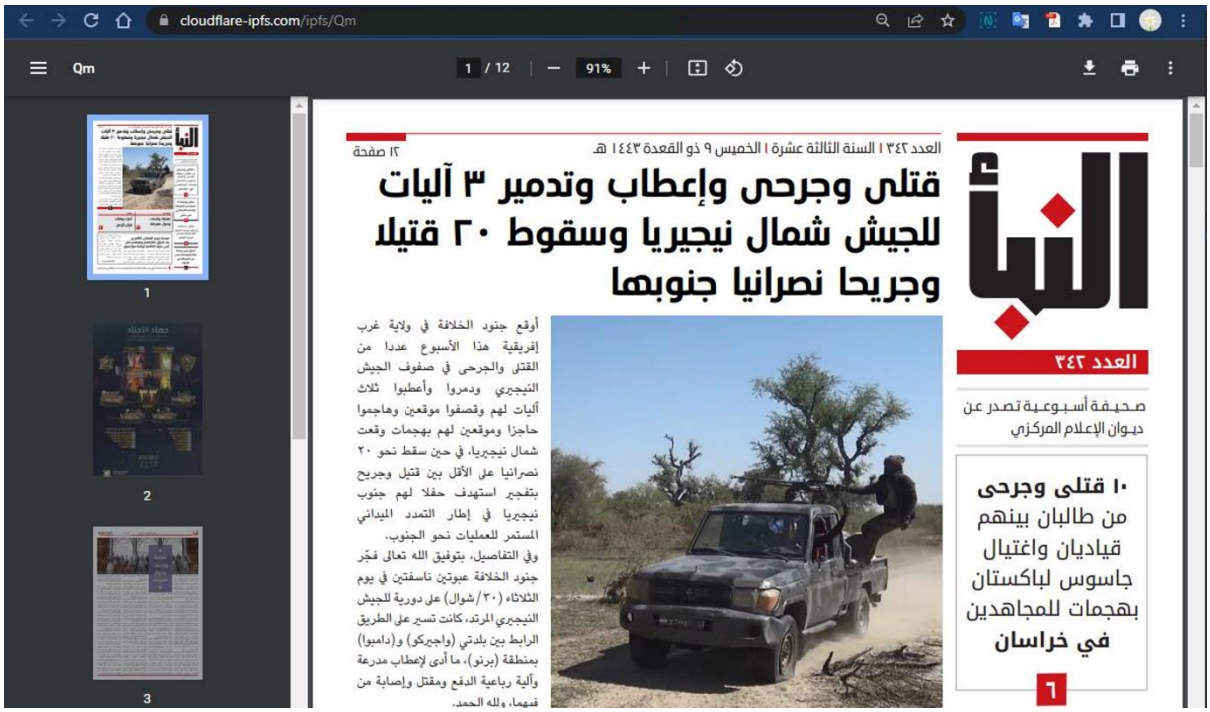
Cloudflare

Cloudflare, better known publicly for providing protection for websites, also provides a gateway to Web3. Described as offering "Easy access to IPFS and Ethereum networks", it

leverages decentralization, implicit trust and peer-to-peer networking central to Web3. Within this approach:

> "The Interplanetary File System (IPFS) provides a storage layer for Web3. IPFS is a protocol and peer-to-peer (P2P) distributed network for storing data across nodes within the network. "[119]

The exploitation of Web3 by the Media Mujahidin includes being able to access material, including the IS daily newspaper al-Naba.



The adoption of IPFS marks a fundamental shift in the distribution methods, using a storage layer outside the traditional web2.0 approaches, but accessible from a regular web browser. This and the Swarmcast2.0 present a new and significant challenge for attempts at disruption, as it embraces the decentralised, resilient network of content distribution envisaged for Web3. IPFS is, however, only one part of Web3.

EthLink and Onion

EthLink is one of a range of approaches and services which can be leveraged to deliver a much more resilient, Web3-enabled distribution system. "EthDNS is a way to access information in the Ethereum Name Service (ENS) from DNS" and "EthLink is EthDNS for the .eth domain".[120]

“Because .eth is not a registered DNS top-level domain, it is normally inaccessible from DNS, but by appending .link to the domain the relevant information can be obtained. For example, a DNS A record request for mydomain.eth.link would look up the A records in ENS for mydomain.eth.”[121]

This system makes users or material findable outside the current DNS system usually required for making a website findable, making websites with regular domain names susceptible to disruption and removal, as highlighted in a recent Tech Against Terrorism report.[122]

While organisations like Tech Against Terrorism seek to draw governmental attention to the issue of individual websites by using a single Ethlink, https://f####s.eth.limo, IS media operatives have created a system to circumvent the disruption effort of removing individual websites. The eth.link provides a regularly updated index page of their websites. Rather than return to the domain name for a website, the user just accesses the index page from their browser and selects the link to their desired website, wherever it is currently hosted. This capacity effectively renders the disruption through the removal of individual websites obsolete, at a time when the Western CVE industry is still grappling with developing potential mechanisms for the removal of individual websites.[123]

To add an extra layer of resilience, a very similar approach has been deployed with an onion link.[124] Like the EthLink, this also provides the index of existing webpages. One need only bookmark the link in a Tor browser (or ethLink in any browser) and the whack-a-mole deletion of domain-named websites is circumvented almost in its entirety. This approach combines the elements of decentralisation with the structure of dispersed nodes, that are hallmarks of Web3, with the utility of existing services, such as Tor, that have pursued this approach to security and resilience for well over a decade.[125]

Worthy of additional note are two elements, which are highlighted by the use of eth and onion. First, the ability of the Media Mujahidin to adapt to the changing tech landscape, and second, the commitment and technical competence these steps demonstrate.

Firstly, as observed previously, the tech landscape has changed significantly, and the Media Mujahidin have evolved their tactics to maximise the impact of their efforts. Tor was once thought of as relatively hard to use, and, by 2013, had become “a focus of criticism, accused of facilitating a dangerous "dark web" of pedophiles, drug dealers, and arms traders”,[126] or, as an NSA document described it: "Very naughty people use Tor".[127] In this mindset it became common to lump criminals using the dark web and Tor users into one category, with multiple stories surfacing of the National Security Agency based in the US and GCHQ in the UK attempting to attack the Tor network and undermine the anonymity of users.[128]

However, the current Tor browser, a variant of Mozilla Firefox, is as easy to download and install as Chrome, Edge, Safari, Opera or any of the many other browser options.[129] It is easy to use on Windows, macOS and Linux, with a version for Andriod and Onion

Browser for iOS.[130] Tor can even be made 'portable', so an individual can take it with them and use it from a USB stick or SD Card on other computers.[131]

One can access the software via the website or via the GetTor service. GetTor "provides alternative methods to download the Tor Browser, especially for people living in places with high levels of censorship, where access to Tor Project's website is restricted".[132] In addition to highlighting the relative ease of accessing Tor, even in environments with high levels of web filtering, the methodology behind GetTor of emailing to receive an automated response with links is also used by the Media Mujahidin. In the case of Salafi-Jihadi groups, the method is used to provide access to websites that have been forced to change their URL, due to law enforcement action to block it from using a specific domain name.

In parallel to the easy access to Tor, many surface web services are also accessible via the Tor browser. Wired.com, for example, is directly accessible, while shopping on Amazon via Tor requires a successful captcha test to allow access to the site.[133] Other sites provide a specific Onion service, including the BBC, who launched their service in 2019,[134] Deutsche Welle (DW), Germany's international broadcaster, and the American funded Radio Free Asia who created services in 2020.[135] Other organisations including the CIA, The New York Times, ProtonMail, and Facebook also provide specific onion links for Tor users.[136] Far from being a service just used by 'naughty people', the way users interact online has evolved, and many now use VPN and/or Tor as additional layers of protection for their identity and privacy. As greater numbers of people and services use Tor, so the Media Mujahidin have adapted to new ways to reach their target audience.

Secondly, the way Tor and Onion services are being used by the Media Mujahidin highlights the level of commitment and technical competence they have at their disposal. Onion links are usually random strings. Time and computing effort must be invested to create a custom or vanity string. This process takes a few seconds for the first three or four characters, but rapidly escalates to around thirty minutes for six characters, and from there reaches a day, a month, and approximately 40 years if ten characters were required.[137] The onion link starts with a six-character custom string which matches the EthLink. This effort comes at a time when some advocates of the OTS 'success narrative' claim the Media Mujahidin are being degraded, are tiring, and have been worn down by having to create new pages and accounts on various social media platforms.

It is hard to square such assertions with the evidence-base, which shows the Salafi-Jihadi movement innovating new ways of working and making the 'website' element of their distribution system more resilient. This even while those websites are claimed to be a "blind spot for policymakers, practitioners, and researchers", according to Tech Against Terrorism.[138] Rather than struggling under pressure, IS is going the extra mile to give their onion link a custom identity.[139] The gap between the innovation and technical ability of the Media Mujahidin on the one hand and the OTS researchers claiming to be measuring the decline of IS and Salafi-Jihadi groups on the other is vast and growing rapidly. It has

already grown to such an extent, that much of the Swarmcast2.0 is effectively invisible to elements within OTS producing reassuring rhetoric and policy positive findings for policymakers and social media companies. At the current rate it will soon become the contrast, envisioned by Darcy DiNucci, between pong and *The Matrix*.[140]

Conclusion

A Web3-enabled Swarmcast2.0 has arrived. Swarmcast2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than the original version, which emerged by 2014.

Swarmcast2.0 circumvents or renders obsolete many of the current tactics intended to disrupt the online activity of the Media Mujahidin.

The need for a strategic-level approach to disruption and collaborative strategies is increasingly pressing and can no longer be held back by the comfort and reassuring rhetoric of the OTS 'success narrative'. The future of disruption efforts requires a Web3 strategy. The risk posed by relying on Web 2.0 disruption approaches in an increasingly Web3 world approaches the equivalence, to lean on Darcy DiNucci's analogy, of planning to play Pong but finding yourself in *The Matrix*.

About the Autor

DR. ALI FISHER

Ali Fisher is an advisor, strategist and author who delivers strategic insight into complex information ecosystems, often containing extreme or illegal content. Ali has a dual specialism in Strategic Communication and Data Science and has worked on Strategic Communication projects for European and US Government Departments specifically focused on achieving and measuring influence.

His analysis has helped organisations build or disrupt networks of influence and impact the flow of information through a community across a diverse range of fields commercial and governmental sectors including Strategic Communication, Public Diplomacy, Counter Terrorism and Child Protection.

Now Director and Explorer of Extreme Realms of Human Cognition and previously Principal Data Scientist at VORTEX, University of Vienna. Ali created BlackLight, the cloud-based system that provides strategic insight into the spread of extremist digital content. Ali previously directed Mappa Mundi Consulting and the cultural relations think-tank, Counterpoint. He worked as Associate Director of Digital Media Research at Intermedia and was lecturer in International Relations at Exeter University. Ali received his Ph.D. at the University of Birmingham.

His books include Collaborative Public Diplomacy (2012), The Connective Mindshift (2013), and Trails of Engagement(2010), Fisher's 2015-2017 CPD Research Fellowship project was titled, Netwar in Cyberia: Decoding the Media Mujahedeen and the Jihadist Swarmcast.

DR. NICO PRUCHA

is Chief Content Curator at Human Cognition. He is a fluent Arabic speaking specialist in Jihadist theology and strategy. His work has covered the use of the internet by Jihadist groups from the mid-2000s to the present and documented shifts in strategy from Forum to Twitter to Telegram.

Main aspects of his research cover the relationship of textual and audio-visual content of jihadist activity online, specifically focusing on the extremist definition of applying theology. Another major focus is the understanding and analysis of the social media strategies used by groups such as the Islamic State in theory and practice. His blog is available at www.onlinejihad.net.

References

[1] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[2] Fisher, Ali. "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence." Perspectives on Terrorism, vol. 9, no. 3.
Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018,
Ali Fisher, Nico Prucha, Follow the White Rabbit – Tracking IS Online and Insights into What Jihadists Share, in Marone, Francesco (ed.) *Digital Jihad: Online Communication and Violent Extremism*. Ledizioni, (2019).
[3] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[4] Prucha, Nico, and Ali Fisher. "Tweeting for the caliphate: Twitter as the new frontier for jihadist propaganda." *CTC Sentinel* 6.6 (2013): 19-23.
Fisher, Ali; Prucha, Nico (2014, August): "The Call-up: The Roots of a Resilient and Persistent Jihadist Presence on Twitter". *CTX*, *4*(3), 73-88.
Jamie Bartlett and Ali Fisher, "How to beat the media mujahideen", DEMOS Quarterly, Issue #5, Winter 2014/15
Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018,
[5] The role of 'embedded academics' in the transatlantic orthodoxy of Terrorism Studies, Jackson, RDW, 'The Case for a Critical Terrorism Studies' (2007) http://hdl.handle.net/2160/1945 and https://pure.aber.ac.uk/portal/files/99753/APSA-2007-Paper-final2.pdf
[6] The claims of victory over jihadi groups covered in depth in:
https://www.eictp.eu/wp-content/uploads/2021/12/FINAL_EICTP_Expert-Paper_Jihadist-Movement.pdf
[7] And by the continued claim of their defeat. The claims of victory over jihadi groups by the covered in depth in:
https://www.eictp.eu/wp-content/uploads/2021/12/FINAL_EICTP_Expert-Paper_Jihadist-Movement.pdf
[8] Dominic Giannini, ISIS app ignored by governments: inquiry, The Canberra Times, NOVEMBER 17 2021
https://www.canberratimes.com.au/story/7515010/isis-app-ignored-by-governments-inquiry/?utm_source=Tech+Against+Terrorism&utm_campaign=4e8f78f06d-EMAIL_CAMPAIGN_2019_03_24_07_51_COPY_01&utm_medium=email&utm_term=0_cb464fdb7d-4e8f78f06d-68658615
[9] THE THREAT OF TERRORIST AND VIOLENT EXTREMIST OPERATED WEBSITES, Tech Against Terrorism, January 2022, p.4
https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf
[10] See for example, Anne Craanen and Charley Gleeson, "The Overlap Between Terrorist Content Online, Disinfomration and the Tech Sector Response", *Spotlight* (RAN, March 2022)
https://ec.europa.eu/home-affairs/system/files/2022-03/spotlight_on_the_digital_ecosystem_en.pdf
[11] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[12] Especially AQ has a long-standing tradition of adopting communication technology and developments for the sole intention to inform why they fight and what for. In the early 2000s AQ initiated a 'digitalization campaign' by producing professional PDFs of theological writings and military handbooks that had been used in the 1980s (Afghanistan), 1990s (Chechnya, Bosnia, Kashmir, Somalia), perhaps most famous among these PDFs is the "Encyclopaedia of Jihad". For a brief description: https://onlinejihad.net/2007/06/03/saying-thanks-to-the-government-of-pakistan-and-the-jihad-of-the-80ties/
[13] Ingram, Haroro J., Craig Whiteside, and Charlie Winter. *The ISIS Reader: Milestone texts of the Islamic state movement*. Oxford University Press, USA, 2020. pp. 7, 225
[14] An earlier report detailed an authentic understanding of Salafi-Jihadi theology distinct from that understood within a Western habitus and the transatlantic orthodoxy of terrorism studies;
Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021.
[15] Conway, M, "Why Deplatforming the Extreme Right is a Lot More Challenging than Deplatforming IS" GNET, 15th January 2021, https://gnet-research.org/2021/01/15/why-deplatforming-the-extreme-right-is-a-lot-more-challenging-than-deplatforming-is/
Also see: Maura Conway, Moign Khawaja, Suraj Lakhani, Jeremy Reffin, Andrew Robertson & David Weir (2019) Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts, Studies in Conflict & Terrorism, 42:1-2, 141-160,
https://www.tandfonline.com/doi/full/10.1080/1057610X.2018.1513984
https://twitter.com/MubarazAhmed/status/1031484324485509121?s=20&t=3nwcSbodsiXRNuXcplirZw
[16] This critique of this approach common within the transatlantic orthodoxy of terrorism studies is discussed in detail in;
Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021.
[17] Critique at the time was offered in:
Fisher, Ali. "No Respite on Social Media After ISIS Attacks in Paris." CPD Blog, 9 Dec. 2017, uscpublicdiplomacy.org/blog/no-respite-social-media-after-isis-attacks-paris.
[18] Conway, Maura, et al. "Disrupting Daesh: measuring takedown of online terrorist material and it's impacts." (2017): 1-45.
[19] Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. *The New Netwar: Countering extremism online*. Policy Exchange, 2017
[20] Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018,
[21] Simon Kemp, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 https://blog.hootsuite.com/simon-kemp-social-media/
[22] https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-103-Favourite-Social-Media-Platforms.png
[23] The graph is unlabelled as most of the channels are still live as of 02 / 02 / 2022
[24] The Global State of Digital 2022, Hootsuite, January 2022, https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-233-App-Annie-App-Ranking-Downloads.png
https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-99-The-Worlds-Most-Used-Social-Platforms.png
[25] An evidence based discussion of the purpose of the Salafi-Jihadi movement is presented in:
Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021.
Where the dominant narrative in OTS is that of building a Jihadi 'Utopia'(comma) the evidence base shows service defined by Salafi-Jihadi theology to be the purpose of the movement.
[26] https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-103-Favourite-Social-Media-Platforms.png
[27] https://www.isdglobal.org/isd-in-the-news/islamic-extremists-troll-each-other-online-and-manage-to-stay-under-facebooks-radar/
MARK SCOTT, Islamic extremists sidestep Facebook's content police, POLITICO, December 19, 2021
https://www.politico.eu/article/islamic-extremists-facebook-content-social-media-islamic-state-terrorism/
[28] https://www.isdglobal.org/isd-in-the-news/islamic-extremists-troll-each-other-online-and-manage-to-stay-under-facebooks-radar/
MARK SCOTT, Islamic extremists sidestep Facebook's content police, POLITICO, December 19, 2021
https://www.politico.eu/article/islamic-extremists-facebook-content-social-media-islamic-state-terrorism/
[29] Images have been edited to obscure user information.
[30] Disclosure: Human Cognition previously worked with YouTube flagging Salafi-Jihadi videos.
[31] Most used as published by Hootesuite, January 2022.
https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-99-The-Worlds-Most-Used-Social-Platforms.png
[32] Charlie Winter and Jade Parker, "Virtual Caliphate Rebooted: The Islamic State's Evolving Online Strategy", Lawfare, (January 2018)
https://www.lawfareblog.com/virtual-caliphate-rebooted-islamic-states-evolving-online-strategy

Berger, Jonathon M., and Jonathon Morgan. "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter." The Brookings project on US relations with the Islamic world 3.20 (2015): 4-1
[33] Paige Cooper, All the Social Media Apps You Should Know in 2021, Hootsuite blog, May 17, 2021
https://blog.hootsuite.com/best-social-media-apps-list/
[34] Simon Kemp, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 https://blog.hootsuite.com/simon-kemp-social-media/
https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Mobile-App-Rankings-Downloads.png
https://blog.hootsuite.com/wp-content/uploads/2021/07/Digital-2021-Report-October-Update-Worlds-Most-Used-Social-Platforms.png
[35] There is significant doubt that the reason Salafi-Jihadi groups set up on Telegram is because of disruption on Twitter.
[36] Charlie Winter and Jade Parker, "Virtual Caliphate Rebooted: The Islamic State's Evolving Online Strategy", Lawfare, (January 2018)
https://www.lawfareblog.com/virtual-caliphate-rebooted-islamic-states-evolving-online-strategy
Berger, Jonathon M., and Jonathon Morgan. "The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter." The Brookings project on US relations with the Islamic world 3.20 (2015): 4-1
[37] Ali Fisher, How Jihadist Groups exploit Western researchers to promote their theology, *Online Jihad*, February 2019,
https://onlinejihad.net/2019/02/18/how-jihadist-groups-exploit-western-researchers-to-promote-their-theology/
[38] Paige Cooper, All the Social Media Apps You Should Know in 2021, Hootsuite blog, May 17, 2021
https://blog.hootsuite.com/best-social-media-apps-list/
[39] Images captured seven days after release (25th November 2021) Channel names have been obscured, but channel icon shows they are distinct channels. View statistics were recorded at the same time but are not mutually exclusive.
[40] View statistics were recorded at the same time but are not mutually exclusive.
[41] Simon Kemp, TikTok Hits 1 Billion Users—Faster Than Facebook (And More New Stats), October 21, 2021 https://blog.hootsuite.com/simon-kemp-social-media/
[42] Jackson, R. D. W. (2007). *The Case for a Critical Terrorism Studies*. http://hdl.handle.net/2160/1945
[43] Mohamedou, Mohammad-Mahmoud Ould. A Theory of ISIS: Political Violence and the Transformation of the Global Order. Pluto Press, 2017. (p.9)
[44] https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-87-Overview-of-Social-Media-Use.png
[45] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[46] Fisher, Ali. "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence." Perspectives on Terrorism, vol. 9, no. 3.
[47] John Arquilla, David Ronfeldt, The Advent Of Netwar, St. Monica: RAND Corporation, 1996, p. 4
[48] http://uscpublicdiplomacy.org/blog/eye-swarm-rise-isis-and-media-mujahedeen
[49] Abu Mus'ab as-Suri, *Call for a Global Islamic Resistance*, (Parts One and Two) December 2004.
[50] http://www.motherjones.com/politics/2014/09/isis-social-media-state-department
[51] One of the major difficulties here is that hierarchy is a form of network structure.- Fisher, Ali. «Mapping the great beyond: Identifying meaningful networks in public diplomacy.» *CPD Perspectives in Public Diplomacy, Paper 2* (2010)
Also see; Edwards, Sean J. *Swarming and the Future of Warfare*. St. Monica, RAND, 2005
[52] The concepts of Emergence and Self-Organisation are, strictly speaking, defined differently,; each term emphasises very different characteristics of a system's behaviour. Both phenomena can exist in a dynamical system. See, for example: De Wolf, Tom, and Tom Holvoet. "Emergence versus self-organisation: Different concepts but promising when combined". *Engineering self-organising systems*. Springer Berlin Heidelberg, 2005, 1-15.
[53] Evelyn Fox Keller. "The Force of the Pacemaker Concept in Theories of Aggregation in Cellular Slime Mold". *Perspectives in Biology and Medicine* 26.4 (1983): 515-521.
[54] Jeffrey Goldstein, 'Emergence as a Construct: History and Issues', *Emergence*, Vol. 1, no 1,
[55] Jeffrey Goldstein, 'Emergence as a Construct: History and Issues', *Emergence*, Vol. 1, no 1,
[56] H. Haken, Synergetics, An Introduction: Nonequilibrium Phase Transitions and Self-Organization in Physics, Chemistry, and Biology (Springer-Verlag, New York, 1983); R. Graham and A. Wunderlin, Eds., Lasers and Synergetics: A Colloquium on Coherence and Self-Organization in Nature (Springer-Verlag, New York, 1987)
[57] The evolutionary metaphor is discussed in greater depth in:
Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018,
[58] Parrish, Julia K., and Leah Edelstein-Keshet. "Complexity, pattern, and evolutionary trade-offs in animal aggregation." Science 284.5411 (1999): 99-101
[59] Cole Bunzel, "Are the Jihadi Forums Flagging? An Ideologue's Lament," Jihadica.com, March 20, 2013
[60] Nader Dabit, What is Web3? The Decentralized Internet of the Future Explained, Freecodecamp.org, 8th September 2021
https://www.freecodecamp.org/news/what-is-web3/
[61] Bobby Allyn, "People are talking about Web3. Is it the Internet of the future or just a buzzword?" NPR, 21 November 2021,
https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision?t=1639411948920
[62] https://www.wired.com/story/web3-gavin-wood-interview/
[63] DiNucci, Darcy, "Fragmented Future". Print Magazine. 53 (4) (April 1999) pp. 32, 221, 222
[64] Bobby Allyn, "People are talking about Web3. Is it the Internet of the future or just a buzzword?" NPR, 21 November 2021,
https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision?t=1639411948920
[65] GILAD EDELMAN, The Father of Web3 Wants You to Trust Less, Wired.com (comma)29th November 2021.
https://www.wired.com/story/web3-gavin-wood-interview/
[66] David Pierce, How IPFS is building a new internet from the ground up, Protocol, October 13, 2021
https://www.protocol.com/ipfs-new-internet
[67] Nader Dabit, What is Web3? The Decentralized Internet of the Future Explained, Freecodecamp.org, 8th September 2021
https://www.freecodecamp.org/news/what-is-web3/
[68] Nader Dabit, What is Web3? The Decentralized Internet of the Future Explained, Freecodecamp.org, 8th September 2021
https://www.freecodecamp.org/news/what-is-web3/
[69] David Pierce, How IPFS is building a new internet from the ground up, Protocol, October 13, 2021
https://www.protocol.com/ipfs-new-internet
[70] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[71] For example an overview of the Salafi-Jihadi use of Telegram is presented here:
Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[72] Prucha, Nico, and Ali Fisher. "Tweeting for the caliphate: Twitter as the new frontier for jihadist propaganda." *CTC Sentinel* 6.6 (2013): 19-23.
[73] Prucha, Nico. "Is and the jihadist information highway–projecting influence and religious identity via telegram." Perspectives on Terrorism 10.6 (2016): 48-58.
Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. *The New Netwar: Countering extremism online*. Policy Exchange, 2017.
[74] https://telegram.org/
[75] https://telegram.org/blog/voice-chats-on-steroids#limitless-voice-chats
[76] https://core.telegram.org/bots

[77] Ali Fisher and Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[78] For detail on the Salafi-Jihadi Nexus see: Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021.
[79] The data to support this finding is presented in:
Ali Fisher and Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[80] A significantly longer version of this analysis is offered in:
Ali Fisher andNico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[81] Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[82] Charlie Winter, Amarnah Amarasingam, "The decimation of Isis on Telegram is big, but it has consequences", Wired, 2nd December 2019.
https://www.wired.co.uk/article/isis-telegram-security
[83] Ali Fisher and Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021
Sicurezza, Terrorismo e Società 15 (1), 141-170
https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf
[84] Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021. p. 23
[85] For example, current options promoted on the site include: KuCoin, Bitdeer, Binance, HOO, Indoex
[86] http://islamhouse.com/en
[87] For a description of the Salafi-Jihadi Nexus see:
Fisher, Prucha, 'Understanding the Global Jihadist Movement 20 years after 9/11', *EICTP Expert Paper*, October 2021. p. 23
[88] https://rocket.chat/company/about-us
[89] https://rocket.chat/company/about-us
[90] To 'Fork' means to take a copy of the source code from one software package and start the development of a distinct and separate piece of software.
[91] About Github: "Millions of developers and companies build, ship, and maintain their software on GitHub—the largest and most advanced development platform in the world" https://github.com/about
[92] https://nextcloud.com/
[93] https://docs.nextcloud.com/server/latest/user_manual/en/
[94] The full domain is intentionally not provided
[95] https://spec.matrix.org/latest/
[96] https://matrix.org/
[97] In addition to paid services, Nginx provides an open source web server that powers more than 400 million websites https://www.nginx.com/
[98] For an explanation of node prerogative see: David Pierce, How IPFS is building a new internet from the ground up, Protocol, October 13 2021, https://www.protocol.com/ipfs-new-internet
[99] System messages not displayed in graph
[100] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019)
[101] https://decoo.io/ offers an IPFS Pinning service discussed in more detail below.
[102] For FAQ relating to IPFS see: https://docs.ipfs.io/concepts/faq/
For a history of the project see: https://docs.ipfs.io/project/history/#a-p2p-summer-1999-2003
[103] Examples of IPFS projects can be found at: https://awesome.ipfs.io/
[104] For an extended introduction to IPFS, see: https://docs.ipfs.io/concepts/what-is-ipfs/
[105] https://docs.ipfs.io/concepts/what-is-ipfs/#decentralization
[106] https://docs.ipfs.io/concepts/what-is-ipfs/#decentralization
[107] https://docs.ipfs.io/concepts/what-is-ipfs/#participation
[108] The attempt to make Wikipedia 'uncesorable' via IPFS is discussed in: "Uncensorable Wikipedia on IPFS", May 2017
https://blog.ipfs.io/24-uncensorable-wikipedia/
[109] https://wiki.decoo.io/general/gettingStarted
[110] https://git-scm.com/
[111] http://bittorrent.org/
[112] https://en.wikipedia.org/wiki/Kademlia
[113] https://eth.wiki/
[114] https://bitcoin.org/en/
[115] https://github.com/ipfs/ipfs#quick-summary
[116] Screenshot taken 4th February 2022.
[117] The emphasis on blue collar knowledge can be found in:
Lohlker, Rüdiger. "Collective Organizers: Lone Wolves, Remote Control, and Virtual Guidance." *World Wide Warriors* 1 (2019): 157-192.
[118] See for example the 105th edition of the Arabic language magazine al-Jihad (February, 1994) with the territorial gains made in Afghanistan and the question of state rule.
[119] https://www.cloudflare.com/web3/
[120] See: https://eth.link/
[121] See: https://eth.link/
For examples of use see: https://ens.domains/
[122] The Threat of Terrorist and Violent Extremist Operated Websites, Tech Against Terrorism, 28 January 2022.
https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf
[123] The Threat of Terrorist and Violent Extremist Operated Websites, Tech Against Terrorism, 28 January 2022.
https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf
[124] http://f####s4fw3s5bi3enjrompr6kxpywkscqmmcvyiyey3xamrv5zjllgad.onion
[125] https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router
[126] Stuart Dredge, What is Tor? A beginner's guide to the privacy tool, The Guardian, 5th November 2013,
https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser
[127] Stuart Dredge, What is Tor? A beginner's guide to the privacy tool, The Guardian, 5th November 2013,

https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser
[128] https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption
[129] https://www.myrasecurity.com/en/what-is-the-darknet/
[130] See https://www.torproject.org/download/ and https://onionbrowser.com/
[131] https://tb-manual.torproject.org/make-tor-portable/
[132] https://gettor.torproject.org/
[133] https://web.archive.org/web/20171027203659/https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html
[134] https://www.bbc.com/news/technology-50150981
The onion link was later updated to:
https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/
[135] https://www.dw.com/en/dw-websites-accessible-via-tor-protocol/a-51338328
DW News: https://dwnewsgngmhlplxy6o2twtfgjnrnjxbegbwqx6wnotdhkzt562tszfid.onion/
https://www.rfa.org/about/releases/mirror_websites-04172020105949.html
[136] Proton Mail: https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/
Facebook: https://www.facebook.com/onion-service, https://facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion
New York Times: https://www.nytimesn7cgmftshazwhfgzm37qxb44r64ytbb2dj3x62d2lljsciiyd.onion/
Lily Hay Newman, The CIA Sets Up Shop on Tor, the Anonymous Internet, Wired.com, May 7, 2019 https://www.wired.com/story/cia-sets-up-shop-on-tor/
CIA Tor Service: ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion
Others are listed: https://opensourcelibs.com/lib/real-world-onion-sites
[137] The process is discussed here: https://opensource.com/article/19/8/how-create-vanity-tor-onion-address as with many things increased computing power can be used to shorten the process.
[138] The Threat of Terrorist and Violent Extremist Operated Websites, Tech Against Terrorism, 28 January 2022.
https://www.techagainstterrorism.org/wp-content/uploads/2022/01/The-Threat-of-Terrorist-and-Violent-Extremist-Operated-Websites-Jan-2022-1.pdf
[139] Custom element of the link obscured: http://f####s4fw3s5bi3enjrompr6kxpywkscgmmcvyiyey3xamrv5zjllgad.onion
[140] DiNucci, Darcy, "Fragmented Future". Print Magazine. 53 (4) (April 1999) pp. 32, 221, 222