

ISD

Powering solutions
to extremism
and polarisation

The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook

Moustafa Ayad

13th July 2020

The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook

Moustafa Ayad

Executive Summary

In the last two years, Facebook's transparency reporting shows the company detecting and deleting 99 per cent of terrorism-related posts — about 26 million pieces of content — before they were reported to the social network. But what about the remaining one per cent?

This new investigation from the Institute for Strategic Dialogue (ISD) delves into the inner workings of a pro-ISIS account network on Facebook, providing a case study of the resilient network dynamics, technological loopholes, and cross-platform activity that allowed a web of accounts to survive and flourish for over three months on a platform which purports to be a hostile environment for terrorist actors.

This specific pro-ISIS network — comprised of several hundred accounts and reaching audiences in the tens of thousands — represents one island in an archipelago of self-contained but interlocking networks geared towards spreading terrorist content on the platform. Our qualitative study only scratches the surface of this ecosystem, providing examples of what insights can be uncovered through manual investigation. Such analysis needs to be scaled up and automated to understand the true scope and nature of the challenge.

Key Findings

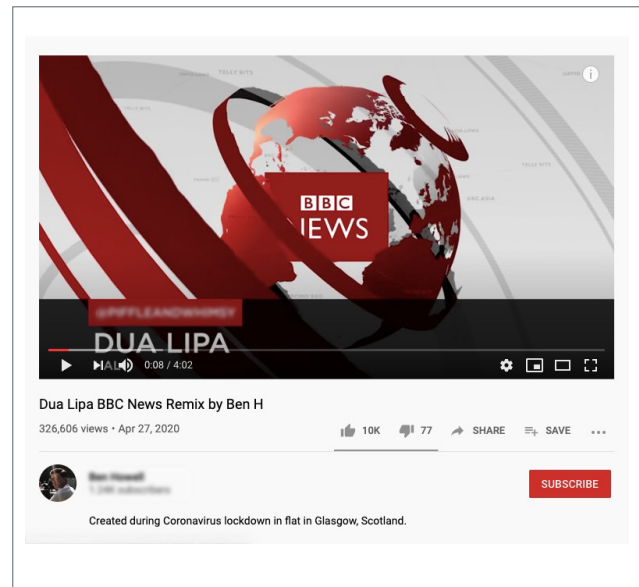
Through ethnographic monitoring, ISD researchers tracked, analysed and dissected the behaviours of a network of pro-ISIS Facebook accounts which branded itself the Fuouaris Upload across the platform, from April 7 to July 3 (87 days). Of 288 pro-ISIS accounts discovered during this monitoring — many of whom had followings in the thousands — a third (90 accounts) were controlled by one user named Luqmen Ben Tachafin, which comprised the core of the network. By May 21, the network had shared 50 pieces of video content and had collectively garnered more than 34,000 views.

During the three months of ISD analysis, the Fuouaris Upload network expanded to other platforms, namely SoundCloud, where it currently controls 18 branded accounts that have seeded 91 pieces of ISIS audio content. While 70 percent of the Fuouaris Upload accounts were taken down during the monitoring period, these decentralised networks demonstrated considerable resilience. Sixty-two of the core accounts were removed, but 28 identical accounts remained, highlighting the uneven nature of moderation. As individual accounts were taken down, ISIS users mocked Facebook moderators for not understanding the scale of their presence across the platform.

What is evident from ISD's research are the new evasion tactics being employed by ISIS supporters, seemingly geared towards stymieing either automated or manual detection and moderation of terrorist content and accounts. Researchers identified six central tactics that allow these accounts to survive, sidestep, and continue to seed ISIS content across the platform:

Account Hijacking: ISIS supporters appear to be exploiting a major loophole on Facebook to hijack accounts from other users, using two applications that facilitate the intercepting of password reset text messages sent by the platform. A number of accounts not only detailed this tactic, but produced and shared tutorial videos in order to teach their fellow e-jihadists across the platform how to exploit this weakness in Facebook's account security protocols.

Content Masking: The survival of ISIS content on Facebook relies on cosmetic modifications, including video effects that overlay popular news outlet branding on 'official' ISIS propaganda (e.g. France24, Russia Today and the BBC), as well as blurring overt ISIS iconography. Such content appears to be bypassing Facebook's hashing technology for the automated detection of terrorist material, which is seemingly unable to identify lightly-edited 'official' terrorist media.



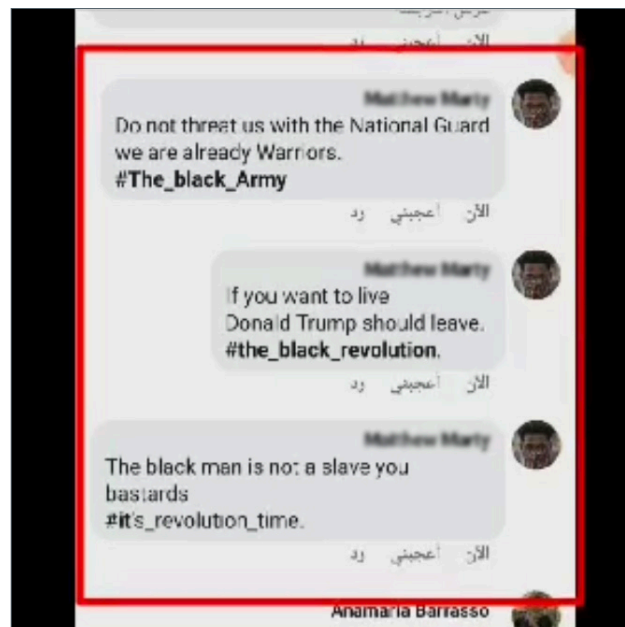
Link Sharing: Decentralised networks of ISIS supporters are using comment threads to share links to known jihadi sites, mimicking tactics from encrypted platforms such as Telegram and Hoop. One account tracked through the Fuouaris Upload network, posted 21 shortlinks in a 21-day timespan to a diverse array of ISIS-linked websites, newsletters, and videos, in the comments section of its Facebook wall. The posts including the shortlinks were shared 2,412 times during that time period. Another group of users, although seemingly opposed to ISIS, nonetheless shared links to "The Punishment," a jihadist website touted as the "ISIS Netflix," which has garnered 234,000 views over the past month. A direct link to the website was found graphically overlaid onto an ISIS video of an attack on Egyptian armed forces in the Sinai Peninsula.

Coordinated Raids: Networks of ISIS supporters on Facebook are plotting, preparing, and launching organized "raids" on other Facebook pages, including those of the US Department of Defence, US Army and the US Air Force Academy. ISD researchers



witnessed these “raids” in real time, as followers posted instructions including the “target,” “objective” and content needed to flood comment sections with terrorist material. This raiding network had two Facebook pages as central gathering points during the monitoring period, both of which were taken down. One “raid” on US President Donald J. Trump’s Facebook page involved creating fake African-American accounts and carrying out high-volume posting in the comments section, with comments including “weapons not only for the white we can shot them too #war_timeweapons not only for the white we can shot them too #war_time” [sic]. Similar tactics were used to attack comments sections on the US Department of Defence and US Air Force Academy Facebook pages, using images of the smouldering World Trade Centre emblazoned with the words “we will do it again wait for the date.” The US Air Force Office of Special Investigations is now launching an inquiry into the “raid.”

Hashtag Hijacking: A number of these raids appeared geared towards generating polarisation around global protests (including in Lebanon and the United States). ISIS-linked accounts used George Floyd’s avatar to post “marching to the edge you make it a challenge and we will revenge #The_Black_Is_Back.” This resembles tactics used by pro-ISIS accounts around the Ferguson protests of 2014, which aimed to hijack online discourse around divisive social issues and spread propaganda through the co-option of popular hashtags.



Gaming Text Analysis: Accounts were seeking to evade text analysis moderation by using a “broken text” format in their posts, or specialized fonts. A prime example of this was a recently-released ISIS Syria video, which included numerous beheadings and was not taken down more than two weeks after its posting, likely due to the fact the offending user described the video as “the terrorist Daesh.” If moderators had checked the user’s history, they would have found them posting ISIS content throughout June, and that this video served as a key source of digital propaganda for other accounts — it was viewed more than 16,300 times and shared 472 times by other ISIS-supporting accounts.

The case study presented in this report, and the tactics and behaviours of decentralised networks across Facebook, indicate just how interconnected ISIS supporters are online. It underscores the need for further investigative work into these resilient pockets of terrorist support across platforms, which seem to be evading Facebook’s efforts to improve “image matching,” target “terrorist clusters,” and deepen terrorist “language understanding”, as well as train artificial intelligence approaches to detecting “text that might be advocating terrorism.”

Not only are terrorist group and ideologue avatars easily found across the platform, but our research unearthed dormant and inactive accounts with avatars that have branded terrorist insignia like the al Qaeda flag, as well as users dubbed Amiriki al-Qaeda with bios that list work occupation as “jihad” or at “Islamic State.” Users who were clearly repeat offenders continued to hijack new accounts after they were taken down, patterns of behaviour that were seemingly not interrupted. Meanwhile, terrorist-supporting accounts that launched coordinated campaigns to “raid” other Facebook pages were not removed from the site almost a full week after the “raids” had been conducted. The accounts gloated about being able to game the system, and boasted of their intention to keep conducting terrorist activity on the platform.

While these highlight single instances of evasion, the Fuouaris Upload network reveals a more systemic set of gaps that need addressing. The primary insight from this case study is that Facebook’s automated and manual moderation practices need to be coupled with real “street level” understanding of these users’ tactics and behaviours. Until that is accomplished in a more transparent, systematic, and coordinated fashion, these ISIS-supporting accounts will continue to remain and expand their playbook of platform exploitation tactics. Facebook confirmed that of the 288 accounts analysed in this report, 250 were removed naturally via the platform’s counter-terrorism protocols, while 30 remained live without detection. Facebook later removed the 30 that remained live without detection. These users have since been flagged for imminent review and actioned by the moderation team. They also highlighted the crucial role played by the Trusted Partners programme, which allows expert third parties to flag terrorist content and trigger an expedited review.



The Knights

The Fuouaris Upload network draws its inspiration from knights from a golden era of Islam. Fuorusiyya (knightsmanship), was a scientific practice of warriorhood that peaked in the 14th century and required mastery of equestrianism, archery and swordsmanship. Eliciting visions of this practice, the Fuouaris Upload network is a new type of knight, albeit digital. They loot Facebook for accounts, spread the Salafi-jihadist¹ gospel, and hunker down for digital tit-for-tats with automated and manual detection systems on the platform. The network, its members, and those in its ambit recognise the strength of their opponents but continue to fight because they are, in their words, a “super-spreader”, determined “to flood” Facebook with “wave after wave Islamic State of Iraq and Syria (ISIS) content”.²

Researchers from the ISD traced a network of 90 accounts at the core of the Fuouaris Upload network on Facebook. These accounts were discovered via links shared by a daily, regenerating set of ISIS-content-sharing accounts on Twitter that linked to Facebook Watch Parties³, hosted by key accounts within the network. Seizing on gaps in both automated and manual moderation on Facebook, the Fuouaris Upload network is not just a case study into the tactics and strategies of a new generation of ISIS supporters online, but it highlights an integrated, multilingual and multiplatform approach to seeding official and do-it-yourself terrorist content on platforms such as Facebook, Twitter and SoundCloud.

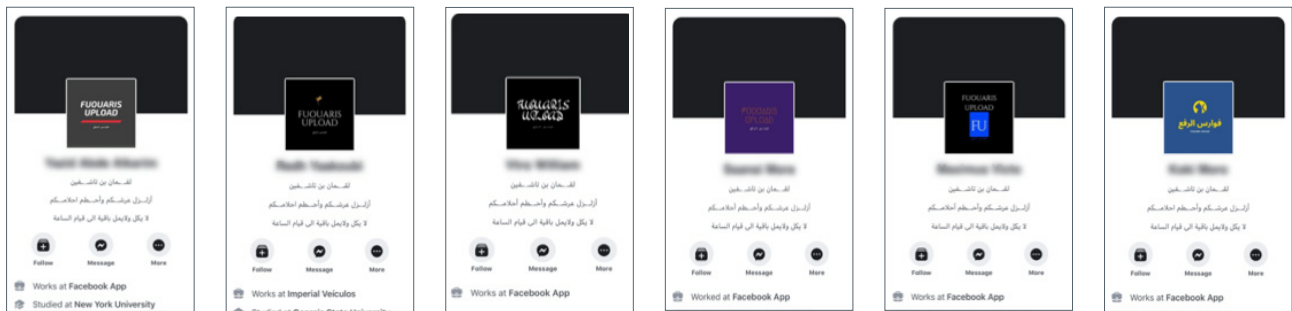


Figure 1: Sample of Facebook accounts from the Fuouaris Upload network.

While there were 90 primary accounts at the heart of the Fuouaris Upload network on Facebook, researchers actually identified 288 ISIS accounts that were part of the friends and follower bases of the Fuouaris Upload set of accounts. These accounts make up a loosely networked community of Arabic, Indonesian, Ethiopian, Somali, Bengali, and Albanian-language ISIS supporters on the platform. Researchers did not just uncover the Fuouaris Upload network, but others connected to its followers with similarly branding profiles that have created their own disparate communities to pump out ISIS content. Just like the Fuouaris Upload network, these profiles have calling card avatars and specialised fonts that distinguish them. These networks within networks are growing, adapting, and ultimately continuing to blunt the effect of takedowns.

These polyglot networks of accounts on Facebook have similarly adapted their content to suit a COVID-19 pandemic reality, creating pages that celebrate the daily “kuffar kill counts”⁴ of the coronavirus while sharing official ISIS COVID-19 content. This network is sustaining its existence by duplicating numerous key accounts, sharing links to new profiles, and hoarding placeholder accounts as a repository of backups prepared for eventual takedowns. The accounts thrive off sharing links to a number of ISIS websites and cloud-storage drives that house gigabytes-worth of ISIS content. Simultaneously, the accounts connect the various nodes of the network to encrypted messaging applications such as Telegram, which was the subject of a EUROPOL cull to root out ISIS and al-Qaeda communities on the platform, and inadvertently dispersed ISIS supporters across a range of disparate platforms.⁵

In the wake of Facebook’s announcement of an official oversight board to: “help Facebook answer some of the most difficult questions of expression online: what to take down, what to leave up, and why”,⁶ the Fuouaris Upload network and the profiles and pages in its sphere of influence pose an immediate challenge to manual and automated moderation. While the oversight board represents an attempt to deal with the broader issues with “grey zone” content on the website that call into question the lines drawn between

freedom of expression and censorship, there are still lingering and long-standing issues on the platform with clearly terrorist content that violates the platform's guidelines.

A key issue is the lack of transparency about the tools used to automate moderation beyond the "hashing" of terrorist content, which is an algorithmic process to root out terrorist content based on practices: "to identify and remove copyrighted material from the internet."⁷ What is clear is that the Fuouaris Upload network seemed to be frustrating those automated efforts and, similarly, manual detection practices. Researchers have been studying the use of social media by ISIS supporters since the introduction of the group onto the world stage.⁸ While much of the research has delved into the mechanics and content of these accounts and its supporters, there has been less attention paid in an era where the world has turned its attention to the spread of a global pandemic, as key Islamic State figures have been assassinated, and territorial ground has been lost.

This report seeks to present a glimpse into a new era of ISIS support on Facebook, one that ultimately has ties to the preceding years but also presents new challenges for companies, governments and community groups actively working to root out the vestiges of ISIS support online. Using the Fuouaris Upload network of accounts as a case study, ISD researchers have pinpointed new dynamics and mechanics used to sustain, seed and sow fertile soil for continued social media propagation. The persistence and the perseverance of this fledgling ISIS network on Facebook can be attributed to practices and learnings built on years of takedowns, as well as a clear gap in moderation that has only emboldened these digital "knights" to, in the words of ISIS supporters themselves, "remain" and "expand".

Avatars and Auxiliary Accounts

Researchers began tracking the Fuouaris Upload network on 7 April 2020, when a series of hijacked or bought ISIS Twitter accounts began tweeting out links to Facebook watch parties for a video titled "The Grit of War — The Bloodshed of Mosul", connected to a Facebook account. The first account linked through these tweets was named Miro Williams and the content was an ISIS video about the siege of Mosul.⁹ Researchers tracked Miro Williams to other accounts on Facebook that shared the same avatar, albeit with different profile names and with each sharing different pieces of ISIS content. The accounts' avatars, each with a geometric symbol and the words Fuouaris Upload in Arabic and English, signalled that they were part of a coordinated effort by ISIS supporters to begin amassing territory on Facebook.

Researchers found that the first Fuouaris Upload account to appear on Facebook was on 21 March and was dubbed Ibrahim Nouh. The Ibrahim Nouh account — like nine others within the Fuouaris Upload network — did not share content and instead was positioned as a placeholder account to be used as a backup once other network accounts were either taken down or needed to seed new content. Out of 86 Fuouaris Upload accounts tracked, 66 accounts within the network claimed to work for the Facebook App or Facebook. On the first day of Ramadan, the network introduced a network member named Ramadan Karim, the traditional first-day greeting of the holy month of fasting, also claiming to be an employee at Facebook App. All of the accounts featured the same bio, which read in Arabic: "Luqmen Ben Tachafin. I shake your throne and destroy your dreams. Never tired, never bored, until the Judgement Day."

ISD researchers pinpointed the Luqmen Ben Tachafin account as the genesis of the Fuouaris Upload network, based on the linkages in the accounts and several other factors. The account bio states it is the: "primary account of the Fuouaris Upload, and the primary defender who shakes thrones and destroys dreams",¹⁰ followed by an emoji of two crossing swords and a burning flame. In fact, the Luqmen Ben Tachafin account not only seemingly controls the rest of the Fuouaris Upload accounts, but also at one point in time during the period of ISD monitoring and tracking of the network, controlled four accounts with the same name.

The tactic seems to allow that the account holder could survive content takedowns, shifting content from one account to the other, posting content natively on one account and then fanning it out through the other accounts. The strategy also guarded against suspensions. During ISD's monitoring and tracking period, all of the Luqmen Ben Tachafin primary accounts were eventually suspended. The account, however,

returned under a new name, Thabat Mounacar, which was promoted in public posts by the two remaining Luqmen Ben Tachafin accounts. The day of the suspension, the accounts posted requests for “the brothers in aqidah (ideology)” to follow and share the new account — Thabat Mounacar — as the primary account.

The Luqmen Ben Tachafin accounts seem to be either hijacked or bought Facebook accounts, a similar tactic used for the daily horde of ISIS Twitter accounts ISD researchers previously tracked and monitored in the immediate aftermath of the death of ISIS ideologue Abu Bakr al-Baghdadi.¹¹ Researchers found that two of the Luqmen Ben Tachafin accounts still had profile photos linked to other people, presumably the account holders, which date back to 2010 and 2016. Based on the profiles’ URLs, one account seemed to belong to a user called SG, and the other to an SP, whose photos with “Jesus is the Greatest Gift” filter remained on the account.¹²

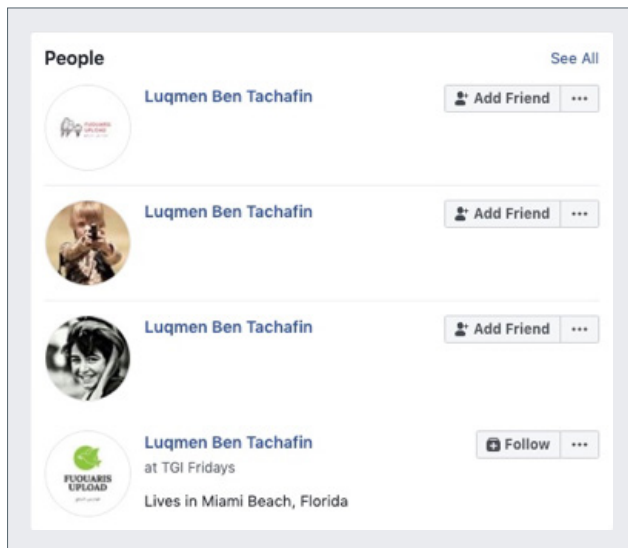


Figure 2: Researchers identified four Luqmen Ben Tachafin accounts.



Figure 3: Remaining Luqmen Ben Tachafin accounts signpost to new primary account

During the time period ISD was monitoring and tracking the Fuouaris Upload network accounts on Facebook, researchers noted select followers and friends of all the Luqmen Ben Tachafin accounts utilising the same tactic. Sinan Güner, one of these followers, seemed to be controlling four other accounts with different names but with the same avatar. All the accounts were sharing ISIS content and each noted in their bios that the accounts were mughtanim (war spoils). Researchers found a number of these duplicate, ISIS auxiliary accounts. The Luqmen Ben Tachafin account was the only one that used the exact same profile name for all its auxiliary profiles.



Figure 4: Post by Hiatham al-Qurayshi starting with “Takbir”, followed by “Mosul”.

The account Cris Silvia Monteiro boasted about three other accounts under its control. Each of the accounts had the same avatar and each was posting ISIS content.¹³ Researchers tracked the account between April and May 2020 and recorded seven connected accounts. The account did not hide the fact that it was controlling numerous others – on 6 May the account posted: “I have 100 war spoils accounts and I won’t give them to anyone [smiling emoji with tongue sticking out]. They delete one account, and I replace it with 10 others.” Each of

the accounts used a different screenshot from an ISIS video as a cover photo. Beyond the use of multiple accounts to seed ISIS content across Facebook, and the use of auxiliary accounts if one is suspended or taken down altogether, these networked profiles continuously signposted other users to micronetworks of ISIS-content spreading accounts.

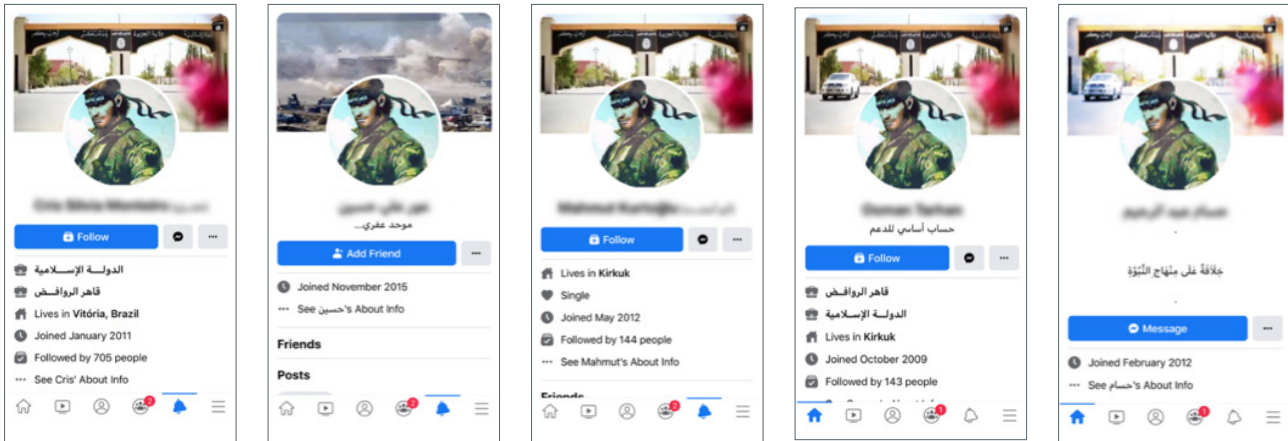


Figure 5: Accounts controlled by account Cris Silvia Monteiro.

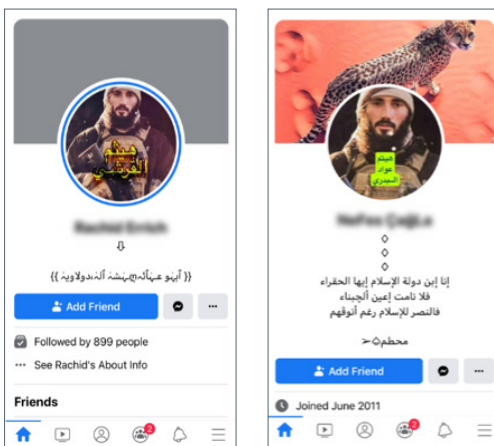


Figure 6: Two accounts with Hiatham al-Qurayshi's calling card.

Researchers noted instances of this tactic continually throughout the monitoring period. The account Hiatham al-Qurayshi was connected to at least three accounts and a public page masquerading as a personal blog with 1,974 followers. The page functioned as a gathering place for other ISIS accounts on Facebook and was a primary location to find veiled blog posts functioning as official ISIS news bulletins. Post after post on the page would begin with “Takbir” (the greatness of God), followed by a location, such as Mosul, Kirkuk, or Salah el-Din, then a bulletin about an ISIS attack, explosion, or capture of soldiers and/or weapons. They were often congratulatory and mimicked the language of official ISIS bulletins from outlets such as the al-Amaq News Agency and the al-Nabā newsletter. The accounts would share the origins of the news in the first comment under one of these posts, providing the page’s following with the official ISIS source.

Hiatham al-Qurayshi’s calling card, which researchers tracked, was a photo that included the same ISIS fighter with the words Hiatham al-Qurayshi emblazoned across the chest. These accounts used anglicised, Turkish and Arabic profile names and connected up to 3,000 other accounts that were either leftover from the previous account holders or newly-added ISIS accounts. The lifeblood of these accounts was ISIS content (video, audio, standalone photographs, and print). The ability to spread ISIS content through these networked auxiliary accounts was continually trialed and tested throughout ISD’s monitoring period, some with much more success than others.

Content Cloaking

The accounts within the Fuouaris Upload network proficiently seeded ISIS content across Facebook from March until May 2020. Researchers found 50 pieces of content, excluding the central account of Luqmen Ben Tachafin, which functioned like an aggregator for all of the content seeded through the network. Those 50 pieces of ISIS content generated more than 34,000 views and managed to survive for a month on Facebook.

Central to its survival was a set of critical, boilerplate tactics that seemed to confuse the branding of ISIS content long enough to save it from takedowns. Using a 52-minute long Islamic State in Yemen video — a violent hate-laden screed levelled against al-Qaeda and political Islamist organisations like the Muslim Brotherhood released on 29 April — researchers were able to track the content seeded through the Fuouaris Upload network and note how the video was masked, cloaked and edited to get past both automated and manual detection. The same tactics to mask the content were used for all of the Fuouaris Upload network’s content.

Nassim Oussama, a Fuouaris Upload network account created on 30 April, shared the ISIS Yemen video on 1 May, generating some 239 views, 84 shares and 23 reactions 24 hours after it was posted. The account noted the video was being reshared based on the fact it was deleted previously, stating it was “new and in 480P format”.¹⁴ How the account uploaded and stopped takedowns is based on several factors, the first being content-masking. The Yemen video and others shared by the Fuouaris Upload network begin with a 36-second introduction that is part-Quranic recital and part-mainstream content. This 30-second gap is not terrorist or extremist content and is essentially used as a ploy to assist in fooling detection practices. The hope is that moderators or software used for moderation will spare the video since it does not have the trappings of ISIS content. The content beyond the initial Quranic introduction is followed by a few seconds lifted from a Journeyman Pictures documentary filmed in 2014 and titled “An Insight into ISIS”. At roughly the 36-second mark, the documentary film cuts into the official ISIS video with its branding intact.

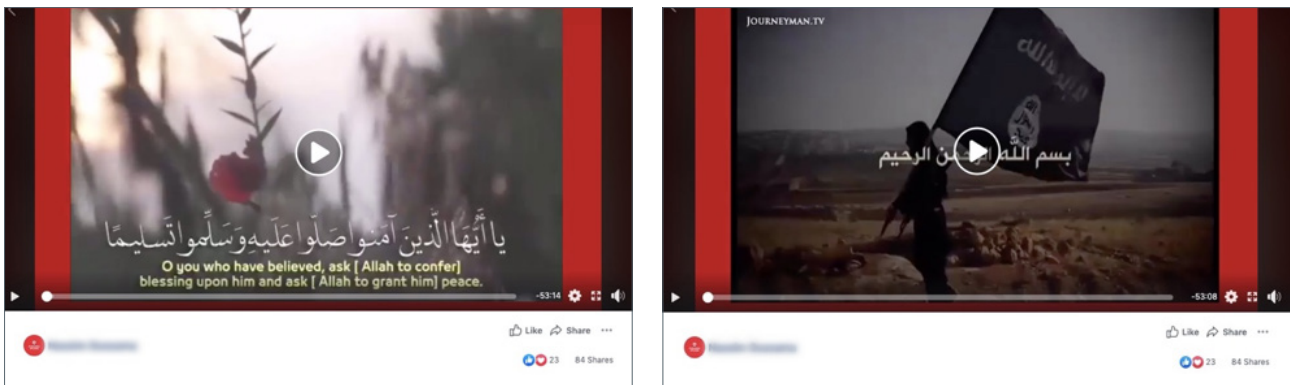


Figure 7: Video shared by account Nassim Oussama that masks ISIS content with an introductory Quranic recitation.

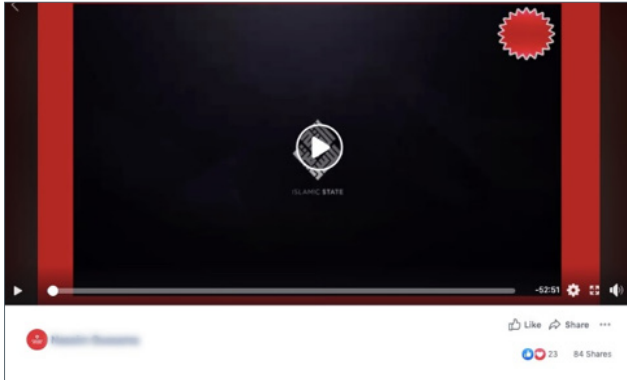


Figure 8: A red symbol conceals ISIS’s logo

With an introduction edited in from a combination of non-terrorist or extremist content, the next step is to mask the branding of the ISIS video. This is accomplished by graphically overlaying a symbol that covers the official ISIS Yemen logo in the video as it plays. This tactic was used by all the Fuouaris Upload accounts and was not exclusive to the Yemen video. The Fuouaris Upload account Billal Rida shared two ISIS videos on 18 April. The videos were testimonials from ISIS fighters in Aleppo, and specifically about infighting between groups in northern Syria. Similar to the Yemen video shared by the Nassim Oussama account, the video begins with 18-seconds of the Journeyman Pictures

documentary before launching into the official video from the ISIS stronghold in Aleppo, once again masking the trappings of the ISIS brand with a symbol concealing the logo in the right-hand corner. The video amassed some 765 views, 44 shares and 31 reactions in a three-week period.

Not all of the Fuouaris Upload network required this amount of masking, cloaking and reediting of content. In some instances, the network accounts created completely new content. Often times these were videos that were created purely from ISIS audio content. The network account Youcef Ibrahim was one such account. Appearing on 28 April, the account shared a 2hr 30min-long audio message titled “rules for those who do not excommunicate unbelievers”, a two-part audio series delivered by Shaykh Abu Malik al-Tamimi, a Saudi cleric turned Islamic State foreign fighter and “mujahid shaykh”¹⁵ who died in Homs in 2015. For a 2hr 30min-long piece of media — a duration that would often represent a death knell for social media promotion — it accrued 29 shares. Its ability to survive was purely based on the lack of ISIS insignia on the video. Instead, the video opened with on-screen text that seemed rather bland — retrograde graphics are a hallmark of this network — that read the title of the piece and then the words: “Shaykh al-Muhajid Abu

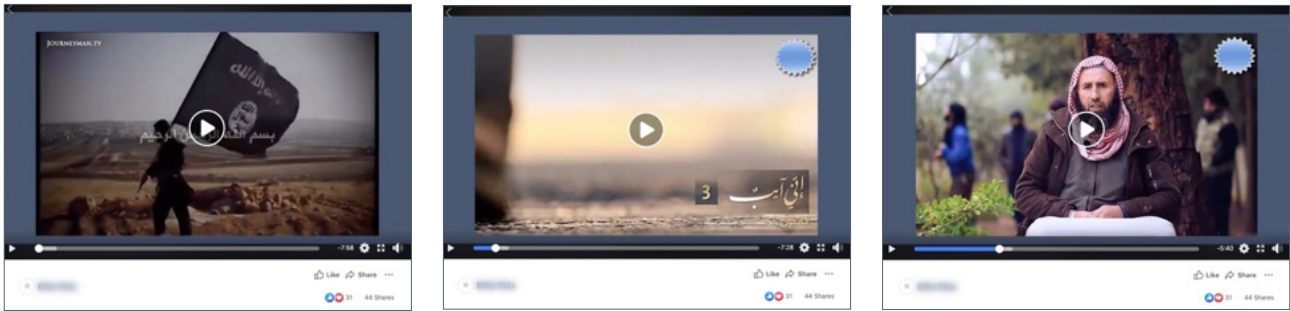


Figure 9: Account Billal Rida shares testimonials from ISIS soldiers in Aleppo, with the ISIS brand masked by blue circles.



Figure 10: A 2hr 30min-long audio message titled “Rules for those who do not excommunicated unbelievers” shared by account Youcef Ibrahim.

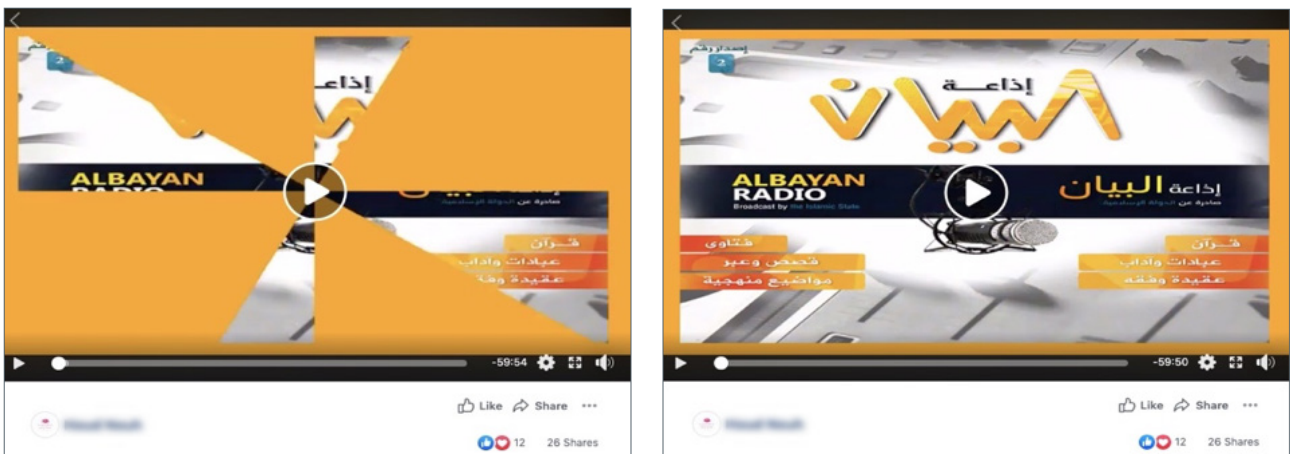


Figure 11: An account by the name of Houd Nough shares a video version of audio content from ISIS’s al-Bayan radio station. The video starts with a harmless orange screen that then disappears to reveal al-Bayan’s logo.

Malik al-Tamimi, may God bless him.”¹⁶ This was followed by a screenshot image of al-Tamimi that stayed in place for the full length of the video.

The Fuouaris Upload account Houd Nough similarly shared ISIS audio content, only instead of a lesson delivered by an ideologue, it was an hour-long programme from ISIS’s al-Bayan radio station, which was bombed off the FM airwaves back in 2016.¹⁷ The video shared by the Houd Nough account began as an orange screen that faded into a 1980s-esque windmill graphic, revealing a stationary ISIS al-Bayan logo that stayed on screen for the length of the video. The video, withstanding takedowns by either manual or

automated detection, is slightly remarkable as it is clearly ISIS content and uses the radio station's well-known logo. The video also contains on-screen text that clearly reads "broadcast by the Islamic State" in both English and Arabic on the stationary image that lasted the full hour of the video. The ability of this particular piece of content to withstand takedowns was likely due to the fact that it is completely do-it-yourself content and no existing hash of the video would be in place to prevent it from being uploaded. However, what automated detection likely could not assist with would presumably be flagged by manual moderators, who should be trained on the official logos and content that ISIS has put out over the years.

The Fuouaris Upload network's content used a mix of masking, cloaking and reediting to ensure the continued survival of ISIS content on Facebook. However, the multilingual accounts within the friends and followers' bases of these 86 accounts, which number in the tens of thousands, do not. Researchers analysed a subset of these accounts in order to understand if the dynamics and strategies employed by the network influenced its faithful base of followers.

Polyglot Pals in Propaganda

Tucked away among the followers and friends of the Fuouaris Upload network on Facebook are multilingual profiles of ISIS supporters that are self-sustaining ISIS Albanian, Turkish, Somali, Ethiopian, and Indonesian-language communities. While they might not function as a network as the Fuouaris Upload accounts do, the profiles use similar tactics and often share ISIS media overtly rather than attempting to mask or cloak the content. Researchers found that these accounts, and specifically in these languages, seemed to be less heavily moderated than the Arabic ISIS accounts. However, it was unclear why these accounts in particular languages were able to brazenly post ISIS-branded official media across the platform.

An account named Abu Surya shared the most disconcerting piece of content found in the multilingual set of profiles in the Fuouaris Upload network's ambit of friends and followers. The Indonesian-language account posted five full-length official ISIS videos over the course of the first week of May. On the 8 May, a video subtitled in English and Indonesian, of an ISIS fighter took viewers through a how-to video on the creation of an explosive made by mixing household items.

The video, produced by the wiliyat, or in English, state, of Raqqa, was posted by the account with no attempts at masking the logo, its origins or its content. Set in an undisclosed kitchen, complete with a bowl of fruit in the background, a sole fighter named Abu Nur al-Shami wears a black balaclava and desert camouflage while mixing and carefully crafting an improvised explosive device out of household items in a scene reminiscent of the al-Qaeda in the Arabian Peninsula Inspire magazine article "make a bomb in the kitchen of your mom".¹⁸ That article would go down as inspiring the Boston Marathon bombers in 2015 and countless others.



Figure 12: A screenshot from a tutorial on how to create the explosive, "White Ice", shared by account Abu Surya.

The video was shared 41 times through other Indonesian and Arabic-language accounts. Researchers flagged the video based on its dangerous nature, and it was removed within 24 hours. One of those accounts, Dian Bekam Refleksi, shared the bomb-making video first shared by the Abu Surya account. The Dian Bekam Refleksi account's avatar was a screengrab of the logo of an Arabic-language learning application created by ISIS – harouf (letters). The account's cover photo was of a child in military garb holding a pistol pointing toward the sky underneath the Seal of Muhammad, which has doubled as the ISIS flag since the group's founding. Another account Oranglama Akunbaru was connected to the Fuouaris Upload network as well as both the Dian Bekam Refleksi and Abu Surya Indonesian-language accounts.



Figure 13: One of the branded-ISIS videos shared by account Abu Surya.



Figure 14: Video content shared by account Oranglama Akunbaru.



Figure 15: Account Sariyatu Nashri shares an infographic from ISIS's al-Naba newsletter.

The Oranglama Akunbaru account continuously denigrated democracy as anti-Islamic and criticised “infidels” in its posts. In one post, the account mixed both, claiming democracy was an infidel system, and then proceeded to seed two pieces of ISIS official content in the comment threads. The two videos, produced by the ISIS-linked al-Hayat Media Center, slammed Muslims that did not take sides in the war between ISIS, Arab governments, and the West, as murtad (apostates – someone who rejects Islam).

All of the Indonesian-ISIS accounts traced during ISD’s monitoring period were linked to more than 500 followers and friends, exponentially increasing the chances these videos would be reshared across the platform and increasing the potential for them to bridge divides between Indonesian and other ISIS supporters on Facebook. Researchers tracked accounts in one language only to be linked to other accounts exhibiting similar dynamics in Amharic and Somali languages.

For instance, the three accounts of Sairyatul Nashri were central to the ISIS-supporting Somali community on Facebook sharing and reposting ISIS content. Each of the accounts had the same avatar, a stylised version of the racing car video game Grand Turismo that read Faafinta Guutada. Each of the accounts’ avatars had a number in the lower portion of the “F” signifying the different accounts, all of which were presumably held centrally.

Connected to some 804 friends all three of the accounts were responsible for sharing repurposed ISIS content in Somali. Faafinta Guutada 1 primarily shared news bulletins from al-Amaq and al-Naba newsletters, Faafinta Guutada 2 shared more photographs from official ISIS sources. And Faafinta Guutada 3 was an amalgamation of the first two accounts but shared more videos as well as links to archive.org repositories of al-Hijrateyn radio, a Somali version of the ISIS al-Bayan radio station.

Linked to this series of Somali accounts was the Ethiopian account አልሙዊዲያ ሐበሺያ, which donned an avatar of a Kalashnikov rifle next to an ISIS flag and a Quran. On 29 April, the account posted a jubilant account of the ISIS Yemen video — attacking al-Qaeda and its affiliates such as al-

Shabaab — with four downward finger emojis pointing at the comment section. In the comments section, the first post by the account holder was a Facebook story with a snippet of the latest ISIS video. The two subsequent posts were two full-length versions of the same ISIS Yemen video already shared by the account holder. Other users in the same comment thread followed suit, posting more versions of the video. The use of the comments section as a means to share official ISIS content was a strategy used by other ISIS-

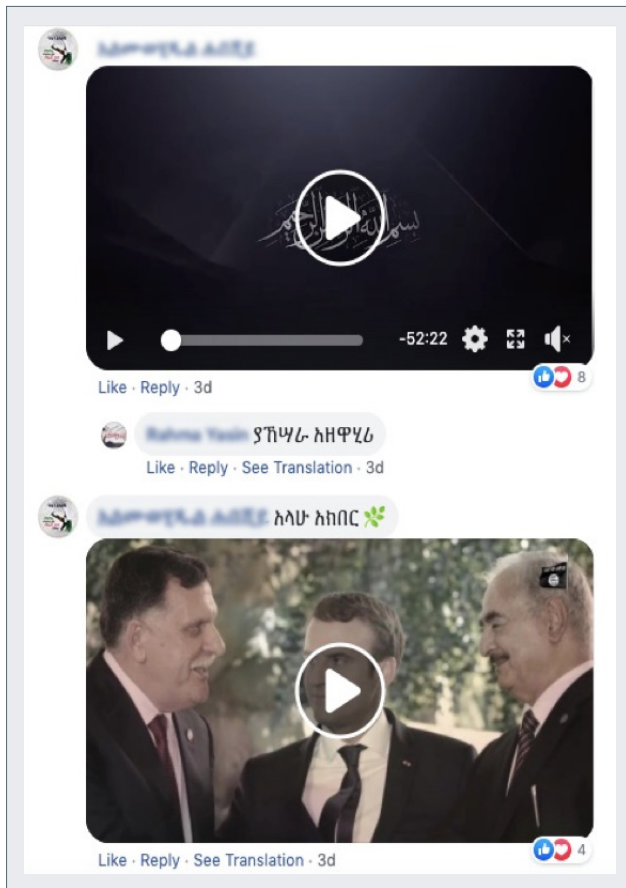


Figure 16: An Ethiopian account by the name of አልሙረካዊ ሐበሺያ shares full-length, branded ISIS video content.

supporting accounts on the platform and seemed to be a workaround to having the video stricken as a public post. Hiding content in comments was also a primary method used to share links to Telegram channels, WhatsApp groups, and ISIS stand-alone websites.

The account Musliman Elhamdulilah, an Albanian-language ISIS account linked to other central accounts in the Fuouaris Upload network's influence, shared numerous ISIS al-Nabā newsletter posts as well as ISIS al-Amaq bulletins and photographs. This included Albanian-language content created by groups such as Bejtul Muhaxhirin that venerated the now dead militant group al-Qaeda in Iraq Jordanian ideologue Abu Musab al-Zarqawi, who built the group's calculated, nihilistic strategy and inspired the ideological pillars of ISIS.

While focusing on the central accounts of the Fuouaris Upload network was key for researchers, the friends and followers of the accounts showcased the wider reach of ISIS support across Facebook. Multilingual accounts seemed to be just as prolific, if not more brazen, in sharing official ISIS content across the platform. Linking both the Fuouaris Upload network accounts and these friends and followers were a series of public pages and profiles that functioned as gathering spots for many of these accounts and central tools in the spreading and sharing of ISIS COVID-19 content.



Figure 17: Account name Musliman Elhamdulilah shares official ISIS media outputs in Albanian on Facebook.

The COVID-19 Connection

Mixed between the hijacked and repurposed ISIS accounts of the Fuouaris Upload network are public pages that disseminate ISIS content from personal accounts to larger audiences. The Arabic-language corona page identifies itself as a health and wellness website. The page posts often and engages with comments. It diversifies its content, sharing memes and videos while resharing the posted content of its followers and keeping a distinct page voice. The page boasts some 10,483 followers and is managed by eight administrators based in Egypt, Syria and Yemen. Dotted between posts about COVID-19 infection and death rates — posts that often excite its followers, especially those that focus on the American death toll— are pieces of ISIS content from accounts in the Fuouaris Upload network’s range, as well as full pages from the ISIS weekly newsletter al-Naba.



Figure 18: The Arabic-language coronavirus page shares an ISIS video produced by the group’s Al-Hayat Media Center.



Figure 19: Cover photo of the account Abdulllah, which reads: “dear God, this virus is a creation of Yours so make it a punishment on your enemies and heal the chests of Your supporters.”

In early April, the page’s administrators penned a Facebook post that read: “everyone should be of the belief that this virus is a soldier of God who is supporting His servants on Earth — the monotheists — whose chests are healed by the extensive death toll of infidels.” At the end of the post was a link to the account Moez Messadi, which had shared multiple re-edited pieces of ISIS content in the past month. Then, exactly a month after the page first emerged on 21 March, the corona page shared a video on the development of a precious metal-based currency to sustain ISIS. While the corona page plays a tertiary role in the Fuouaris Upload network that fanned out across Facebook over the past two months, connecting several of the ISIS-supporting accounts, it highlights a gap in the Facebook response to both extremist content and misinformation around the pandemic. Using the spread of the virus as a rallying cry, terrorist groups, such as ISIS, have praised “God’s smallest soldier”, while highlighting and celebrating the death toll of the virus in countries that are part of the Global Coalition against Daesh.

While the corona page serves as a platform for some ISIS content, and the clearest direct link between ISIS support on Facebook and the exploitation of the pandemic, the Fuouaris Upload network has been sharing COVID-19-focused posts since late March. The account Abdulllah is an ISIS-content-sharing account in the Fuouaris Upload ambit. The account is connected to a number of the network’s central nodes and follows several of the pages set up by ISIS supporters on the platform. The Abdulllah account boasts a coronavirus cover photo, stripped from the counter-terrorism organisation SITE, with the organisation’s watermark on the photograph. The cover photo reads: “dear God this virus is a creation of Yours so make it a punishment on your enemies and heal the chests of Your supporters.” The image is of a giant, glowing coronavirus bursting through a brick wall as a fighter reads with his weapon laying against the wall.



Figure 20: Video shared by the account Abdullah, which claims the coronavirus is a punishment “for the infidels”.

The account similarly shared a COVID-19-themed video that was a montage of various ISIS ministries from when they controlled physical territories in Iraq and Syria, like the ministry of vice and virtue, interspersed with mainstream news accounts of the death and infection rates of the global pandemic. The video’s primary message is “coronavirus is punishment for the infidels” and a “creation of their infidel hands”. The video is an amalgamation of the key narratives espoused by the group, awash with soundbites from Russia Today, Al Jazeera and Al Arabiya, that the COVID-19 pandemic is divine punishment for the “Crusader Coalition” that fought the “righteous warriors of the caliphate”.

Across the friends and followers of the Fuouaris Upload network, COVID-19 narratives and

corresponding imagery were repeated – whether as ISIS-inspired profile and cover photos or standalone digital posters and videos. However, based on the recent focus on COVID-19 narratives by terrorist and extremist groups, while currently popular due to the worldwide impact, the narratives are simply extensions of long-standing ISIS tropes such as denigration of Arab leaders, anti-ISIS coalition countries, and mainstream Muslims. The pandemic-induced pain felt by countries such as the US, the UK and others in the West will, of course, excite ISIS-supporter communities. The ISIS-supporter pandemic narratives are hype, meant to highlight established extremist ideology.

The study of these new tactics and ideas, while valuable, is nothing out of the ordinary for the group or its supporters. The global economic crisis of 2008, the 2016 US election, as well as Brexit, all similarly excited terrorists and extremists online. They developed tailored messaging and new content to address these global and regional issues. It would be foolish to think that terrorist and extremist groups would not latch onto a crisis that affects their enemies, whether artificially-made or natural. The more pertinent question around these pandemic narratives is how they draw in new support for the group while drawing others closer to their ideological worldview. Will ISIS, through its use of coronavirus narratives, build a larger supporter base?

To date and based on the research conducted, it is unclear if ISIS’s pandemic talking points do more than excite an already rabid support base. The latest ISIS COVID-19 poster is nothing more than any other ISIS poster, taking into consideration the contextual factors around its production, such as loss of territory and public support. The ability of the group to create relevant content has never been a question. With this in mind, the study of how crises feed into the social media propaganda strategies and tactics of ISIS supporters is lacking — for instance, setting up seemingly mainstream pages that count coronavirus infection and death rates as honeypots for the eventual inception of terrorist or extremist ideologies in non-extremist circles.

Links to Links

Running through the beating heart of the Fuouaris Upload network on Facebook, as well as the network’s friends’ and followers’ circles, are links to Telegram, WhatsApp, ISIS standalone websites, SoundCloud, and other ISIS accounts on the platform. In the driver’s seat of the Fuouaris Upload network was Luqmen Ben Tachafin, a prolific account hijacker on Facebook, and who ISD researchers believe orchestrated a highly coordinated ISIS raid across the platform. During ISD’s monitoring period, Luqmen Ben Tachafin had up to six accounts under the same name, while leaving his name as the calling card in the centre of the bios of the other accounts in the Fuouaris Upload network. Similarly, throughout the length of the monitoring period, Luqmen Ben Tachafin did not just signpost to his other accounts on Facebook, he similarly posted links to his Telegram and his burgeoning group of accounts on SoundCloud.

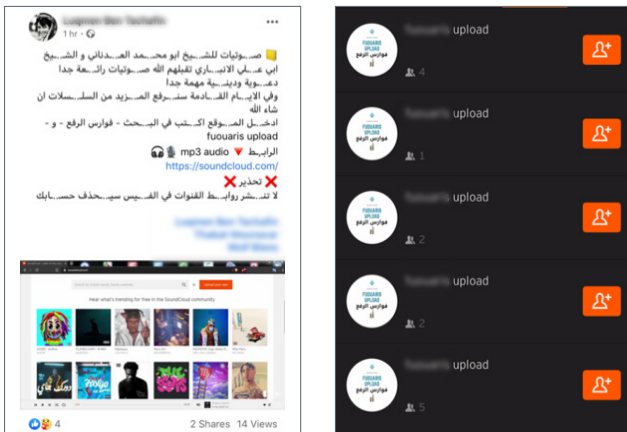


Figure 21: Account Luqmen Ben Tachafin uses Facebook to signpost users to the Fuouaris Upload Soundcloud accounts, of which there were 18.



Figure 22: Account Abu Bakr Abd al-Haq Idris was al-Ma'shibee shares a Telegram channel called "The News of the Sun of the Caliphate."

Between 6 May and 15 May Luqmen Ben Tachafin created 18 accounts on SoundCloud, and shared 91 pieces of ISIS audio content, and then used three Facebook accounts to signpost users to each, instructing friends and followers of his accounts to: "go to the website and write into the search function Fuouaris Upload." While the Luqmen Ben Tachafin accounts illustrated this dynamic rather clearly, other accounts throughout the network were more discreet in the ways they signposted users to Telegram channels and WhatsApp groups. The account Ahmad Muhammad al Ali shared a post on 30 April advertising a Telegram channel for: "whomever wants the latest release, the release is available on my Telegram channel in every format. First comment."

The Telegram channel linked in the first comment as per the post was a veritable ISIS video repository. The account Abu Bakr Abd al-Haq Idris was al Ma'shibee shared a similar post linking to the: "very, very, very important" Telegram account dubbed "The News of the Sun of the Caliphate" while asterisking the words "official" as a means to stress that the content shared in the Telegram channel was direct from an ISIS media outlet and not supporter-made content.

The account Rachid Errich shared a similar post to a different Telegram account and flagged the post as "breaking" like a developing news story. The post used an emoji finger pointing down to the comments and described: "a new channel for news and visuals" that was an ISIS community on Telegram. Researcher found that the channel was in the first comment in the thread under the post.

While Telegram channels were routinely placed into comment threads, researchers also found that friends and followers of the Fuouaris Upload network similarly shared WhatsApp groups, but with less frequency. The account Tamba Tahir Mongolia Tamba — which self-identified as a war spoils account, meaning it was hijacked by ISIS supporters — shared a link to a WhatsApp group dubbed "fatwas over the airwaves" (orders over the airwaves) to its 115 followers. The WhatsApp group was sharing content labelled as "lessons from al-Bayan radio", and voiced by an ISIS shayookh (sheikh). The account Xaashi Adan shared numerous links to an ISIS standalone website — The Punishment — which ISD researchers first tracked via Twitter through a Netflix-imposter account on 24 March.

The faux Netflix account on Twitter was promising "a golden opportunity" to "watch realistic and enthusiastic films while at home" in order to "learn who will rule the world after this corona". The site itself is a digital repository for ISIS videos, neatly organised and user-friendly. Xaashi Adan's next post was to ISIS's online al-Bayan radio website, newly created and dubbed "Al Anfal",¹⁹ a 24/7 live online radio station that was unlike "anything you will find at all". Then on 25 April, the account shared a link to an ISIS blog titled "know the truth, know his family". The first blog post on the site dispelled conspiracy theories such as ISIS being a creation of the West. "The Islamic State is an Islamic creation 100 per cent", the blog post read, and was created "in the year 1400 hijiri [1979]". The account similarly shared an open link to a 7.4-gigabyte digital repository of all the fatwas ever broadcast on the airwaves of al-Bayan radio. The link opened to a



Figures 23 and 24: The account Xaashi Adan shares links to The Punishment, an ISIS website ISD researchers first found via a Twitter account that uses Netflix branding but serves as a repository of ISIS video content.



Figure 25: Account Ömer Can shares a video tutorial on how to hijack Facebook accounts through services that provide American or Canadian phone numbers, like 2ndLine and TextNow.

NextCloud storage drive dubbed “al-Bayan radio lessons” and contained 33 folders of ISIS radio content available for download and sharing by users. ISD researchers have been monitoring the use of NextCloud as a primary archive for ISIS propaganda material since October 2019, when links to drives containing more than one terabyte of ISIS content began appearing on platforms such as Twitter and Facebook.

Many of the accounts ISD researchers tracked and monitored on Facebook over 85 days used two primary modes of sharing links to other ISIS-associated platforms and accounts. The first was a broken text format for posts that would place dots or commas in between Arabic letters, effectively breaking up the words to evade automated detection of key jihadist terminology. ISIS accounts both within the Fuouaris Upload network, as well

as in the friend and follower ambit of the network, did this proficiently. Posts that followed this format often lasted longer on the platform than others that did not use this posting technique. The second tactic was to make posts that contained links to ISIS-specific platforms available publicly on their timeline for a given period – one or two weeks – then effectively closing all posts on the account to the public. This posting format was observed while monitoring accounts that shared links to ISIS storage drives.

Each One, Teach One

The Fuouaris Upload network presents many lessons learnt for researchers and social media platforms today, and similarly, the network also prides itself on sharing its lessons learnt with other users about content moderation tools and moderators. The first of these lessons is the hijacking and hoarding of auxiliary accounts. This lesson, one that researchers came across in a range of different accounts in the network’s sphere of influence, involves the use of mobile applications that provide users with the ability to garner virtual US and Canadian phone numbers. The applications seem to be the primary tool for users hijacking and setting up auxiliary accounts on Facebook and WhatsApp.

The Fuouaris Upload network users created a number of videos during ISD's monitoring period to teach other ISIS supporters' techniques for hijacking and creating multiple accounts on the platform. Using several specific virtual phone applications, users search for accounts with the same US and Canadian phone numbers and then claim that they want to reset their passwords on Facebook. The users then receive a text with the official Facebook code to their newly-acquired virtual number and then proceed to lock out the original account holder from accessing their Facebook profile. Ömer Can — one of numerous ISIS-supporting accounts on Facebook tracked by ISD researchers — shared a 3hr 30-min video tutorial on this process, complete with on-screen text that took users through the process of commandeering a Facebook account. The video shared on 8 May had 333 views, 43 reactions of happiness, and eight shares in less than eight hours of being uploaded.

The Facebook page “the techniques of the digital caliphate”, which had gained 835 followers about a month after its creation on 5 April, functioned as a library for simple video tutorials on hacking and hijacking of accounts. The two videos uploaded by the page were titled “techniques for garnering a phone number for Facebook and Telegram” and “getting an American number for WhatsApp”. Both videos gained 1,823 views in six weeks. While one video illustrated the use of one particular application, the other described the process of using yet another virtual number application, which allows you to purchase multiple American, English and French phone numbers.

The hijacked account of Conner Kathryn similarly shared an account hijacking tutorial video, and in the post the account referenced the best area codes in the US and Canada to use for gaining multiple accounts on WhatsApp and Facebook. “On Facebook these [referring to specific area codes] will unlock 3 accounts on ‘face’ with one number”, the account posted on 17 May.



Figure 26: A hijacked account shares the best area codes to use to gain multiple Facebook profiles.

The second lesson is one around masking ISIS branding on content. Across the Fuouaris Upload network, masked content was prolifically shared using a template format of re-edits to the introductions of official ISIS content. This lesson is the clearest from the monitoring and tracking of the network. While accounts may not have created videos on how to edit or mask content, the friends and followers of the network shared similar practices.

The account Khaled Lhachmi used a beaming sun emoji to cover up the waving ISIS flag in a snippet from a recently-released 50-minute ISIS video out of the “state of” Iraq. The account Daiana Stellinha, with its micronetwork of hijacked ISIS accounts, posted the full-length ISIS Iraq video but masked the content with 30-seconds of the mainstream, state-owned France 24 news channel as an introduction, before launching onscreen text

over the channel's logo that read “God's greetings”. The remaining 49 minutes of the video was the official ISIS Iraq video, with no other video augmentation, except for the France 24 logo in the upper right-hand corner. The video was shared 282 times and viewed 1,400 times by 17 May. The account even went as far to hashtag the video with anti-ISIS and France 24 hashtags in English, and then in Arabic hashtags that read “repeat upload”, “neeeeeeeew” and “broadcast”.

Accounts like Mohamad Yusef Wanees did not simply mask ISIS content branding with sun, flower, or explosion symbols, but created alternative branding based on calling card avatars utilised to hijack accounts on the platform. The Wanees accounts were always demarcated by an avatar of a small, curly-haired girl staring out. When the Wanees accounts shared pieces of ISIS content they would mask ISIS branding in the top right-hand corner of videos with the calling card little girl avatars they used on Facebook.



Figure 27 and 28: Masked content – account Khaled Lhachmi shares ISIS video content with the ISIS branding masked by a sun. Account Daiana Stellinha shares official ISIS content masked by an introduction from France 24.



Figures 29, 30 and 31: Creating alternative branding – Wanees accounts brand their content with an avatar of a curly-haired girl while account Omar Ibrahim masks ISIS branding with a red dot that spells his name.

The account Omar Ibrahim utilised a similar calling card symbol for the masking of ISIS assassination content. Uploaded videos by the Ibrahim accounts always featured a red dot over the ISIS branding in a video and the name Omar within the circle. This technique is one that was used repeatedly both within the Fuouaris Upload network and by its friends and followers. While it was not an advertised strategy such as the use of virtual phone number applications to hijack accounts, it was an unsaid rule, and one that ultimately allowed ISIS content to thrive longer on the platform than non-masked content.

Pillage and Plunder: Recurring Raids

Raids are key to consolidating respect, power and status for ISIS supporters on Facebook. The higher value the target the more attention, follows, and support decentralised micronetworks of terrorist support receive on the platform. On 30 June, the account Ali Arbash, a hijacked Facebook account with its own set of auxiliary accounts across the platform, posted a series of directives for a "terrorist media raid" with a target of the US Air Force Academy Facebook page, and an objective to "terrorise the Crusaders". The account then used a downward finger emoji to indicate that other ISIS-accounts on the platform could find the links to the page in the comments section.

Users from across the platform began to comment underneath the post. Their comments, primarily consisted of links to other ISIS accounts on the platform, signposting them to the news of the raid so that they too could take part. Soon, amid the 138 comments under the post, other users began posting content made especially to harass users following the US Air Force Academy. This includes images of beheadings of the US President



Figure 32: Account name 'Ali Arbash' posts a series of directives for a 'terrorist media raid'

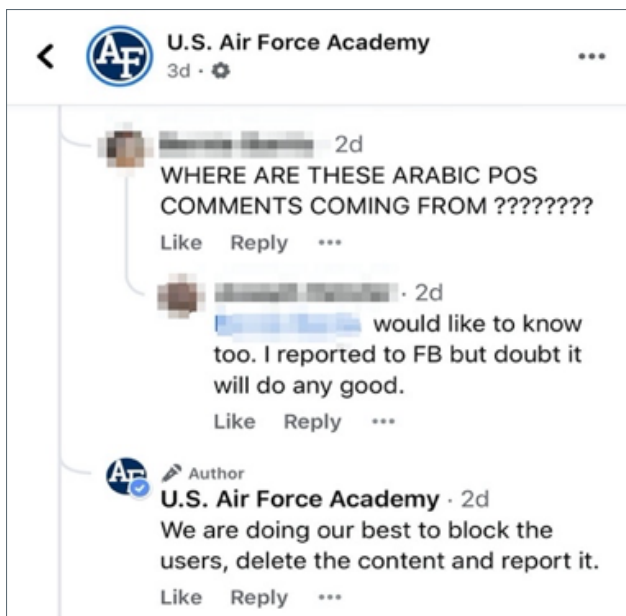


Figure 33: The US Air Force Academy reassures its followers that its responding to the Arabic commentary left under its post.

Donald J Trump with the words "coming soon". Other content shared included photographs of a smouldering World Trade Centre, while a second plane heads into one of the towers, with the words "we will do it again, wait for the date".

Accounts began rapid-fire commenting under a celebratory post for the incoming cadet class of 2024 basic training, with the images shared on Ali Arbash's post as replies to other users. The raid went on for hours. The users hounded followers of the US Air Force Academy page, and soon the administrators had posted a message to its followers, reassuring them they were doing their best to block the users, delete the content and report it. Users openly doubted if Facebook would be able to stem the ISIS account plundering of the comments space on the page.

Two days after the raid, the primary accounts that launched it, such as Ali Arbash, continued to post ISIS content on their hijacked accounts, and even openly mocked the US Air Force in public posts after it stated it was "being spammed" and that it was "blocking these users and reporting them to the OSI (the US Air Force Office of Special Investigations) for investigation". While the US Air Force seemed to be taking the actions of these ISIS networks seriously, the ISIS accounts took the threat of investigation as a sign of impact. It was a badge of honour in the Facebook propaganda war.

On 28 June, two days before the raid on the US Air Force Academy, a user dubbed Suzan Sozdar, which also seemed to be controlling multiple ISIS-supporting accounts on Facebook, penned a similar raid directive post. This time the target was the Pentagon. The post included details about the Facebook page for the US Department of Defence, including the number of followers. The objective was similarly to terrorise the Crusaders. Underneath two posts, in praise of Korean War veterans, ISIS users once again flooded the comment sections with photographs of beheadings, imagery of the September 11 attacks, and open threats. ISIS accounts used the primary directive post to share ready-made attack content in the comment threads.

The two raids, which ISD researchers witnessed in real-time, were not just the work of disparate

accounts across the platform, but a coordinated tactic by an ISIS-supporter outlet called "Roma" or "Rome". A nod to centralised ISIS narratives about conquering Rome as a symbol of Western civilisation. Roma was branded with symbol and had created pages on the platform twice. Before it was taken down it had successfully become an organising point for raids across the platform. Roma was producing its own branded videos, including a 15-minute video dissecting raids on high-profile pages, like the US President Donald J.



Figure 34: Ali Arbash mocks the US Air Force Academy's response.



Figure 35: The Romya (Roma) account, with its branding.

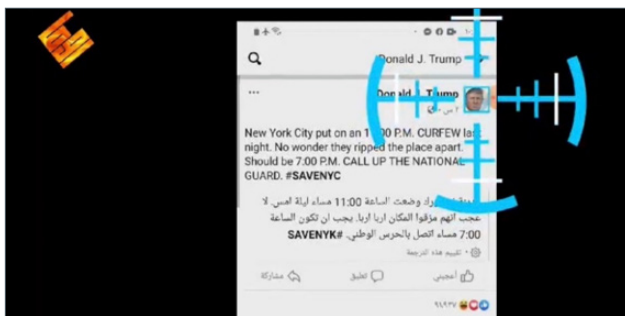


Figure 36: A raid on the US President Donald J. Trump's Facebook page.



Figure 37: Additional Romya (Roma) page content about the raids.

ISD researchers also monitored other ISIS micronetwork accounts on Lebanese pages on Facebook that were calling for raids. Lebanon, a country in the throes of economic and political collapse, has been grappling with a triple-headed crisis that includes a dramatic political fallout, a pandemic, and state corruption. In October 2019, popular frustration materialised into sustained nationwide protests that led to the resignation of the prime minister and government. The focus and objectives for the Lebanese raids — one regarding a news story about the insulting of the Prophet's wife in Tripoli, and the other about the murder of a woman caught in the crossfire in the Palestinian refugee camp Shatila — were meant to "incite Sunni youth to kill rafidah" (Shia or Shiite Muslims). Users peppered the comments with photographs of guns imploring the Sunnis of Lebanon to kill Shia Muslims.

These four raids were just a sample of the coordination between disparate sets of ISIS users, that were controlling accounts, self-branding content, and revealing Facebook's gaps in moderation. Not only do the posts calling for the raids on the US Air Force Academy and the Department of Defence still exist on the platform,

the users that launched them openly mock the notion of an investigation into the launching of the raids. Imbued with a sense of invincibility, and an army of auxiliary accounts, these ISIS decentralised networks are aware that Facebook is unable to keep pace with their activity. While steps were taken to shut down two Roma pages on the platform during the period researchers were monitoring ISIS activity, the organisers of

raids simply transitioned to using their individual profiles, ones of many they control, to continue launching raids and building follower bases.

The Takedowns

The Fuouaris Upload network and its friends and followers across Facebook are not immune to takedowns. Over the monitoring period, between 7 April-3 July, the Fuouaris Upload network lost 62 accounts under its control. However, the ability of the network to adapt plays a role in the survival of its 28 auxiliary accounts that continue to challenge the platform with their ability to spring back to life, and seed ISIS content across Facebook.



Figure 38: The first reference to Luqmen Ben Tachafin found by ISD researchers.

This propaganda pipeline is one that likely began as a series of tests in August 2019, when ISD researchers found the first reference to Luqmen Ben Tachafin on Facebook. The reference was a post by another Facebook user detailing how her sister's account had been hacked. The user shared a public screenshot of the Luqmen Ben Tachafin primary account that ISD researchers found in April 2020.

The network sprang to life during a period when we've faced a global pandemic and lockdown. This has meant we have turned online to communicate even more, meanwhile Luqmen Ben Tahacfin and the Fuouaris Upload network expanded day by day, amassing digital territory, while weathering takedowns, and surviving almost 70 per cent of its war spoils on Facebook being lost. As of 30 June, the Fuouaris Upload network is still in control of 26 accounts, some of which are still actively sharing content from late March.

The relative ease that these accounts can withstand automated and manual moderation efforts on Facebook is worrying. The accounts and nodes within the Fuouaris Upload network have patterns and modes of sharing content that is standardised. These patterns are calling out for further investigative work into terrorist clusters. They are similarly learning both from takedowns and teaching other ISIS supporters' evasive modes of seeding content in the process. This interactive and evolving strategy to exploit moderation gaps on Facebook, Twitter and SoundCloud, is as much multiplatform as it is multilingual. While a majority of the accounts were seeding content in Arabic,



Figure 39: Lobo Noir appears as the new primary account for Luqmen Ben Tachafin after the original accounts were taken down.

the monitoring and tracking period revealed parallel networks were operating in Albanian, Turkish, Somali, Ethiopian, and Indonesian languages.

The Fuouaris Upload network and the friends and followers under its influence is a case study into the mechanics of ISIS support communities on Facebook. It is also a guide into how these networks have expanded and solidified their footholds into the fabric of social media platforms. The network highlights emerging linkages not just in the ISIS content shared, but in the connections between Facebook, Twitter, and SoundCloud ISIS communities. The network, in the words of its account holders, are “expanding” and “remaining”. They are hoarding sleeper accounts and prepared for more takedowns. Their emergence during a time when there is increased focus on misinformation and disinformation around the COVID-19 pandemic, highlights that ISIS supporters online are just as actively exploiting gaps online in security responses, as they are offline.

The primary tactics and behaviours outlined in this report are meant to serve as a means to seriously rethink the practice of both automated and manual moderation across Facebook and other platforms. Facebook has taken steps to address gaps and is attempting to rectify issues with transparency and collaboration with experts and community groups in dealing with terrorist content on the platform. However, the ability of decentralised networks of ISIS accounts — such as the Fuouaris Upload network — to survive, and thrive, highlights a pressing need to plug these gaps in moderation with agile and adept investigations into where manual and automated detection has failed. Creating hybrid approaches that build on independent expert analysis is needed, rather than relying on the ability of AI to solve the issue of terrorist content and accounts. These networks are expanding, and evading both manual and technology-assisted moderation.



Figure 40: a series of Fuouaris Upload network accounts.

Footnotes

- 01 Shiraz, Maher. 2016. Salafi-Jihadism: The History of an Idea. London: Hurst & Company. Maher states that “there are five essential and irreducible features of the Salafi-Jihadi movement: tawhid [the unity of God], hakimiyya [sovereignty], al-wala’ wa-l-bara’ [loyalty and disavowal], jihad and takfir [excommunication, declaring someone an unbeliever]” Accessed at: <https://muse.jhu.edu/article/647594/summary>
- 02 Quote from Luqmen Ben Tachafin account, accessed before take down, on April 16..
- 03 The Watch Party function on Facebook allows users to watch content with friends and followers in real-time.
- 04 Kuffar in Arabic means “nonbelievers.” These were quotes from numerous accounts tracked, that celebrated the death toll in “nonbeliever” countries.
- 05 Europol, Europol and Telegram take on terrorist propaganda online (25 November 2019), <https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online>.
- 06 Facebook, Oversight Board (2020), <https://www.oversightboard.com/>
- 07 MIT Technology Review, Facebook and Google may be fighting terrorist videos with algorithms (27 June 2016), <https://www.technologyreview.com/2016/06/27/159096/facebook-and-google-may-be-fighting-terrorist-videos-with-algorithms/>.
- 08 JM Berger and J 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 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.
- 09 The account names do not represent actual, living people, and are attempts by ISIS supporters to create realistic personalities for these account profiles on Facebook.
- 10 All of Luqmen Ben Tachafin primary accounts had the same bio description, as noted in the text.
- 11 ISD, ‘The Baghdadi Net’: How a Network of ISIL-Supporting Accounts Spread Across Twitter (November 2019), <https://www.isdglobal.org/isd-publications/the-baghdadi-net-how-a-network-of-isil-supporting-accounts-spread-across-twitter-by-moustafa-ayad/>.
- 12 The names of the users noted in the text have been abbreviated to protect their identities.
- 13 The avatar is a modified “Solid Snake,” a character from the Metal Gear Solid video game.
- 14 Quotate is from the Nassim Oussama account, accessed on May 1.
- 15 Mujahid Shaykh is an honorific for shaykhs who joined ISIS ranks on the frontlines.
- 16 Quote is from the 2hr 30min-long video shared by Youcef Ibrahim account, which was a part of the Fuouaris Upload network.
- 17 The New Arab, Air raid silences IS radio station in Iraq’s Mosul, <https://english.alaraby.co.uk/english/news/2017/2/28/air-raid-silences-is-radio-station-in-iraqs-mosul>.
- 18 A Hilary. Peter Sarat-St., “Make a Bomb in the Kitchen of Your Mom”: Jihadist Tactical Technical Communication and the Everyday Practice of Cooking (2017) 26 (1), Technical Communication Quarterly <https://www.tandfonline.com/doi/full/10.1080/10572252.2016.1275862>.
- 19 “Al Anfal” is an Arabic word for used for “bounties.” It can also be used as a means to described knowledge “bounties.”

About ISD

We are a global team of data analysts, researchers, innovators, policy-experts, practitioners and activists - powering solutions to extremism, hate and polarisation.

The Institute for Strategic Dialogue (ISD) is an independent nonprofit organisation dedicated to safeguarding human rights and reversing the rising global tide of hate, extremism and polarisation. We combine sector-leading expertise in global extremist movements with advanced digital analysis of disinformation and weaponised hate to deliver innovative, tailor-made policy and operational responses to these threats.

Over the past decade, we have watched hate groups and extremist movements deploy increasingly sophisticated international propaganda, influence and recruitment operations, skillfully leveraging digital technology, and often boosted by hostile state actors. Alongside an exponential spike in violence (conflict, hate crime, terrorism), societies around the world are being polarised. At ballot boxes, populists have made significant gains and authoritarian nationalism is on the rise.

If left unchecked, these trends will existentially threaten open, free and cohesive civic culture, undermine democratic institutions and put our communities at risk. Progress on the major global challenges of our time – climate change, migration, equality, public health – threatens to be derailed.

We can and must turn the tide. Help us build the infrastructure to safeguard democracy and human rights in the digital age.

ISD draws on fifteen years of anthropological research, leading expertise in global extremist movements, state-of-the-art digital analysis and a track record of trust and delivery in over 30 countries around the world to:

- Support central and local governments in designing and delivering evidence-based policies and programmes in response to hate, extremism, terrorism, polarisation and disinformation
- Empower youth, practitioners and community influencers through innovative education, technology and communications programmes.
- Advise governments and tech companies on policies and strategies to mitigate the online harms we face today and achieve a 'Good Web' that reflects our liberal democratic values

Only in collaboration with all of these groups can we hope to outcompete the extremist mobilization of our time and build safe, free and resilient societies for generations to come. All of ISD's programmes are delivered with the support of donations and grants.



PO Box 75769 | London | SW1P 9ER | UK

www.isdglobal.org