1-1-2018

Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution

Teodor E. Mitew
University of Wollongong, tmitew@uow.edu.au

Ahmad Shehabat
University of Wollongong, ams591@uowmail.edu.au

Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution

Abstract

The study examines three anonymous sharing portals employed strategically by the Islamic State of Iraq and Sham (ISIS) to achieve its political ends. This study argues that anonymous sharing portals such as Sendvid.com, Justpast.it, and Dump.to have been instrumental in allowing individual jihadists to generate content, disseminate propaganda and communicate freely while routing around filtering practiced by popular social media networks. The study draws on Actor Network Theory (ANT) in examining the relationship between ISIS jihadists and the emergence of anonymous sharing portals. The study suggests that, even though used prior to the massive degrading operation across social media, anonymous sharing portals were instrumental in allowing ISIS to maintain its networking structure in the face of coordinated disruption.

Keywords

flag:, black, black-boxing, platforms, distribution, sharing, content, anonymous, isis

Disciplines

Arts and Humanities | Law

Publication Details

Mitew, T. E. & Shehabat, A. "Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution." Perspectives on Terrorism 12 .1 (2018): 81-99.

Black-boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics

by Ahmad Shehabat & Teodor Mitew

Abstract

The study examines three anonymous sharing portals employed strategically by the Islamic State of Iraq and Sham (ISIS) to achieve its political ends. This study argues that anonymous sharing portals such as Sendvid.com, Justpast.it, and Dump.to have been instrumental in allowing individual jihadists to generate content, disseminate propaganda and communicate freely while routing around filtering practiced by popular social media networks. The study draws on Actor Network Theory (ANT) in examining the relationship between ISIS jihadists and the emergence of anonymous sharing portals. The study suggests that, even though used prior to the massive degrading operation across social media, anonymous sharing portals were instrumental in allowing ISIS to maintain its networking structure in the face of coordinated disruption.

Keywords: Anonymous sharing portals, Actor Network Theory, black boxing, Islamic State, degrading operation, Sendvid, Justpaste, Dump.to.

Introduction

The rise of distributed communication networks has offered new possibilities for the emergence and expansion of terror networks. Since its emergence in 2013, the so called Islamic State of Iraq and Sham (ISIS)[1] managed to utilise sophisticated digital media communication technologies to disseminate globally its propaganda content and foster communication between its members. In particular, images and video footage aimed to generate fear have been successfully broadcasted globally by the ISIS propaganda network. Noticing a correlation between the growing spread of ISIS propaganda videos on social media platforms, anonymous sharing portals, and the rise of terrorist activity in the Middle East and Europe, in 2015 the US government established countermeasures aimed to degrade and hinder the spread of ISIS propaganda online. These efforts included deletion of ISIS online content, suspension of social media accounts, as well as hacker attacks against the websites used by ISIS affiliates, and were largely successful in suppressing ISIS propaganda across popular social media platforms.[1]

In a clear effort to adapt to these countermeasures and sustain its information flows ISIS moved the core of its propaganda network to other online platforms substituting for popular sites such as Twitter and YouTube. These were primarily encrypted communication channels such as Telegram, Signal, and WhatsApp, as well as anonymous sharing portals such as Justpaste.it, Sendvid.com and Dump.to. We refer to them as 'anonymous' because they protected the anonymity of their users and were at the time little known to a wider internet audience. It is important to emphasise that ISIS used these channels even before the network degrading countermeasures it faced, however at the time they arguably played an auxiliary role in the overall communication strategy of

1 Also known as IS, ISIL, and Daesh.

the organisation.

The aim of this article is to propose an examination of ISIS's use of these portals as a response to the countermeasures against its online propaganda operations. We suggest that anonymous sharing portals such as Sendvid.com, Justpaste.it, and Dump.to have been instrumental in allowing jihadi groups to generate content, disseminate propaganda, and communicate freely by diminishing the effects of the broad jihadi propaganda filtering efforts of popular social media networks. Crucially, while the majority of research attention has been concentrated on analysing the role of encrypted communication channels such as Telegram, little attention has been paid to anonymous sharing portals acting as black boxes for ISIS-related propaganda. Accordingly, we argue that in order to conceptualise the dynamic role played by anonymous sharing portals in the ISIS network we can use the conceptual toolkit developed by Actor Network Theory (ANT).

The key value that ANT brings to our analysis is an understanding of networks as dynamic phenomena that have to be continuously rebuilt and maintained by the actors performing them. Furthermore, ANT posits that both humans and nonhumans are network actors equally entangled in the flow of agency, and focuses on the dynamic relations between the entities performing the network. This is of fundamental analytical importance as it allows us to understand the agencies and "normative principles […] that build, maintain, and transform networks".[2] Ever since ANT's particular methodological approach to studying networks was proposed by Bruno Latour, its aim has been "to follow the actors […] and describe how they make associations connections, relations, and assemblies".[3] The ANT perspective allows researchers to develop digital methods of high sensitivity for an online problematic, leading to the development of "'natively digital' research tools that 'take advantage of the analytic and empirical capacities that are 'embedded in online media".[4] In the context of this paper, the use of ANT therefore signifies an awareness of the complexity of ISIS's network assemblage, as well as a perspective allowing us to conceptualise the role played by anonymous sharing platforms in ISIS's propaganda networks.

Due to their unique characteristics, anonymous sharing platforms play an important role in ISIS's online strategy, demanding a specific framework of analysis. The ease of sharing content and the anonymity of the users create a dynamic where platforms act as automated message amplifiers, playing the role of black-boxes in the wider information network. Virtually all users on these platforms fall in one of three often overlapping roles: they either dynamically produce and aggregate content, act as intermediaries retranslating and curating content across multiple platforms, or passively consume the information flowing across the network. In other words, the content flowing through these platforms is highly dynamic and visual, lending itself to visual data gathering and ethnographic observation. As Christopher Moore has argued, screenshots are a useful research method in that context because "as digital tools, they diminish permanence in exchange for malleability and performativity. As media objects, they can be dynamically traced across the networks of their dissemination and require a re-evaluation of the axioms of cultural production that considers texts independently of experience".[5]

We first examine the broad online effects of the countermeasures aimed at the ISIS propaganda network. Using the notion of a black box drawn from ANT, we then examine the relationship between ISIS jihadists and the emergence of anonymous sharing platforms. Finally, we look at three anonymous sharing portals in an effort

to understand how they could have contributed to ISIS's information operations.

The Rise of ISIS on Social Media

Since its appearance in 2013, ISIS quickly gained notoriety as a terror network, arguably due to the savagery it demonstrated against its enemies and people under its control. Concurrently, ISIS appeared to quickly recognize the importance of digital communication tools in its self-proclaimed goal to establish a global Caliphate. Images of savagery were broadcasted virally through social media networks and global media, and were clearly intended to frighten enemies and lead to further gains on the ground in both Syria and Iraq. Twitter, YouTube and Justpaste were extensively utilized by ISIS to conduct its information operations, for the purpose of producing and disseminating propaganda videos for potential recruits and spread its radical views among Muslim youth globally.

The role of social media platforms in aiding terror organizations has been examined extensively by scholars, journalists and think tanks. For example, the former Google CEO Eric Schmitt pointed out that ISIS and its supporters are "producing as many as 90,000 tweets and other social media responses every day".[6] The importance of utilizing media by terror networks was highlighted by Philip Sieb and Dana Janbek, who argued that media are the oxygen of terrorism.[7] Furthermore, Abdel Bari Atwan argues that the internet helped ISIS to achieve its recruiting objectives and territorial ambitions in short time.[8] That is, digital communication tools "allow terrorist groups to become regional or even global players […] [they] also allow terrorists to work more effectively […] to protect communications".[9]

However, the social media activities of ISIS were monitored closely by the U.S and proprietors of social media platforms,[10] and were met by a series of countermeasures intended to degrade ISIS's online presence.[11] In our opinion, the efforts to deploy countermeasures against ISIS's online offensive by the US and anti-ISIS powers have demonstrated three distinct phases of development.

Phase one: *Degrade and Destroy*. The US government requested Twitter and Google to delete ISIS's active accounts on their platforms.[12] This measure resulted in deleting thousands of accounts and messages, in effect leading to a global cyberwarfare campaign against ISIS affiliates.

Phase two: *Countering ISIS propaganda.* To compete with ISIS propaganda online, the US government directed the efforts of the Centre of Strategic Counterterrorism Communications (CSCC),[13] which debuted with a video production titled "Welcome to ISIS Land". According to Scott Higham, "the video became a viral phenomenon — viewed more than 844,000 times on YouTube — and a cause of significant irritation to its target".[14] In addition, the CSCC launched the "Turn Away Think Again"[2] page on Twitter to stop foreign fighters joining ISIS and documenting atrocities committed by ISIS jihadists. In return, ISIS launched the "Run Do Not Walk to U.S. Terrorist State" page on Twitter to recruit potential members from the West.

Phase three: *Hacking and Information warfare.* Part of the less overt efforts at suppressing jihadist propaganda online, the hacktivist group *Anonymous* declared 'Operation ISIS'. Andrew Griffin suggests that this operation

2 Now called DOS team, operating in both Arabic and English it produces videos showing the brutality of ISIS and raising awareness among Arab and Muslim youth.

concentrated its efforts on searching and neutralising ISIS online content on both social media platforms and websites using Distributed Denial of Service (DDOS) attacks.[15] Known as #Op-ice-ISIS, this operation succeeded in paralysing hundreds of ISIS-related channels of information dissemination, such as the 'The Dawn of Glad Tidings' app (#op_Isis, 2015). This app, according to Jim Berger (2015) was the official mobile phone application disseminating the latest news about ISIS operations.[16]

The online war against ISIS has reached a point where the US coalition forces, Anonymous hackers and other anti-ISIS actors have managed to seriously degrade ISIS information dissemination capabilities across popular social media networks. The consequences of countering ISIS propaganda on popular social media platforms enforced ISIS to shift the emphasis of its information operation to anonymous digital portals and encrypted communication channels such as Justpaste.it, Sendvid.com, Dump.to, Share.it, Woodvid.com, Archive.org, as well as Telegram, WordPress, Pinterest and Tumblr.

Many scholars have observed the relation between the emergence of anonymous sharing portals and the wide spread of terror narratives. For instance, Alvares and Dahlgern have highlighted the role played by web 2.0 platforms in the pervasiveness of terror narratives by creating space for uncensored violent content.[17] File-sharing portals, videos, and personal spaces are used to target different audiences, namely, supporters, public opinion and enemies. This observation is also corroborated by Klausen, when he argues that the "jihadist insurgents in Syria and Iraq use all manner of social media apps and file-sharing platforms, most prominently Ask.fm, Facebook, Instagram, WhatsApp, Pal Talk, kik, viper, JustPaste.it, and Tumblr".[18]

That being said, it is important to note that anonymous sharing portals such as Telegram, Justpaste.it, Sendvid.com, and Dump.to were already used by ISIS as auxiliary communication channels prior to the degrading operation. However, as we aim to demonstrate, coordinated filtering across popular social media forced ISIS to switch its primary information operations to these platforms and to leverage them as communication black-boxes, thus circumventing the primary vector of the campaign against its operations.

Telegram in particular, largely due to its native support of encrypted one-to-one and one-to-many communications, has been widely adopted by ISIS and its affiliates globally following the start of the filtering campaign against it in the fall of 2014. The significance of ISIS' use of the platform lies in the ability to establish multi-purpose channels strengthening its propaganda machine. Crucially, this allows for ISIS affiliates, only latently connected to the central hubs of the organization, to both receive and share a coherent centralized propaganda message as well as establish encrypted communication channels with each other. Such anonymous channels therefore act as systems of coordination, message reinforcement, and activity planning.

A separate analysis by the authors of this paper, published elsewhere, suggests that ISIS-related Telegram channels play a critical role in personal communication between potential recruits and the dissemination of propaganda encouraging 'lone wolf' attacks.[19] This study, however, focuses on the less known anonymous sharing platforms Justpaste.it, Sendvid.com, and Dump.to, used by ISIS in furthering its information operations and communication objectives.

Degrading ISIS Online Activities

Popular social media platforms such as Twitter, Facebook and YouTube are using their terms of service (TOS) to exercise control over the type of information produced and disseminated through their networks. For example, YouTube's TOS state in relation to hateful, violent and graphic content that, "it's not okay to post violent or gory content that's primarily intended to be shocking, sensational or disrespectful. If a video is particularly graphic or disturbing, it should be balanced with additional context and information".[3] Jacob Silverman observed that YouTube acts robustly when dealing with terror content. It only takes couple of clicks to delete content and suspend associated accounts.[20] Under YouTube's TOS, the platform reserves the right to remove content and in some instances, suspend accounts. According to a YouTube spokesperson, "YouTube has clear policies prohibiting content intended to incite violence, and we remove videos violating these policies when flagged by our users. We also terminate any account registered by a member of a designated Foreign Terrorist Organization and used in an official capacity to further its interests".

Berger and Strathearn indicated that when it comes to freedom of speech, social media platforms are biased. They suggest that these platforms should make it clear that freedom of speech is limited when it comes to using their service.[21] In a similar vein, Twitter governs what is posted against its TOS policies. With rising international pressure on these social network platforms, particularly from the US government over ISIS's online materials, Twitter, Facebook and YouTube have acted swiftly and imposed harsh policies targeting gruesome content generated by ISIS. Twitter, for instance, waged a 'Twitter war' against pro-ISIS accounts and managed to suspend many thousands of accounts which resulted in significant degradation of ISIS' Twitter presence.

In their report, *The ISIS Twitter Census*, Jim Berger and Johnathan Morgan collected Twitter data in an attempt to map ISIS's activities on that platform.[22] The study was based on a sample of 20,000 ISIS supporter accounts, and it established, among others, that in October through November 2014 "at least 46,000 Twitter accounts were used by ISIS supporters".[23] The study also revealed that 20,000 confirmed ISIS supporters are residing in the territories controlled by the Islamic State. Saudi Arabia was the second-most common location for ISIS supporters. In addition, one fifth of ISIS supporters used English and almost three quarters selected Arabic as their primary language. It also appeared that the broad countermeasures aimed at degrading ISIS propaganda was successful, at least in part because of wide Twitter account suspensions. The authors concluded that the mass account suspension strategy – known as "whack-a-mole"— is highly successful as a network degrading tool, and that ISIS finds it challenging to keep up with replacing suspended accounts without suffering any negative consequences.

3 YouTube TOS page: https://www.youtube.com/static?gl=AU&template=terms

Figure 1: A tweet posted by J.M. Berger on 20 September 2014.

In other words, the latter study offers conclusive evidence that when account suspensions are carried out on a consistent basis across a range of platforms they have an adverse effect on the targeted network. While Twitter has been largely successful in suppressing ISIS propaganda, Silverman suggests that hosting extreme content poses long-term challenges for all social media platforms,[24] and that YouTube and Facebook in particular must keep updating their tools in order to dynamically trace and report graphic materials disseminated by potential terrorists. In this respect, proactive monitoring of platforms and targeted account removals have noticeably harmed ISIS' content distribution and propaganda tactics on social media.

Interestingly, and in an apparent effort to resist such persistent network degrading operations, ISIS has tried to recruit personnel tasked with mitigating the effects of network attacks and sustaining their information operation. As Atwan observed in 2015, "most of Islamic state commanders and recruits are tech-savvy; coding (writing software programs putting information in html) is as familiar to them as their mother tongue. Most of the digital caliphate business is conducted online, from recruitment to propaganda to battlefield strategy and instructions".[25] ISIS members and sympathizers have specifically targeted unpoliced, anonymous, and safe sharing platforms allowing the anonymous dissemination of uncensored content. Often, such platforms are also relatively obscure and unknown to the wider public, a factor contributing to their anonymity.

Ironically, and in a development reminiscent of the network-centric warfare theories of John Boyd, the overall success of the strategy of degrading any overt social media presence by ISIS appears to have led to the rapid changing of media dissemination tactics by ISIS, and the fast adoption of anonymous alternatives. Specifically, it appears that the ISIS switch to anonymous and obscure alternatives to popular social media platforms was made possible through the adoption of storage and sharing portals such as justpaste.it, dump.to, sendvid.com, archive.org, dailymotion.com and liveleak.com. As John Boyd (1976) famously argued, "generating a rapidly changing environment—that is, engaging in activity that is so quick it is disorienting and appears uncertain or ambiguous to the enemy—inhibits the adversary's ability to adapt and causes confusion and disorder that, in turn, causes an adversary to overreact or underreact... [T]he message is that whoever can handle the quickest rate of change is the one who survives".[26] Boyd famously suggested that to win in an environment of high information density one has to manoeuvre at speed and therefore operate inside the Observe, Orient, Decide and Act (OODA) loop of your adversary. The weaponization of anonymous sharing platforms has arguably enabled ISIS to mass-disseminate propaganda while avoiding suppressive actions, an information equivalent of manoeuvre at speed, and therefore operate inside the OODA loop of its adversaries. Furthermore, as the authors have argued elsewhere, ISIS has successfully trialled using stigmergic swarming operations harnessing

multiple anonymous platforms to maintain its network structure.[27]

Below, we focus on three case studies of anonymous online portals in order to illustrate their use by ISIS in establishing new channels of content dissemination and communication, as well as examine how these portals allowed ISIS to maintain an operational network structure.

Anonymous Platforms as Black Boxes

As discussed above, we believe that in order to understand how ISIS has managed to route around extensive account suspension operations waged against it on popular social media platforms it is necessary to examine the role played by anonymous sharing platforms with a conceptual toolkit informed by ANT.[28] From an ANT perspective, networks are populated by entities conceptualised as *actants* because they simultaneously *act* and are *acted upon*. Actants, whether human or nonhuman, always have agency, which here stands for the ability to force change, a *detour*, in the interactions between networks.[29] Agency, and action in turn, are always already the property of associations of human and nonhuman elements.[30] Accordingly, one of the main strengths of ANT is that it allows the tracing of actors in a network, based on their actual role in the flow of agency.[31]

When examining the role played by an anonymous sharing platform within the wider ISIS network an ANT-informed perspective makes no a priori difference between social or technical nodes in the network. All that it sees are entities actively performing a network. However, anonymous sharing platforms immediately stand out because they act as accelerators of information flows while making it harder to trace the logistics of how these flows are performed. In effect, they black-box certain elements of the network. In this context, the black box is a conceptual metaphor developed in ANT to describe network assemblages which function so well that their internal logistics are *opaque from the outside.*[32] Black boxes are created through what ANT terms as 'acts of translation', in which actors are first enrolled in the network, and then work to stabilise it from the inside thus creating the appearance of a monolithic assemblage.[33] From the perspective of our case studies, the black box concept helps to understand how ISIS maintains its networking structure by adaptively shifting operations to less known online sharing portals.

Opening a black box allows us to examine the ways in which "a variety of social aspects and technical elements are associated and come together as a durable whole".[34] The notion of opening and examining a black box is possible, because when focusing on a black-boxed entity seemingly homogenous from the outside, ANT sees "processes, performances, socio-technical rituals, and enactments […] driven by the dynamics of making connections, of binding things together, of extending associations, of 'translating' and 'enrolling' actors into networks".[35] The same could be said for the role of online sharing portals, mobile phone apps, and other technical assemblages enrolled in the networks of ISIS affiliates.

When analysing the case studies below, it appears that ISIS is leveraging the stability and distributed nature of their relatively established communication networks to enlist new actants which in turn help in the emergence of new networks. Crucially, the relative opacity of less known cloud portals such as Justpaste.it and Sendvid.com, coupled with the migration of already established distributed networks of ISIS affiliates, drawn to these platforms by their TOS, creates a black-boxing dynamic. Ironically, the operations degrading ISIS's overt digital

capabilities on popular social media sites have resulted in the migration and development of this dynamic. That is, ISIS networks seem to have reacted to the degradation of their capabilities on popular social media networks and rapidly migrated to new anonymous portals. As Stern and Modi have pointed out, "terrorists respond to changes in their environments by changing their mission and changing their shape. What is important in such events is that information logistics is essential in disseminating messages of terror".[36]

ISIS's Black Boxes

1. *Justpaste.it*

Justpaste.it is a free content sharing portal providing document storage and file sharing services under the motto of 'sharing text and images the easy way'. The site is hosted by Cloud Flare and owned by Polish entrepreneur Mariusz Zurawek, who sums up justpaste.it as follows: "You are able to do what you want with almost two clicks. It doesn't require registration, it isn't searchable and access to specific content is only available via a link or if it makes the 'most popular' page".[37] However**,** early 2014 ISIS has harnessed this service to disseminate its online videos, brutal images of beheadings, texts that aim to spread its radical ideology, and most importantly the controversial digital edition of the ISIS online magazine 'Dabiq'. Since its emergence in July 2014, Dabiq was hosted by justpaste.it, and archive.org. The English language magazine ostensibly targets Western audiences to garner new recruits [Figures 2-4].

Figure 2: Dabiq Magazine issue hosted by justpaste.it [full url is obfuscated]

Figure 3: Tweet with extreme content posted by ISIS members on justpaste.it [full url is obfuscated]

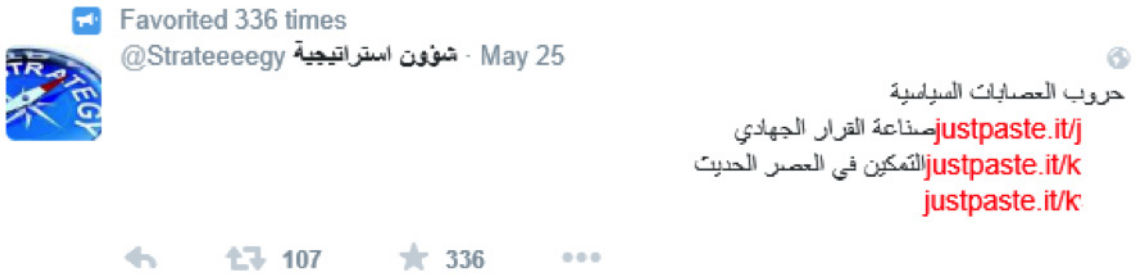


Figure 4: Tweet with material advertising migration to ISIS-held territory posted on justpaste.it [full url is obfuscated]

Justpaste.it not only allows ISIS to host the magazine but also offers a free folder share option which ISIS's networked affiliates can use to share, store and disseminate information to global audiences. The platform offers advanced features such as pasting text directly from a word processor or a webpage, formatting and exporting to PDF, automatic importing of images, secure content publishing, secure SSL connection, and password-protected access. To protect the contents of text notes from web crawlers the site allows the use of [encrypt] tags. Indeed, one of the most valuable options Justpaste.it offers is password protection for disseminated content which makes it a uniquely secure environment for exchanging messages or files.

Describing the site's appeal to users, Carmen Fishwick also pointed out the easy to use template working well even on slow internet connections.[38] Justpaste.it, also has a mobile phone app with no interruptions from pop-ups or other advertising materials. [4] Leveraging these features, ISIS members and affiliates have utilized Justpaste.it to send encrypted messages, upload videos and files (such as jihadi materials, books, instructions), share information and upload online magazines. Links to content uploaded on the site have been shared via Twitter, Facebook, Telegram, and other social media platforms to increase participation for potential recruits, propaganda, and other logistical support. Overall, Justpaste.it appears to have proved helpful to ISIS affiliates, as folders and files can be widely shared by only copying a hybrid link allowing the file to be printed or read online.

4 Writing formatting tools are also available for right-to-left languages (e.g. Arabic). No logon credentials are needed and the platform works on mobile phone devices (justpaste.it, 2014).

Arguably, the pervasiveness of ISIS' Dabiq and Romyiah magazines is indebted to the existence of this sharing portal. Interestingly, files uploaded to justpaste.it can be deleted under the TOS agreement, according to Justpaste TOS:

- Any material posted anonymously will be deleted after five days.
- Any content that may spread hate or cause harm will be removed instantly.

Fishwick underlines how the anonymity of justpaste.it served ISIS, noting that "JustPaste.it's role in Islamic state's propaganda machine has largely gone unnoticed".[39] All the images uploaded to the service by ISIS members have details of a related Twitter account stamped on them. The user's Twitter handle is also printed at the bottom of each image, so reporters have been crediting the images to Twitter. The use of justpaste.it by ISIS members has brought international attention to the site as the traffic approached 10 million page views a month [Figure 5].

Figure 5: Justpaste.it traffic. Source: http://www.alexa.com/siteinfo/justpaste.it

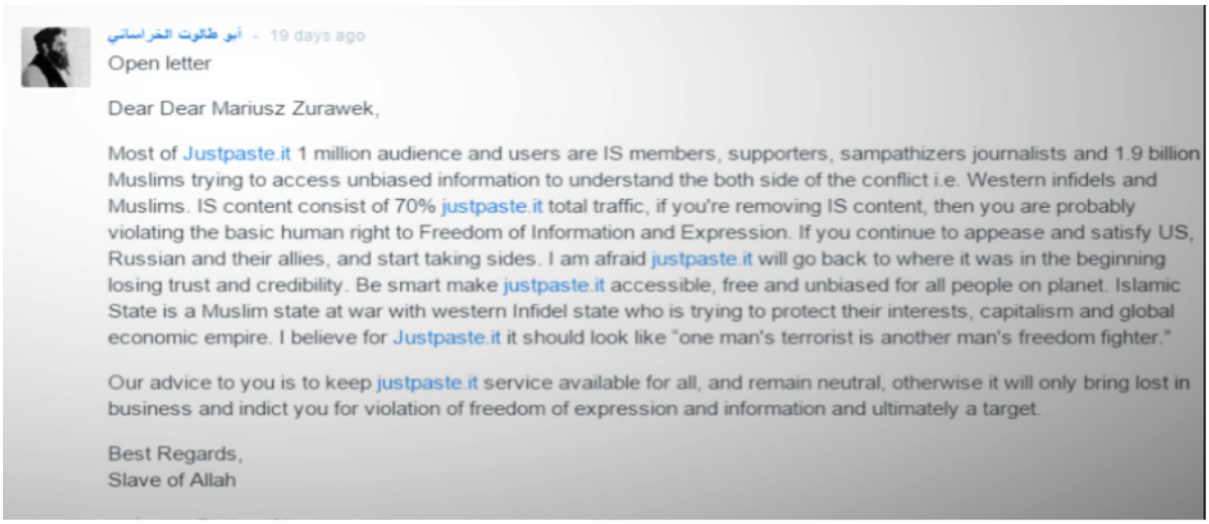
According to Google Analytics (2015), "the platform has about 2.5 million unique users a month, which works out at about 10 million views every month".[5] Zurawek, the site's founder, started seeing what he called "a large growth" of traffic to his website from Saudi Arabia, Egypt and Syria. The site makes it easy to publish text, photos or PDFs, and at the beginning of 2014 rebels and civilians in Syria discovered JustPaste.it and began using it to post news. But sometime over the summer of 2014, Jacob Silverman notes, "jihadists discovered it as well, and the site soon became one of the favoured tools of the Islamic State for sharing news, official communiques, and graphic propaganda".[40]

5 As justpaste.it tweeted on 12/Aug/2014. See, https://twitter.com/justpasteit/status/499153334377660417

As stated by its founder, the site "does not compete with advanced online text editors, such as Google Docs or Microsoft Office 365, but rather creates a place that is extremely easy and simple to use. It's similar to Pastebin, the service popular with hackers, but with image files too".[41] As the activity of ISIS on Justpaste.it drew the attention of authorities in the United Kingdom, the police requested the site delete content including all videos showing graphic executions at the hands of ISIS, as well as all pro-ISIS propaganda. In combating ISIS' use of his service, Zurawek commented: "It's not my choice that ISIS has selected my site [...] As long as I'm cooperating with the police, removing content, and not allowing ISIS to make propaganda, I think it's good for the site that many people will know about it".[42]

The architecture of justpaste.it, coupled with the possibility of using VPNs and TOR to obfuscate IP addresses makes it hard to ban specific users.[43] Nevertheless, the site appears to have made an effort to police the content uploaded by users and actively remove extremist materials. In response, an ISIS affiliate - Abo-Taloot al-Khrasani - messaged Zurawek to condemn the site's efforts to police uploaded content. This demonstrates how significant the platform is to ISIS in maintaining its communication and dissemination structure. In the letter below the author claims that 70% of justpase.it traffic is ISIS content [Figure 6].

Figure 6: A copy of letter sent by Abo Talout al-Khurasani to Zurawek (source: justpaste.it)



2. *Sendvid.com*

Sendvid is an instant video upload portal used by ISIS to route around wide account suspension and content deletion on YouTube and Daily Motion. Specifically, ISIS media production outlets such as Al-Hayat, al-Furqan, and al-Etisam extensively used the video uploading portal in their propaganda dissemination. High-definition quality videos such as *Flames of War, Message Covered with Blood*, and *Healing of the Hearts* were first uploaded to Sendvid, and then popularized virally through Twitter follower networks. A simple search for Sendvid on Twitter returns mostly links to ISIS propaganda videos. Sendvid is a crucial element of ISIS's information logistics as videos linked to Sendvid can also be shared via other social networks such as Facebook, Twitter, archive.org, Tumblr, Telegram, dump.to and e-mail, or can be stored in users' Google drive or Dropbox for future retrieval.

Sendvid has been used by ISIS affiliates early 2015 to widely copy and aggregate propaganda materials, thus building publicly available collections of terrorist-related content. As Remzy Mahzam points out, "the electronic digitisation of the extremist identity of ISIS has been made effective through its frequent injection of videos, incessant release of periodicals and downloading of visual reports in multiple languages, eventually building up a digital compendium that will remain accessible for future generations for reference".[44] Furthermore, unlike YouTube, Facebook and Twitter, where admins are alerted to remove both jihadi content and the associated accounts, Sendvid is a safely unpoliced archiving platform where data can be uploaded anonymously even under false Facebook, Twitter or Google accounts.

The following appears to be the standard reply to enquiries regarding jihadi content by the Sendvid Support Team: "Thank you for contacting us regarding this matter. As a service provider, we try to promote freedom of speech and remain as neutral as possible to all groups regardless of their views. With that being said, we do work with several foreign and domestic agencies in removing videos that we deem to be in violation of our Terms of Service. If you encounter any videos that violate our TOS, we encourage you to report them to our abuse department at: abuse@sendvid.com". In theory, all online sharing portals have very much the same TOS in regard to removing videos or documents promoting violence. Sendvid's TOS are quite clear that the service does not allow "adult, obscene, illegal or objectionable content", and that "accounts and content that violate this will be removed without warning". In practice, Sendvid host these videos unless explicitly notified of breach of TOS. Most of the gruesome videos uploaded by ISIS are in fact still available on the Sendvid service, and are freely shared on Twitter [Figure7 - 8].

Figure 7: Video titled 'The happiness of almojahideen' posted to Sendvid.

Figure 8: Sendvid links to ISIS content, titled: message to the tyrants of Jordan.

Interestingly, recently Sendvid has become a preferred site for pornographic materials, which appears to have caused ISIS affiliates to reduce their presence as this contradicts with Islamic Sharia values.

3. *Dump.to*

Dump.to is an online sharing platform with no login credentials,[6] using archive.is as a web carrier. The sharing portal also has no clear TOS policies that govern dissemination of content. The importance of this service in the context of ISIS is that it allows users to share, upload and converge links from similar sharing sites such as *justpast.it* and *sendvid.com* where all types of data can be stored and shared via link to ISIS' affiliate networks. Dump.to allows documents, video, voice messages, and music to be stored and shared, which in turn allows ISIS affiliates to aggregate, edit, curate, re-classify, and re-publish jihadi propaganda content. In addition, content shared on the site can be protected by password, and be commented on and edited by anyone using a pseudonym or anonymously. Most importantly, the lack of policing and governance makes Dump.to a vital medium for information sharing among jihadists, who can communicate in the open through encrypted messages posted directly through the site's interface.

The site hosts most of ISIS' online video propaganda content, as well as jihadi music (nasheed), Dabiq magazine links, and extreme jihadi books. For example, most of ISIS's controversial books such as *Hijra to the Islamic state* (migrating to ISIS land) and *How to Survive in the West* were available to download for free, arguably helping ISIS to recruit western affiliates and encouraging migration to ISIS-controlled territories (Figures 9-14).

6 Dump.to is registered to a German company operating behind the kasserver.com domain

Figure 9: iBRABO highlights the use of dump.to by ISIS

Figure 10: Jihadi training materials, books, and propaganda

Figure 11: Dabiq propaganda magazine on Dump.to web addresses

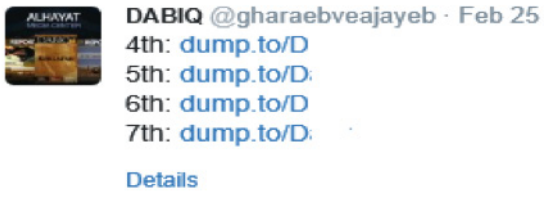


Figure 12: Dump.to hosts Welayat news

Figure 13: Some significant dumps by Al Hayat media centre (news reports, breaking news)

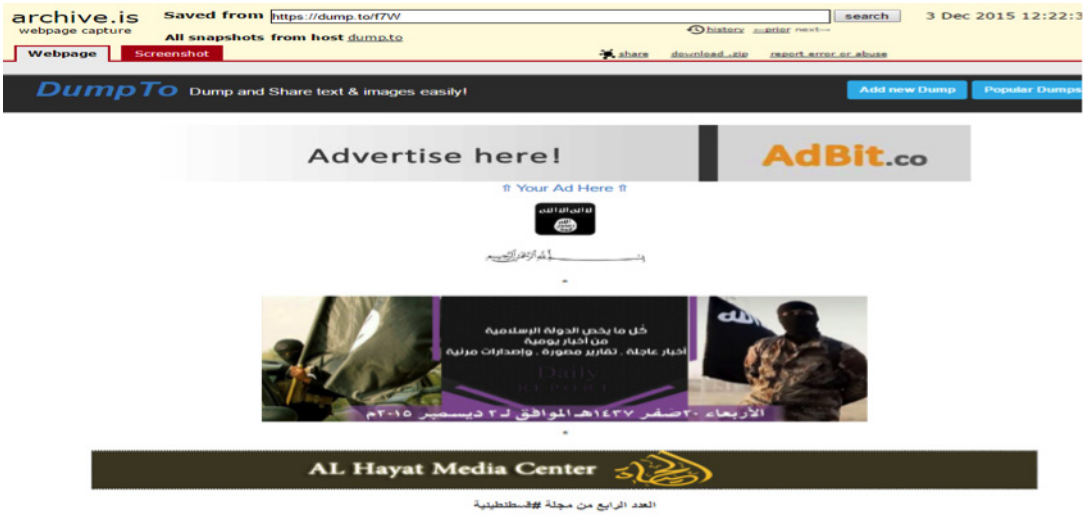


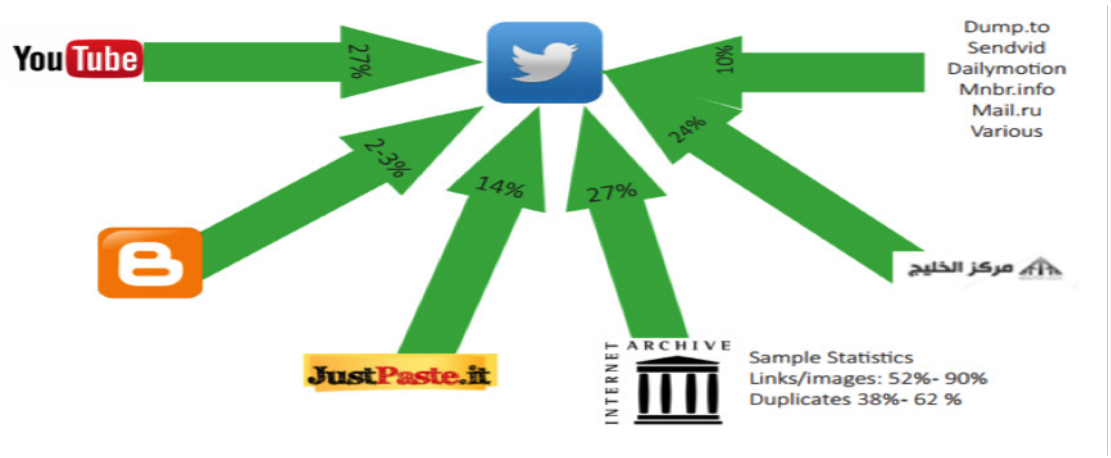
Figure 14: ISIS breaking news shared instantly on Dump.to

Dump.to considers itself a free and anonymous publishing platform that never takes responsibility for content being published. Typical of similar sharing portals, Dump.to TOS claim to prevent content or material containing child pornography, phishing & malware, violent threats, spam campaigns, private and confidential information, invasion of privacy.[7]

Discussion

As their presence started to fade on Twitter and YouTube as a result of the globally coordinated filtering campaign, ISIS decided to move the primary hub of their information operations to anonymous sharing portals such as Telegram, Justpaste.it, Sendvid.com, and Dump.to. This was a strategic decision, as these sites transitioned from being auxiliary platforms to primary communication and dissemination channels in ISIS's strategy. The characteristics and typology of these anonymous sharing portals, ready templates, easy video uploads and mobile phone supported applications created participatory media environments where information can be accessed across multiple social media networks. It is estimated that Justpaste.it, Sendvid.com and Dump.to portals have contributed around 20% of information disseminated by ISIS to Twitter alone (Figure 15).

Figure 15: Detrimental Use of Social Media by Daesh. An Information Warfare Perspective



Source: Joseph Shasheen, 'Detrimental Use of Social Media and the Case of Daesh: An Information Warfare Perspective', *Riga Strategic Communication Dialogue: Perception Matters,* August 2015.

7 An enquiry about ISIS' use of Dump.to services leads to the following standard reply from the company:

> Dear visitor,
>
> We are sorry that you have found improper content in our network. Please note that in order to process your abuse report and protect our users' privacy and integrity, we request that you provide a photo ID (ID/Driving License/Passport/...) within 24 hours by replying to this email.
>
> NOTE: Your report will automatically be rejected if you do not submit the requested documents
>
> Dump.To team.

To an extent, these new sharing portals empower ISIS's message by enhancing connectivity in the network and by adding more actors to its structure. From an ANT perspective, these new sharing portals serve as information intermediaries, allowing for fluid and anonymous information aggregation, curation, and dispersal. Publicly available, no-login anonymity allows links and content to be aggregated and mass-distributed continuously and with variable dynamic intensity based on ad-hoc requirements. These platform architectures allowed ISIS to maintain its flow of information, enlist new actors, and leverage its distributed affiliate and sympathizer networks to reach and mobilize potential jihadists around the world. Furthermore, as we suggested above, anonymous sharing platforms play a key role in the ongoing information warfare waged by ISIS. By using anonymous sharing platforms as black boxes in its information network, ISIS was able to route around social media account suspensions, and leverage these platforms as strategic information weapons serving its information operation objectives.

Importantly, as Krieger and Belliger point out, enhancing connectivity across the network generates information flows that are "increasingly difficult to control and steer".[45] It can be argued that anonymous sharing portals such as Sendvid.com, Justpast.it and Dump.to, "consisting neither of objects nor subjects, but actors and mediators",[46] act as enabling black box media hubs in ISIS' sinformation operation strategy.

In examining the TOS policies of social media networks and anonymous sharing portals in relation to ISIS use of their services, we found out that the financial capabilities and reputation of Twitter, Facebook and Google motivated them to take immediate actions against jihadi content. Meanwhile, the three anonymous sharing portals we examined have the overriding aim of expanding their user-base, and seem to have extremely limited resources to track down content disseminated by ISIS or other extremist networks who seek an easy, secure and fast medium of communication. The lack of resources makes policing and active removal of ISIS content prohibitively expensive to the proprietors of these platforms.

Moreover, as already mentioned, the coordinated campaign to police Twitter and YouTube for jihadist content has forced ISIS to shift its focus towards using anonymous sharing portals as primary tools for aggregation and dissemination of propaganda content. The anonymous functionality of these portals acts as a black box, obfuscating the logistics of ISIS's global propaganda network. When coupled with the ability to create hybrid weblinks and PDF files, which then can be disseminated across most social media, these platforms enable the rapid redistribution of content even under conditions of drastic policing and filtering. Even though anonymous sharing portals seem to have intensified their efforts to remove ISIS-related content, this does not solve the underlying problem as ISIS affiliates can still use these services as aggregators for content advertised on other anonymous social media platforms such as Telegram.

Conclusion

This article is a first step in examining the role of anonymous sharing portals in relation to the dissemination of ISIS propaganda and network communication in the aftermath of the global ISIS-related content degrading operation orchestrated by the most popular social media platforms. Our aim was to highlight the significance of anonymous sharing portals in terms of ISIS's propaganda campaign. We argued that anonymous sharing portals acted as black boxes for ISIS-related propaganda content, helping terror networks to sustain high-

intensity information flows and maintain global communication channels. The emergence of these portals has fundamentally changed the way ISIS distributes its propaganda globally, in that these platforms allow terror networks safe aggregation and the ability to disseminate content links rapidly across popular social media without suffering from efforts to degrade the network. This in turn has enabled terror networks to maintain global information operations even in the face of coordinated efforts at policing and filtering.

About the Authors: **Ahmad Shehabat *is*** *a PhD candidate in the School of the Arts, English and Media, University of Wollongong. His current research examines the digital media logistics of ISIS networks. Ahmad's previous research focused on the role of digital media networks during the Arab Spring uprisings. (ams591@uowmail.edu.au).* **Teodor Mitew** *is a Senior Lecturer in digital media at the University of Wollongong, with a background in actor network theory and internet studies. His current projects range across the internet of things, swarm content networks, memetic warfare, object oriented ontology, and smart textiles. (tmitew@uow.edu.au)*

Notes

[1] Berger, J. (2015). The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion. *Perspectives on Terrorism, 9*(4).

[2] Krieger, D. J. and A. Belliger (2014). *Interpreting Networks: Hermeneutics, Actor-network Theory & New Media*, Transcript-Verlag,p. 9.

[3] Ibid, p.38.

[4] Cited in Kanngieser, A., Neilson, B., Rossiter, N. (2014) 'What is a research platform? Mapping methods, mobilities and subjectivities', *Media, Culture & Society,* 36 (3), 302-318.

[5] Moore, C. (2014). "Screenshots as Virtual Photography." In Arthur, P., Bode, K. (Eds.) *Advancing Digital Humanities: Research, Methods, Theories*, Palgrave Macmilan: London. P. 141.

[6] Schmitt, E. (2015). [U.S Intensifies Effort to Blunt ISIS' Message].

[7] Seib, P., & Janbek, D. M. (2010). *Global terrorism and new media: The post-Al Qaeda generation*: Routledge. p. 114.

[8] Atwan, A. B. (2015). *Islamic State: The Digital Caliphate*: Univ of California Press. p.145.

[9] Seib & Janbek, 2010, p.114.

[10] Kimery, A. (2015, 23/3/2015). ISIS' Hit List Of US Military Personnel Isn't First Hit List Issued By Jihadists; Service Members On Aler, *Today.us*. Retrieved from http://www.hstoday.us/channels/dhs/single-article-page/isis-hit-list-of-us-military-personnel-isnt-first-hit-list-issued-by-jihadists-service-members-on-alert/72d87ad61e4d8038409fd59646bedde9.html

[11] Higham, G. M. S. (2015, 8/may). In a propaganda war against ISIS, the U.S. tried to play by the enemy's rules, national security, *The washington post*. Retrieved from https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html.

[12] Arthur, C. (2014, 23/6/2014). Taking down Isis material from Twitter or YouTube not as clear cut as it seems, *Theguardian*. Retrieved from http://www.theguardian.com/world/2014/jun/23/taking-down-isis-youtube-twitter-google-video

[13] Higham, 2015, ibid.

[14] ibid.

[15] Griffin, A. (2015, 28 December, 2015). Anonymous war on Isis: Online activists claim to have foiled terror attack on Italy as part of 'Operation Isis', *The Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-war-on-isis-online-activists-claim-to-have-foiled-terror-attack-on-italy-as-part-of-a6788001.html

[16] Berger, 2015, ibid.

[17] Alvares, C., & Dahlgren, P. (2016). Populism, extremism and media: Mapping an uncertain terrain, *European Journal of Communication, 31*(1), 46-57.

[18] Klausen, J. (2015). Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict*

& Terrorism, 38(1), 1-22.

[19] Shehabat, A., Mitew, T., Alzoubi, Y. (2017) 'Encrypted Jihad: Investigating the Role of the Telegram App in Lone Wolf Attacks in the West', *Journal of Strategic Security*, 10(3), 27-53.

[20] Silverman, J. (2014). "Loose Tweets Sink Ships: Will the Islamic State's aggressive Internet strategy expose it to investigators?", *Politico*. Retrieved from http://www.politico.com/magazine/story/2014/08/islamic-state-twitter-110418.html#.VbrPIPmqqko

[21] Berger, J., & Strathearn, B. (2013). *Who Matters Online: Measuring Influence, Evaluating Content and Countering Violent Exremism in Online Social Networks*. p.41.

[22] Berger, 2015, ibid.

[23] ibid. p.9.

[24] Silverman, ibid.

[25] Atwan, 2015, ibid.

[26] Brehmer, B. (2005). *The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control.* Paper presented at the Proceedings of the 10th international command and control research technology symposium, p.10.

[27] Shehabat, A., & Mitew, T. (2017). Distributed Swarming and Stigmergic Effects on ISIS Networks: OODA Loop Model. *Journal of media and information Warfare,* 10, p. 79-109.

[28] For an accessible introduction to the methodology of ANT, see Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory,* Oxford: Oxford University Press.

[29] ibid, p.7.

[30] Latour, B. (1999). On recalling ANT. In J. Law & J. Hassard (Eds.), *Actor Network Theory and After* (pp. 15-25). Oxford: Blackwell Publishers.

[31] Law, J. (1999). After ANT: complexity, naming and topology. In J. Law & J. Hassard (Eds.), *Actor Network Theory and After* (pp. 1-14). Oxford: Blackwell Publishers, p.3

[32] Callon, M. (1986). The sociology of an Actor-Network: the case of the electric vehicle. In M. Callon, J. Law & A. Rip (Eds.), *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World* (pp. 19-34). London: Macmillan Press, p.31.

[33] Besel, R. D. (2011). Opening the "Black Box" of Climate Change Science: Actor-Network Theory and Rhetorical Practice in Scientific Controversies. *Southern Communication Journal, 76*(2), p. 120-136.

[34] Cressman, D. (2009). A brief overview of actor-network theory: Punctualization, heterogeneous engineering & translation, p.6.

[35] Krieger, D. J., & Belliger, 2014, p. 9.

[36] Stern, J., & Modi, A. (2010). Producing terror: organizational dynamics of survival. In D.M. Jones, A. Lane, and P. Schulte (Eds.), *Terrorism, Security and the Power of Informal Networks*, (pp. 257-288), UK: Edward Elgar Publishing, p. 282.

[37] Fishwick, C. (2015, 15/Aug/2014). How a Polish student's website became an Isis propaganda tool, *The Guardian*. Retrieved from https://www.theguardian.com/world/2014/aug/15/-sp-polish-man-website-isis-propaganda-tool

[38] ibid.

[39] ibid.

[40] Silverman, 2014, ibid.

[41] Fishwick, 2015, ibid.

[42] ibid.

[43] ibid.

[44] Mahzam, R. (2015, 1/11/2015). the electronic digitisation of ISIS building a multimedia legacy analysis, *Euroasia review* Retrieved from http://www.eurasiareview.com/01112015-the-electronic-digitisation-of-isis-building-a-multi-media-legacy-analysis/

[45] Krieger, D. J., & Belliger, 2014, p. 143, ibid.

[46] ibid, p.187.