ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

18

ISSUE 2/2023

Milano 2023

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 18/2023

Direttore Responsabile:

Matteo Vergani (Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi (Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou (Lecturer at National Security School – Atene)
Cristian Barna ("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti (senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis (Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio (Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel (London School of Economics – London)
Rovshan Ibrahimov (Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler (German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš (Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi (Università Cattolica del Sacro Cuore – Milano)
Anita Perešin (University of Zagreb – Croatia)
Giovanni Pisapia (Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj (University of Ljubljana)
Eman Ragab (Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli (Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick (University of Aarhus – Denmark)
Arturo Varvelli (Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz (Independent Researcher – Turkish National Police)
Munir Zamir (Fida Management&C7 – London)
Sabina Zgaga (University of Maribor – Slovenia)
Ivo Veenkamp (Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni (Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa (Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini (Università Cattolica del Sacro Cuore – Milano)
Marco Maiolino (Università Cattolica del Sacro Cuore – Milano)
Davide Scotti (Università Cattolica del Sacro Cuore – Milano)

© 2023 EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 979-12-5535-198-6

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Time to be realistic about Swarmcast2.0: How terrorists use WhatsApp

Ali Fisher

Ali Fisher is Lecturer at Università Cattolica del Sacro Cuore, Milano as part of the ITSTIME research team. He is also Explorer of Extreme Realms at Human Cognition and has a dual specialism in Strategic Communication and Data Science focusing on the darkest human behaviors. Ali draws on his dual specialisms of Strategic Communication and Data Science to deliver strategic insight into complex information ecosystems. Influences range from Strategic Communication, Public Diplomacy, and Human Security to the extreme realms; Terrorism, Extremism and Child Sexual Exploitation. Previously Principal Data Scientist at VORTEX, (University of Vienna), CPD Research Fellow, (University of Southern California). Ali uses innovative approaches, network analysis, and big data to help a range of organisations track and counter the behaviour of extremists online.

Abstract

This article addresses two significant gaps in the current literature. First it challenges the orthodox claims that Salafi-Jihadi are forced to use smaller platforms because of the success of 'deplatforming' strategies adopted by so-called internet giants and second it does this by highlighting the significant presence of Salafi-Jihadi networks on WhatsApp. With over two billion users, WhatsApp is an social giant by any estimation.

Through the discussion of the networks on WhatsApp, the article demonstrates that while the Western metanarrative has long been accepted by the orthodoxy of Terrorism Studies, and is still resonates at events hosted by industry funded bodies, the challenge encapsulated by Swarmcast2.0 remains.[1] Salafi-Jihadi groups and the media mujahidin maintain persistent networks which function across multiple platforms simultaneously, including networks on the some of the largest platforms.[2]

The paper argues for greater attention to be paid to an authentic understanding of the ways Salafi-Jihadi communicate shared meaning and maintain networks. It concludes, concludes there is a need for significantly greater understanding of the way Salafi-Jihadi networks are still able to operate on the largest platforms, requiring an understanding of dynamic networks in addition to the static content files they share.

Questo articolo affronta due significative lacune nella letteratura attuale. In primo luogo, mette in discussione le affermazioni ortodosse secondo cui i salafiti-jihadisti sarebbero costretti a utilizzare piattaforme più piccole a causa del successo delle strategie di "deplatforming" adottate dai cosiddetti giganti di Internet; in secondo luogo, evidenzia la presenza significativa di reti salafite-jihadiste su WhatsApp. Con oltre due miliardi di utenti, WhatsApp è un gigante sociale a tutti gli effetti.

[1] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.

[2] https://static.rusi.org/20190716_grntt_paper_06.pdf.

Attraverso la discussione delle reti su WhatsApp, l'articolo dimostra che mentre la metanarrativa occidentale è stata a lungo accettata dall'ortodossia degli studi sul terrorismo e risuona ancora negli eventi ospitati da enti finanziati dall'industria, la sfida incapsulata da Swarmcast2.0 rimane. I gruppi salafiti e jihadisti mediatici mantengono reti persistenti che funzionano su più piattaforme contemporaneamente, comprese quelle su alcune delle piattaforme più grandi.
Il documento sostiene la necessità di prestare maggiore attenzione a una comprensione autentica dei modi in cui i salafiti-jihadisti comunicano un significato condiviso e mantengono le reti. In conclusione, è necessaria una comprensione significativamente maggiore del modo in cui le reti salafite-jihadiste sono ancora in grado di operare sulle piattaforme più grandi, richiedendo una comprensione delle reti dinamiche in aggiunta ai file di contenuto statico che condividono.

Keywords

Swarmcast; networks; Salafi-Jihadi; terrorism; platforms;

1. Introduction

For all the meetings, presentations and reports from embedded academics and industry groups, purporting to show success against Salafi-Jihadi groups, the movement is still comfortably able to disseminate content through Swarmcast2.0.

This article addresses two significant gaps in the current literature. First it challenges the orthodox claims that Salafi-Jihadi are forced to use smaller platforms because of the success of 'deplatforming' strategies adopted by so-called internet giants and second it does this by highlighting the significant presence of Salafi-Jihadi networks on WhatsApp. With over two billion users, group chats with over 1,000 members and now broadcast 'channels', WhatsApp is an social giant by any estimation.[3]

Through the discussion of the networks on WhatsApp, the article demonstrates that while the Western metanarrative has long been accepted by the orthodoxy of Terrorism Studies, and is still resonates at events hosted by industry funded bodies, the challenge encapsulated by Swarmcast2.0 remains.[4] Salafi-Jihadi groups and the media mujahidin maintain persistent networks which function across multiple platforms simultaneously, including networks on the some of the largest platforms.[5]

The paper argues for greater attention to be paid to an authentic understanding of the ways Salafi-Jihadi communicate shared meaning, maintain networks and reiterates as argued previously:

> If Terrorism Studies and policy makers continue to buy into the 'success narrative', rather than grasp the increasing complex constant evolution of the Swarmcast2.0

[3] https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-103-Favourite-Social-Media-Platforms.png. https://techpp.com/2023/09/28/whatsapp-channels-guide/.
[4] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.
[5] https://static.rusi.org/20190716_grntt_paper_06.pdf.

there is an increasing risk that disruption efforts will be using Web 2.0 approaches in a Web3 world.[6]

The paper concludes there is a need for significantly greater understanding of the way Salafi-Jihadi networks are still able to operate on the largest platforms, requiring an understanding of dynamic networks in addition to the static content files they share.

2. Facing Swarmcast2.0 requires clarity

Jihadist groups have used social media sites for over a decade as part of the sanctioned role of the Media Mujahidin.[7] The sanctioning of jihadist activity was related to the existing core fatawa (authoritative rulings and ideological decrees). Thus, any local jihadist, al-Qa`ida-affiliated action is placed under the virtual umbrella, increasing the appeal.[8] Initially sites such as Twitter,[9] Facebook, YouTube,[10] and Tumblr[11] were adopted in their attempts to establish online fronts.[12]

In the last ten years Salafi-Jihadi groups have consistently continued their online da'wa efforts to reach their primary target audience via social media. In these networks, new content reached saturation across the network within two hours.[13] Since 2016 Telegram been the preferred core platform.[14] Until 2019, the core networks of extremist groups tended to focus their effort on individual 'beacon' platforms using

[6] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.
[7] "Al-Manhajiyya fi tahsil al-khibra al-i'lamiyya, Mu'assasat al-Furqan & Markaz al-Yaqin, part 1," Markaz al-Yaqin and al-Furqan, May 2011.
[8] Prem Mahadevan, "The Glocalisation of al-Qaedaism," Center for Security Studies, March 22, 2013.
[9] Ali Fisher and Nico Prucha, "Jihadi Twitter Activism – Introduction," Jihadica.com, April 27, 2013.
[10] Cori E. Dauber, "YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer," U.S. Army War College, 2009.
[11] Rüdiger Lohlker, "Tumbling Along the Straight Path – Jihadis on tumblr.com," University of Vienna, August 2012. Later exploitation was examined in: Carvalho, Claudia. "'Kids in the Green Lands of the Khilafat'—A Tumblr Case Study of Imagery within the Jihad 3.0 Narrative." *European Muslims and New Media* 5 (2017).
[12] Nico Prucha, "Jihadi Twitter Activism – Introduction"; Nico Prucha, "Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors," Orient 4 (2011).
[13] Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018.
[14] Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. The New Netwar: Countering extremism online. Policy Exchange, 2017. Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021 Sicurezza, Terrorismo e Società 15 (1), 141-170 https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movementon-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf.

the speed, agility and resilience of their network structures to maintain a persistent presence.[15]

Now the Media Mujahidin have entered the Multiplatform Communication Paradigm (MCP) where the core channels of extremist groups are present on two or three platforms leading to the development of Swarmcast2.0. The combination of platforms such as Matrix, Telegram, Rocket limits the impact of contemporary disruption efforts, as user networks can be rebuilt via link sharing on a second or third platform.[16]

This multiplatform approach fits the current user behaviour – in 2022 the average social media user accessed seven different platforms monthly.[17] Having material on numerous platforms provides multiple roots to engage with users. In addition to the core of extremist networks comprising 'official' channels, spontaneous groups of supporters create 'shadow networks' on many mainstream platforms, including Facebook, WhatsApp, YouTube and Instagram using privacy settings to hide in plain sight.

Meanwhile, Western industry groups and embedded academics have claimed "smaller platforms and social media services are where extremists moved to after being shut down by giants like Facebook and Twitter".[18] Another Facebook funded researcher has asserted; "If you're not on Telegram or in a forum, the options are increasingly limited".[19] Such claims belie the networks of supporters which still operate across major social media platforms.[20]

As has been detailed previously, there are significant problems with the Western metanarrative which interprets any change in operational activity as the successful result of content removal and "deplatforming" of Salafi-Jihadi groups.[21] On a con-

[15] Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019). Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence", Perspectives on Terrorism, Vol 9, No 3 (2015).

[16] Fisher, Prucha, Swarmcast2.0. https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.

[17] https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-87-Overview-of-Social-Media-Use.png.

[18] https://www.canberratimes.com.au/story/7515010/isis-app-ignored-by-governments-inquiry/.

[19] https://twitter.com/charliewinter/status/1072501785716318209. Discussed in: https://onlinejihad.net/2019/02/18/how-jihadist-groups-exploit-western-researchers-to-promote-their-theology/.

[20] Fisher, Prucha, Swarmcast2.0, https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf. Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021 Sicurezza, Terrorismo e Società 15 (1), 141-170 https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movementon-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf.

[21] See for example: Conway, Maura, et al. "Disrupting Daesh: Measuring takedown of online terrorist material and its impacts." *Islamic State's Online Activity and Responses*. Routledge, 2020. 141-160. Discussed in: Fisher, Prucha, Swarmcast2.0, https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.

ceptual level, the tendency for some OTS researchers to "whittle away" references to theology with the aim to "uncloak", in their words, the real purpose of the movement, leads to a significant deficit in understanding how the movement communicates. As a result, evidence of Salafi-Jihadi material framed in theological terms is dismissed in Western-centric OTS eyes as irrelevant, even functionless, creating instead a caricature of the Salafi-Jihadi movement, by imposing Western frameworks around crime, kittens, gamification, Nutella, or a jihadi utopia.

While theology is undervalued or overlooked in many OTS accounts of the Salafi-Jihadi movement, the shared understanding of theological reference points between producer and primary target audience enables the clear expression of religious concepts – concepts that are obvious in Arabic, and apparent to anyone familiar with the theological content, but which may be impenetrable code to the uninitiated viewing material from a Western habitus.[22]

On a practical level, there has been a tendency to imply that because embedded academics and those publishing within Orthodox Terrorism Studies (OTS) could not locate branded content from Salafi-Jihadi groups on a specific platform, those groups, their supporters and aligned users did not use the platform. Such a focus has contributed to an aspect of the metanarrative which is particularly detrimental to the understanding of how Salafi-Jihadi networks operate online, the extent to which industry groups have emphasised the line that Salafi-Jihadi groups have been forced to use smaller or niche platforms.

There are a number of problems with this idea, which have been discussed in detail elsewhere.[23] Two, however, are of particularly note where the metanarrative is concerned with Salafi-Jihadi being denied access to larger platforms. First, is an issue of scale, that Salafi-Jihadi preferred platform Telegram[24] has a vastly larger user-base[25] than the so-called 'giant' Twitter (now X). Second, in spite of the metanarrative claiming the ongoing success of driving Salafi-Jihadi to smaller platforms, Salafi-Jihadi material can be easily located on WhatsApp. Meta owned WhatsApp is thought to be "the most popular mobile messenger app worldwide with approximately two billion monthly active users" ranked by Statista behind only Facebook and YouTube as is the third most popular social network worldwide.[26]

On WhatsApp content is available from groups including al-Dawlat al-Islamiyya (IS), AQ, HSM (al-Shabab), Taliban, Hamas, and a range of channels which are

[22] Fisher, Prucha, Swarmcast2.0, https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.

[23] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.

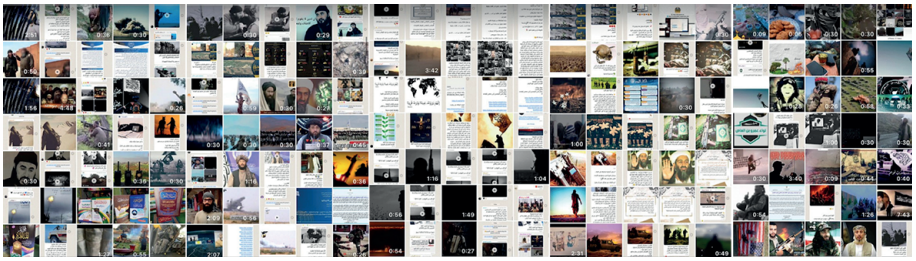
[24] https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf.

[25] https://www.itstime.it/w/towards-a-more-progressive-approach-to-studying-the-salafi-jihadi-movement-by-ali-fisher/.

[26] https://www.statista.com/topics/2018/whatsapp/#topicOverview.

theologically aligned but not branded as supporting a specific group that westerns have labelled a foreign terrorist organisation.

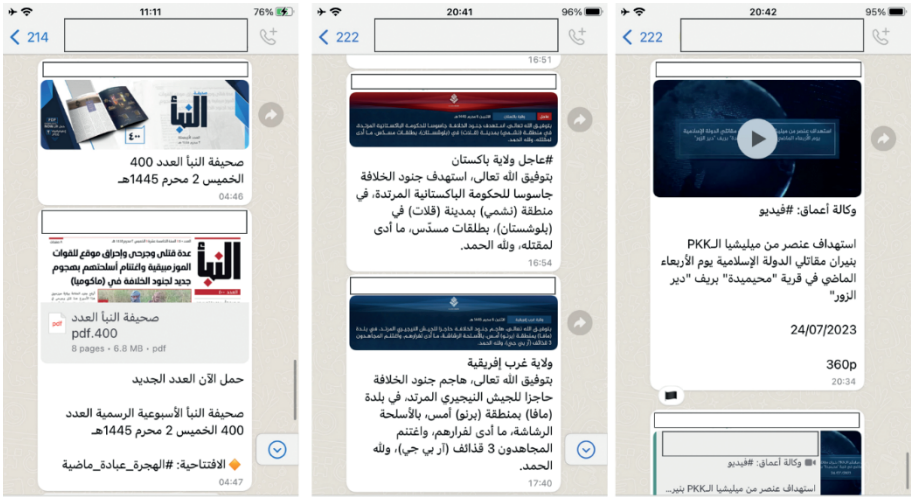
Screenshots of content posted in WhatsApp groups

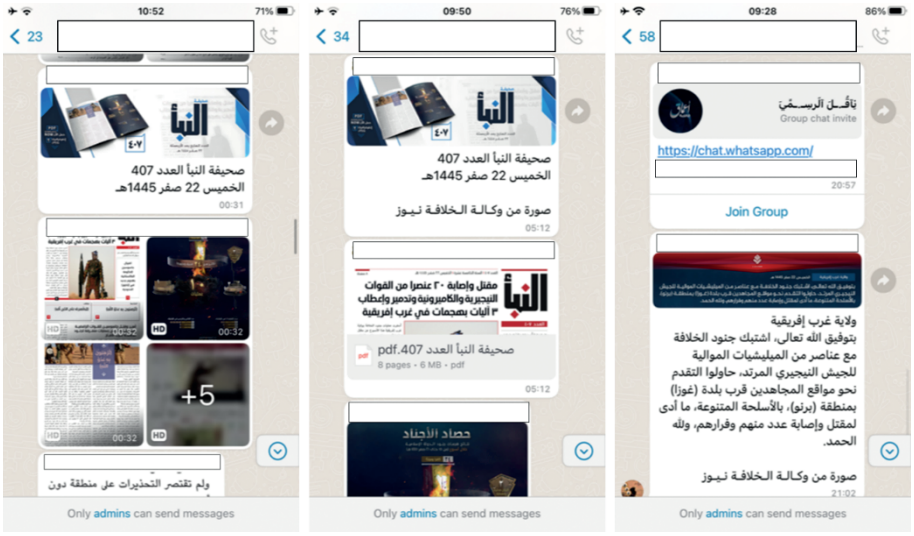


The remaining part of this article will highlight how Salafi-Jihadi networks use their presence on WhatsApp. In each case, personal Identifiable Information and group names have been obscured.

3. IS

Pro-IS networks on WhatsApp have consistently shared the latest issues of al-Naba newspaper, Amaq video statements and the familiar branded announcements of kinetic activity.

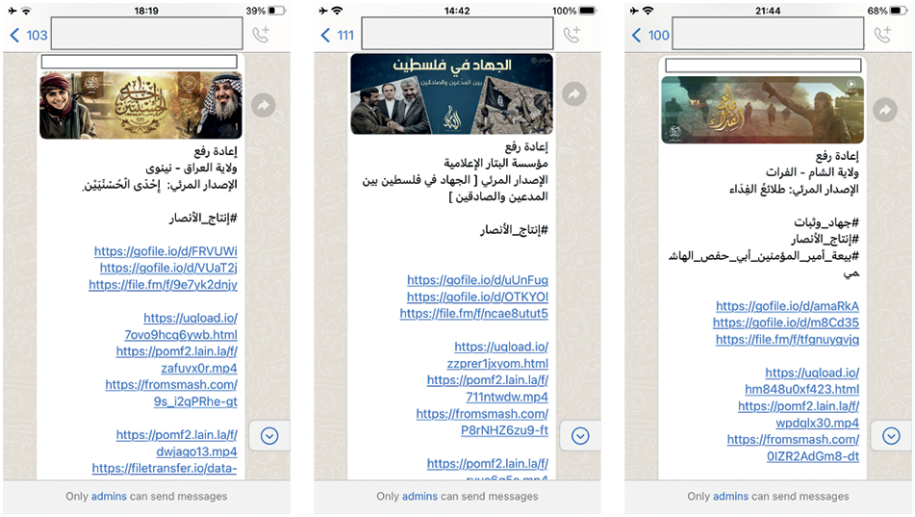




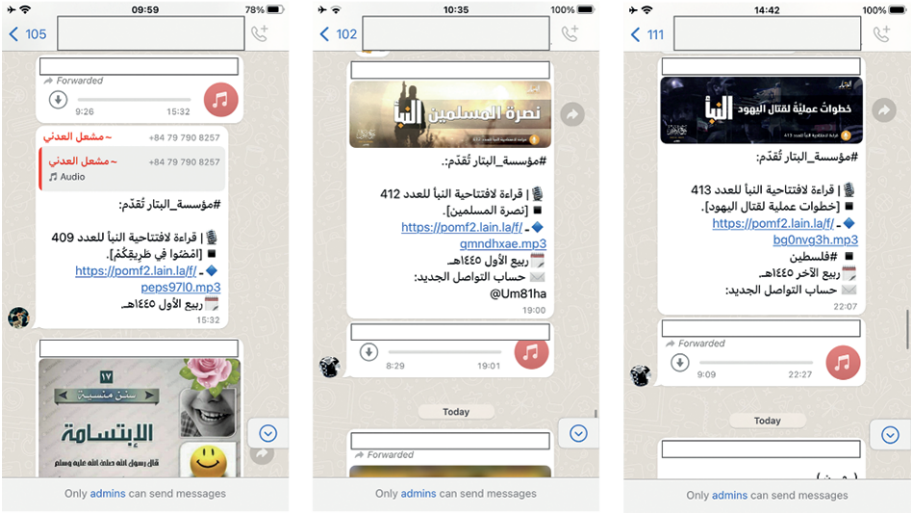
In addition, these networks have used WhatsApp groups to share IS videos.

Here, examples left, a section of a video showing Turkish soldiers being burnt alive. Centre, prisoners executed by being blown up. Right, a prisoner seconds before being executed by an IS child soldier.

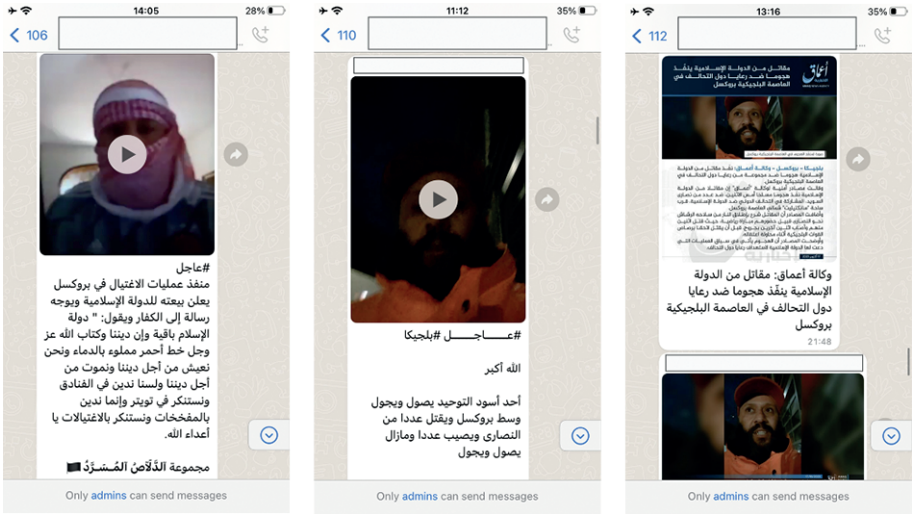
In addition to short sections of videos, the networks also distribute the full videos via filesharing sites and in app downloads.



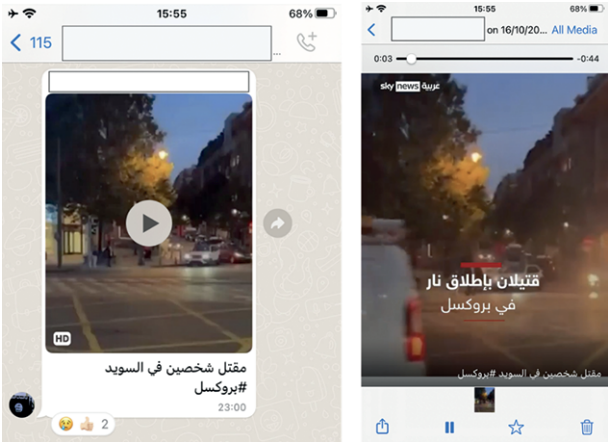
Audio version of al-Naba editorials are made available via in app MP3 and file downloads.



Following the attack killing two Swedish citizens in Brussels on 16th October the official announcements were available on WhatsApp along with the videos made by the attacker.



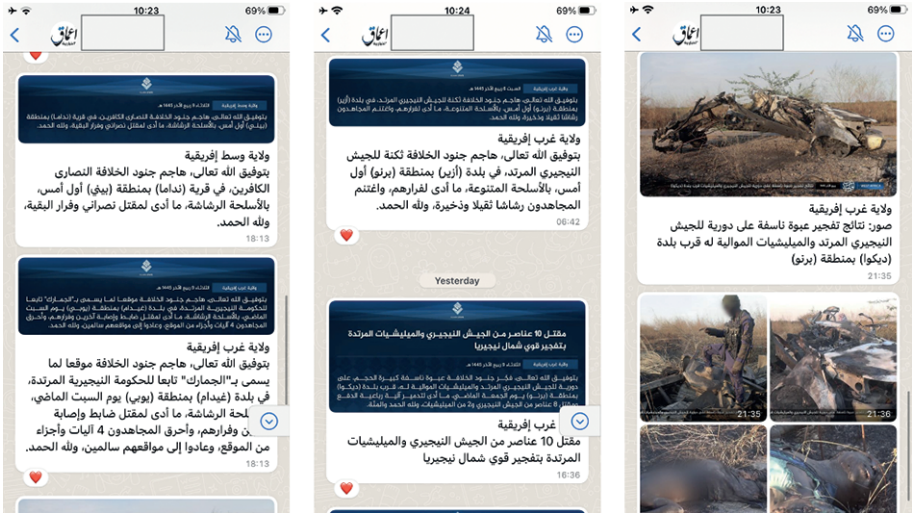
Video of the attack aparently originally broadcast on Sky News, was also shared within groups sharing pro-IS content.



IS have also begun using the WhatsApp Channels which “are a one-way broadcast tool for admins to send text, photos, videos, stickers, and polls”.[27] WhatsApp describes Channels as “a simple, reliable, and private way to receive important updates from people and organizations, right within WhatsApp” as part of their aspiration “to build the most private broadcast service available”.[28] This includes protecting the per-

[27] https://blog.whatsapp.com/introducing-whatsapp-channels-a-private-way-to-follow-what-matters.
[28] https://blog.whatsapp.com/introducing-whatsapp-channels-a-private-way-to-follow-what-matters.

sonal information, such as phone numbers, from both admins and followers.

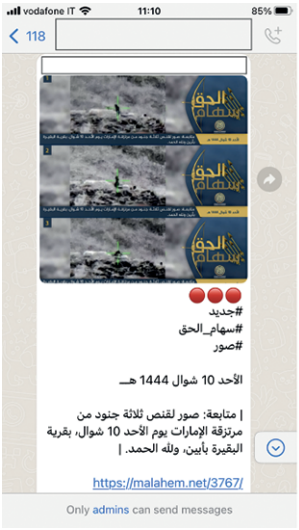


The scale of IS content accessible via WhatsApp alone challenges the metanarrative that Salafi-Jihadi content has been driven onto smaller platforms. However, IS is not alone, based on current tracking Taliban and AQ have been using WhatsApp groups for at least two years.

4. AQ

AQ has used WhatsApp to distribute a wide range of content including, videos, 'news' style announcements, Statements and the One Ummah magazine. As part of the multiplatform communication paradigm (MCP) AQ provide links to other platforms including their Rocket.chat site, and al-Malahem (AQAP) website.[29]

[29] For Multiplatform Communication Paradigm see: Fisher, Ali, Nico Prucha, and Emily Winterbotham. "Mapping the Jihadist Information Ecosystem." *Global Research Network on Terrorism and Technology* 6 (2019). https://static.rusi.org/20190716_grntt_paper_06.pdf.


vodafone IT 11:10 85%
118
#جديد
#سهام_الحق
#صور
الأحد 10 شوال 1444 هـ
| متابعة: صور لقنص ثلاثة جنود من مرتزقة الإمارات يوم الأحد 10 شوال، بقرية البقيرة بأبين، ولله الحمد. |
https://malahem.net/3767/
Only admins can send messages

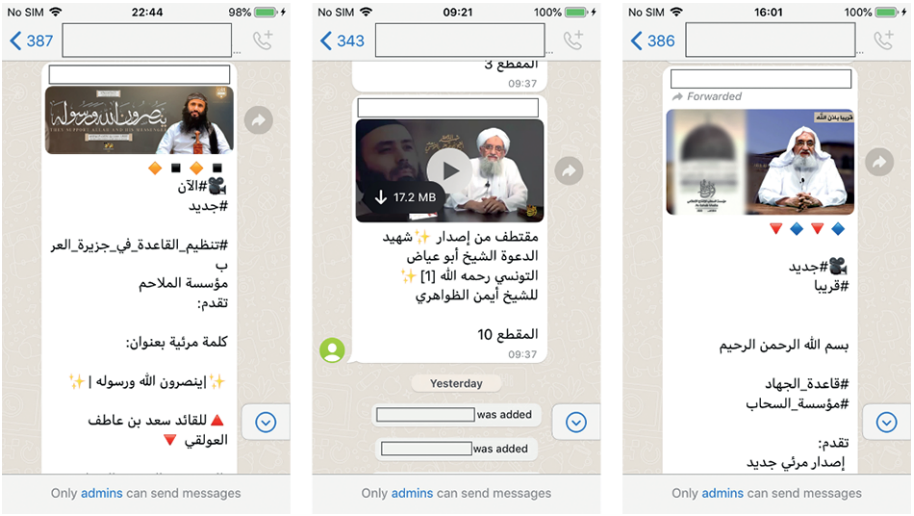

vodafone IT 11:11 84%
118
#إعلان
#جنونيوز
اغلاق التسجيل بعد يومين !!!
بسبب كثرة الرسائل تم تمديد فترة التسجيل على #جنونيوز - المصدر الرسمي لإعلام قاعدة الجهاد - حتى يوم الاربعاء 13 شوال 1444 هـ
للاشتراك على المنصة يرجي الاتصال على الحساب التالي:
https://t.me/GeoNews_Registration_bot
Only admins can send messages


vodafone IT 12:14 32%
38
1 UNREAD MESSAGE
#جديد
بسم الله الرحمن الرحيم
مؤسسة السحاب
قاعدة الجهاد
تقدم
العدد التاسع من مجلة #أمة_واحدة [9]
روابط التحميل والقراءة المباشرة:
Only admins can send messages

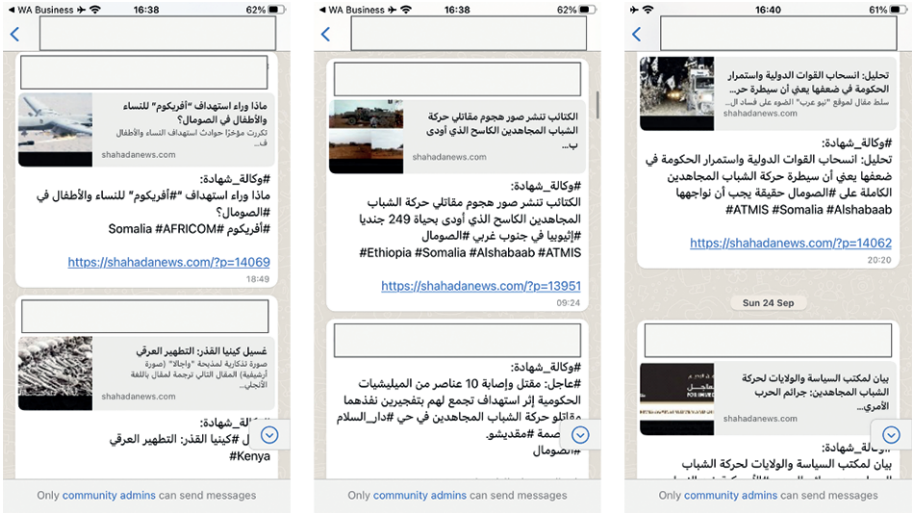

No SIM 16:03 100%
428
3 UNREAD MESSAGES
#الان
#جديد
بسم الله الرحمن الرحيم
#قاعدة_الجهاد
#مؤسسة_السحاب تقدم:
بيان القيادة العامة بعنوان:
Only admins can send messages


No SIM 09:36 100%
439
#جديد
#تنظيم_القاعدة_في_جزيرة_العرب
#مؤسسة_الملاحم
| بيانٌ نَعي الشَّيخ حَمَد بن حمُود التُّميمي |
https://malahem.net/?p=3606
#أنصار_الشريعة
#مهند_المجاهد
Only admins can send messages


No SIM 09:21 100%
343
17.2 MB
مقتطف من إصدار ✨شهيد الدعوة الشيخ أبو عياض التونسي رحمه الله [1] ✨
للشيخ أيمن الظواهري
المقطع 11
16:45
أباد الأمريكان 112 مليون من الهنود الحمر، وتخلل هذه المذابح 731 معاهدة معهم كلما عجزوا عن استئصالهم، لكن الأمريكان لم يلتزموا بتلك المعاهدات.
Only admins can send messages

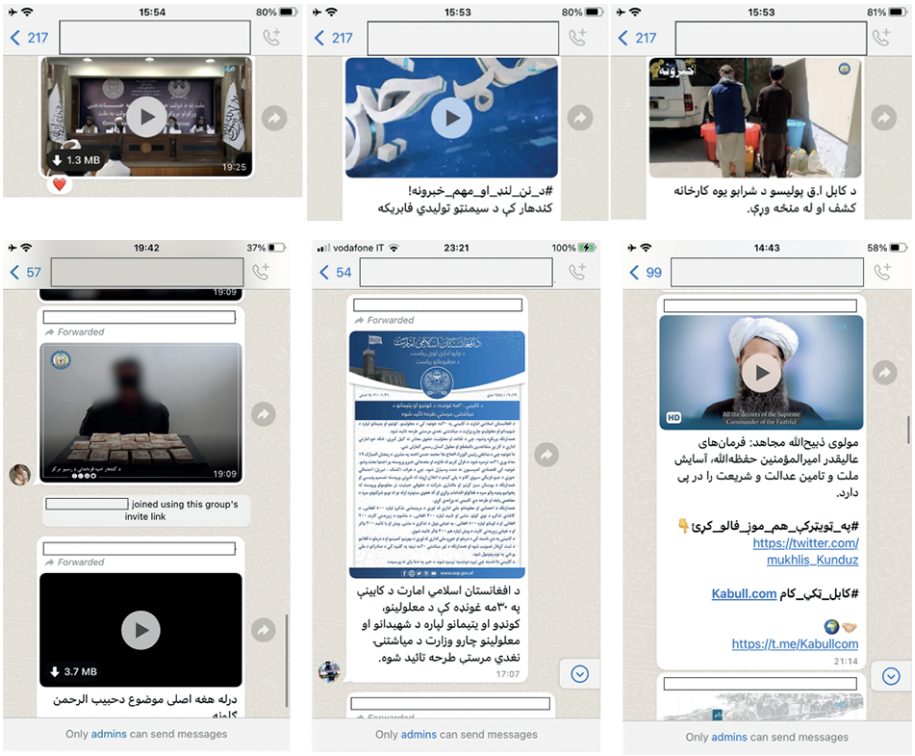


AQAP is not the only AQ 'geographic' presence, for example, HSM (al-Shabaab) uses WhatsApp 'communities' feature. Communities "connect multiple groups together under one umbrella to organize group conversations on WhatsApp".[30] They use the communities within their MCP approach to share links to the articles on Shahada News, and links to their Telegram bots.



[30] https://blog.whatsapp.com/communities-now-available.

5. Taliban / Islamic Emirate of Afghanistan



These are just some of the many thousands of messages, videos and images observed over the last year of monitoring them on WhatApp. The use of WhatsApp as part of the Salafi-Jihadi multiplatform communication paradigm highlights need to break from the pseudo-metrics of the Western Metanarrative and focus on whether the movement can achieve their goal of distributing content to their primary target audience.

Since 2014, there have been those able to find pseudo-metrics[31] through which to claim that a specific tactic had "degraded *IS ability to … distribute content*". The result has been a metanarrative which interprets any development as evidence that the whack-a-mole approach is working. *IS ability to … distribute content*".[32] The result has been a metanarrative which interprets any development as evidence that the whack-a-mole approach is working.[33]

As noted in a recent EICTP report on Swarmcast 2.0:

[31] https://uscpublicdiplomacy.org/blog/interpreting-data-about-isis-online.
[32] https://twitter.com/intelwire/status/513303666368196608.
[33] Frampton, Martin, Ali Fisher, and Nico Prucha. "The New Netwar." *Policy Exchange: Westminster, London* (2017).

> The Salafi-Jihadi movement has continued its da'wa efforts despite repeated claims of success against the movement. We are now seven years after the claims that content distribution had been degraded, six years after the "purported resilience" of Salafi-Jihadi online networks was derided by those in the orthodoxy of Terrorism Studies, and three years after the supposed "full-fledged collapse" of IS media.[34]

Furthermore, during this time the Salafi-Jiahdi movement has adopted a multiplatform communication paradigm and "the tech landscape has changed, some of what are referred to as 'smaller' and 'niche' platforms have become new 'tech giants'," a reality which poses a significant challenge to the metarnarrative of successful action driving the movement to smaller platforms.[35]

Yet as Miron Lakomy put it in an article in *Terrorism and Political Violence*; "despite years of efforts from CVE stakeholders, the propaganda of militant Islamist VEOs is still easily accessible on the Internet".[36] This argument reiterates many of the findings of earlier work, including the article which first identified the mobile enabled Salafi-Jihadi Swarmcast.[37] That 2015 article concluded that;

> future policy to counter the dissemination of Jihadist content must challenge the Swarmcast on a strategic level. To be successful, strategies will need to take account of all three components of the Swarmcast when employing takedowns or other counter measures. his will mean focusing on strategic approaches to disrupting the system-wide emergent structures and collective behaviours rather than the tactical removal of individual accounts.

Eight years on there is little shortage of organisations announcing the latest 'significant blow' they have struck against Salafi-Jihadi groups or reporting the success of their projects.[38] Commentators are frequently willing to report networks being "resolutely trashed".[39] Calls in various so-called 'working groups' are often witness frequent references to how busy people are and how much travel they are doing. However, despite the frenetic pace and the metanarrative of success, Lakomy's study "effectively proves that the current approach to online CVE brought few tangible effects".[40]

[34] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.
[35] https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.
[36] Lakomy, Miron. "Why do online countering violent extremism strategies not work? The case of digital jihad." *Terrorism and political violence* 35.6 (2023): 1261-1298.
[37] https://www.jstor.org/stable/26297378.
[38] https://www.techagainstterrorism.org/2022/12/21/major-al-qaeda-in-arabian-peninsula-aqap-website-disrupted-striking-significant-blow-to-its-online-operations/.
[39] https://www.wired.co.uk/article/isis-telegram-security.
[40] Lakomy, Miron. "Why do online countering violent extremism strategies not work? The case of digital jihad." Terrorism and political violence 35.6 (2023): 1261-1298.

6. When narratives combine

The easy accessibility of content on the largest platforms should cast doubt on the Western metanarrative about success against Salafi-Jihadi online. However, occasionally content sharing on platforms such as WhatsApp also casts doubt on other elements of the Western metanarrative.

For example, Friday 21st July 2023, a WhatsApp group shared the video and pdf released with URL to the AQAP / al-Malahem website.

The screenshot of the release should provide the impetus for much needed reflection on important elements of the current success metanarrative.

First this is the same domain as Tech Against Terrorism had previously claimed credit for removing, saying it was the fifth iteration of al-Qaeda in the Arabian Peninsula's website to go down through their "engagement with infrastructure providers".[41]

A month after the claimed disruption of that .net domain, it was still very much operational, and content was being pushed across multiple social media and digital channels.

The confusion that led a simple connection problem between an AQAP website and the Cloudflare service, to be valorised as a successful disruption effort, is a relatively basic mistake. However, it appears to be a genuine error which in the scheme of things is of relatively little consequence. Afterall,

[41] The now edited post is available on Linkedin: https://www.linkedin.com/feed/update/urn:li:activity:7071432186989588480/.

losing a URL at the rate of less than one per month is hardly going to break the media mujahidin.

Indeed, the outage caused by the previous 'successful' disruption effort of the same AQAP website lasted less time than it took to send out the email announcing the 'significant blow' against AQAP.[42]

The problem is less the specific claims and more the metanarrative to which it contributes. Elements of the largely Transatlantic orthodoxy of Terrorism Studies and CVE industry, often those working with large tech or social media companies, which have consistently claimed Salafi-Jihadi networks are being driven to increasingly niche and small platforms and their distribution capacity is being degraded.

At the same time, larger tech companies such as Meta are keen to point to the efforts made on other platforms, and the support given to smaller platforms through initiatives such as GIFCT and Tech Against Terrorism, and tools like Llama 2 which Meta made available intending it to support safer online interactions.[43]

Indeed, there are also many complexities to be considered about what might be done about content in encrypted group chats, whether on WhatsApp, Telegram or elsewhere. However, the current efforts and complexity of considerations involved should not obscure the contemporary reality that WhatsApp groups are used to distribute Salafi-Jihadi material. Facing Swarmcast 2.0 requires clarity of thought, based on clear identification of the current way Salafi-Jihadi groups exploit web services.

7. A more strategic approach

This article has challenged the orthodox claims that Salafi-Jihadi are forced to use smaller platforms because of the success of 'deplatforming' strategies adopted by so-called internet giants. It has further provided evidence that there is a significant presence of Salafi-Jihadi networks on WhatsApp.

Despite the best efforts of some commentators to talk up a success metanarrative about what has effectively been a decade long game of whack-a-mole, the current approach has consistently failed to make a significant dent in the ability of the Salafi-Jihadi movement to maintain a persistent presence, in either Swarmcast or Swarmcast 2.0 eras. As a result, "these groups

[42] https://www.itstime.it/w/towards-a-more-progressive-approach-to-studying-the-salafi-jihadi-movement-by-ali-fisher/.

[43] https://ai.meta.com/research/publications/llama-2-open-foundation-and-fine-tuned-chat-models/.

have been able to establish a solid foothold on the surface web", according to Miron Lakomy.[44]

Evidence that the world's favourite social platform, with 2 billion users, is being exploited by IS, AQ, and the Taliban should undermine confidence in the claims commonly accepted in the transatlantic orthodoxy of terrorism studies and some parts of the CVE industry that Salafi-Jihadi groups have been pushed from so called tech giants onto smaller platforms.[45]

Facing Swarmcast 2.0 requires clarity of thought, based on clear identification of the current way Salafi-Jihadi groups exploit web services. Media Mujahidin have achieved a persistent presence despite the ongoing efforts to disrupt their communication, due to the speed, agility and resilience of their networks coupled with the willingness to embrace emergent behaviours and web3 technology. In addition to the sanctioned activity of the media mujahidin, here is also growing evidence that supporters operate 'shadow networks' operate across numerous mainstream platforms.

Instead, of playing whack-a-mole and developing tools which are well within the comfort zone of tech platforms, a strategic approach would focus on the elements of the Salafi-Jihadi information ecosystem which make them difficult to disrupt, specifically developing approaches that target the strengths of the media mujahidin and the Salafi-Jihadi movement.

These may include;

- Judging success less by what western-centric commentators are able to locate and focus on the ability of the Arabic speaking primary target audience to access material.
- Targeting the key nodes within a dynamic multiplatform information ecosystem rather than static lists.
- A Web3 strategy – The Salafi-Jihadi movement already has adopted Web3, but disruption efforts lag far behind.
- Committing to lengthy periods of action – The Salafi-Jihadi movement are more than prepared for 'days of action', wearing them down will take weeks of sustained action forcing them to burn through manifold social media accounts, domains, phone numbers and email addresses.
- A paradigm shift to sustained multiplatform action – The Salafi-Jihadi movement are more than prepared for action against their presence on a single platform. Their Multiplatform Communication Paradigm provides resilience against efforts on any individual platform, as Salafi-Jihadi supporters like average social media users, have accounts

[44] Lakomy, Miron. "Why do online countering violent extremism strategies not work? The case of digital jihad." *Terrorism and political violence* 35.6 (2023): 1261-1298.

[45] https://www.techuk.org/resource/natsec2023-faculty-16jan23.html.

on multiple platforms. Losing accounts on one platform only requires reconnecting via links shared on a second or third platform.

In 1999, Darcy DiNucci predicted, "the relationship of Web 1.0 to the Web of tomorrow is roughly the equivalence of Pong to The Matrix".[46] As technology continues to develop, the modus operandi of the Media Mujahidin evolves with it. A Web3-enabled Swarmcast2.0 has arrived. Swarmcast2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than the original version which emerged by 2014. The understanding of the challenge posed by the Media Mujahidin must likewise evolve if we are to avoid trying to play Pong in The Matrix.

References

https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf
https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-103-Favourite-Social-Media-Platforms.png
https://techpp.com/2023/09/28/whatsapp-channels-guide/
https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf
https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf
"Al-Manhajiyya fi tahsil al-khibra al-i'lamiyya, Mu'assasat al-Furqan & Markaz al-Yaqin, part 1," Markaz al-Yaqin and al-Furqan, May 2011
Prem Mahadevan, "The Glocalisation of al-Qaedaism," Center for Security Studies, March 22, 2013
Ali Fisher and Nico Prucha, "Jihadi Twitter Activism – Introduction," Jihadica.com, April 27, 2013
Cori E. Dauber, "YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer," U.S. Army War College, 2009
Rüdiger Lohlker, "Tumbling Along the Straight Path – Jihadis on tumblr.com," University of Vienna, August 2012
Carvalho, Claudia. "'Kids in the Green Lands of the Khilafat'—A Tumblr Case Study of Imagery within the Jihad 3.0 Narrative." *European Muslims and New Media* 5 (2017)
Nico Prucha, "Jihadi Twitter Activism – Introduction"; Nico Prucha, "Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors," Orient 4 (2011)
Ali Fisher, Netwar in Cyberia: decoding the media mujahidin, paper 5, USC Center on Public Diplomacy, 2018
Frampton, Martyn, Ali Fisher, Nico Prucha, and David H. Petraeus. The New Netwar: Countering extremism online. Policy Exchange, 2017
Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021 Sicurezza, Terrorismo e Società 15 (1), 141-170 https://www.

[46] http://darcyd.com/fragmented_future.pdf.

sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movementon-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf

Fisher, A., et al. "Mapping the jihadist information ecosystem: Towards the 3rd generation of disruption capability." *Policy Brief, Royal United Services Institute, London* (2019).

Ali Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence", Perspectives on Terrorism, Vol 9, No 3 (2015)

https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf

https://blog.hootsuite.com/wp-content/uploads/2022/01/Digital-2022-Slide-87-Overview-of-Social-Media-Use.png

https://www.canberratimes.com.au/story/7515010/isis-app-ignored-by-governments-inquiry/

https://twitter.com/charliewinter/status/1072501785716318209

https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf

Ali Fisher Nico Prucha "Working and Waiting": The Salafi-Jihadi movement on Telegram in 2021 Sicurezza, Terrorismo e Società 15 (1), 141-170 https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movementon-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf

Conway, Maura, et al. "Disrupting Daesh: Measuring takedown of online terrorist material and its impacts." *Islamic State's Online Activity and Responses*. Routledge, 2020. 141-160.

https://www.sicurezzaterrorismosocieta.it/wp-content/uploads/2022/05/SicTerSoc-15-2022-Working-and-Waiting-_-The-Salafi-Jihadi-movement-on-Telegram-in-2021-Ali-Fisher-Nico-Prucha.pdf

https://www.itstime.it/w/towards-a-more-progressive-approach-to-studying-the-salafi-jihadi-movement-by-ali-fisher/

https://www.statista.com/topics/2018/whatsapp/#topicOverview

https://blog.whatsapp.com/introducing-whatsapp-channels-a-private-way-to-follow-what-matters

Fisher, Ali, Nico Prucha, and Emily Winterbotham. "Mapping the Jihadist Information Ecosystem." *Global Research Network on Terrorism and Technology* 6 (2019).

https://static.rusi.org/20190716_grntt_paper_06.pdf

https://blog.whatsapp.com/communities-now-available

https://uscpublicdiplomacy.org/blog/interpreting-data-about-isis-online

https://twitter.com/intelwire/status/513303666368196608

Frampton, Martin, Ali Fisher, and Nico Prucha. "The New Netwar." *Policy Exchange: Westminster, London* (2017).

Lakomy, Miron. "Why do online countering violent extremism strategies not work? The case of digital jihad." *Terrorism and political violence* 35.6 (2023): 1261-1298.

https://www.techagainstterrorism.org/2022/12/21/major-al-qaeda-in-arabian-peninsula-aqap-website-disrupted-striking-significant-blow-to-its-online-operations/

https://www.itstime.it/w/towards-a-more-progressive-approach-to-studying-the-salafi-jihadi-movement-by-ali-fisher/
https://ai.meta.com/research/publications/llama-2-open-foundation-and-fine-tuned-chat-models/
https://www.techuk.org/resource/natsec2023-faculty-16jan23.html
http://darcyd.com/fragmented_future.pdf

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 979-12-5535-198-6