THE USE OF ARTIFICIAL INTELLIGENCE WITHIN THE SALAFI-JIHADI ECOSYSTEM ON ROCKET.CHAT: THE UNFOLDING OF A NEW FRONTIER FOR PROPAGANDA?

DOI: https://doi.org/ 10.37458/nstf.25.2.7
Review paper
Received: November 4, 2024
Accepted: November 21, 2024

Alessandro Bolpagni*

Abstract: During the last decades, Salafi-Jihadi groups have exploited the proliferation of social media to create a persistent and ideologically cohesive presence online. Yet, Salafi-Jihadi

* Alessandro Bolpagni is a research analyst at the Italian Team for Security, Terroristic Issues, and Managing Emergencies – ITSTIME. He has a BA in Foreign Languages and International Relations from the Università Cattolica del Sacro Cuore (UCSC), an MA in European and International Policies earned as well at UCSC, and a Postgraduate Master in Middle Eastern Studies (MIMES) at the Alta Scuola di Economia e Relazioni Internazionali (ASERI). He also specialised in digital HUMINT (Human Intelligence) and OSINT/SOCMINT (Open Source and Social Media Intelligence), oriented particularly on Islamic terrorism and Russian Private Military Companies (PMC). He focused on monitoring terrorist networks and modelling recruitment tactics in the digital environment, particularly on new communication technologies implemented by terrorist organizations. He has produced operational reports and lectures for training and education purposes for companies, research centres, and law enforcement agencies.

individuals connected online to form a new dispersed network of 'media mujahedeen' based on loose affiliations, moving from the 'one-to-many' to a 'peer-to-peer' structure described by Ali Fisher as the Swarmcast Model. The Swarmcast model can be adopted to understand the current media war held by media mujahedeen online. Given this context, experts observed a new centrality of non-institutional media houses, which spread jihadist propaganda and/or produce propaganda content. During the last decade, Telegram was Salafi-Jihadi organizations' main messaging platform for both institutional and non-institutional media houses. However, in late November 2019, the 16th Referral Action Day coordinated by EUROPOL took place and forced Salafi-Jihadi propaganda operators to adopt what was described by Ali Fisher and Nico Prucha as the Multiplatform Communication Paradigm (MCP) to create a more resilient digital network. Among the messaging platforms, there was Rocket.Chat, which became their primary launchpad and digital safe haven. In late March, inside the Islamic State (IS) server on Rocket.Chat, the first massive use of Artificial Intelligence (AI) was individuated, which was aimed at producing what can be described as a news broadcast in Arabic of IS's wilayat operations all over the world made by a pro-IS non-institutional media house. The producer inserted all the main characteristics of news broadcasts created through the support of AI. From that day to now, the user posted ten different propaganda videos employing the same production techniques, albeit with some graphic and content differences. Against the backdrop of the evolution of Salafi-Jihadi communication that occurred in the last decades, this paper seeks to illustrate the use of AI inside IS's server on Rocket.Chat and trace possible countermeasures to prevent using such technologies to produce Salafi-Jihadi propaganda.

Keywords: artificial intelligence, terrorism, Islamic State, Rocket.Chat, propaganda

The Evolution of Salafi-Jihadi Communication in the last decades

Salafi-Jihadi organizations have exploited the proliferation of social media to forge a stable and ideologically cohesive presence online to disseminate propaganda aimed at attracting new fighters, fundraising, and encouraging attacks against 'the far and the near enemy' (Fisher 2015). Specifically, the Syrian Civil War has been a fundamental step in the evolution of digital Salafi-Jihadi communication since it was described as the "most socially mediated" and because it became "a new focal point of jihadi media culture" (Lynch, Freelon, and Aday 2014). As Nico Prucha underlined, on May 6th, 2011, al-Fajr Media argued that the "Internet is a battlefield for jihad, a place for missionary work, a field of confronting the enemies of God. It is upon any individual to consider himself as a media-mujahid" (Prucha 2011).

During the early 2010s, the role of Salafi-Jihadi individuals online, especially those supporting the Islamic State (IS), ascended to another dimension. They connected to form a dispersed network of "media mujahedeen" based on loose affiliations, within which users disseminate propaganda content, constantly reconfiguring and reorganizing in mid-flight like a swarm of bees or a flock of birds (Fisher 2015). This structure embodied the transformation of Salafi-Jihadi communication online from a mass communication model – usually referred to as 'one-to-many' – to a new and dispersed and resilient communication network – commonly referred to as 'peer-to-peer' – described by Ali Fisher as the Swarmcast model (Fisher 2015). The

Swarmcast model can be adopted to understand the current media war held by media mujahedeen online.

The model is based on three main characteristics. The first is resilience, namely the ability to overcome takedowns and bans. Since jihadist groups have moved from broadcasting propaganda from a few official media houses to a dispersed network of media mujahedeen, they needed a solid and long-lasting presence online (Fisher 2015). Secondly, speed, to wit the ability to transfer content inside the whole digital network. In other words, once the initial wave of propaganda content has been removed from one specific social media, media mujahedeen have already downloaded it and are ready to disseminate it faster and on a variety of other digital platforms (Fisher 2015). Finally, agility, meaning to say the ability to move from one digital platform to another and even adopt new technologies for short periods before moving to other digital platforms.

The value of agility in establishing a constant online presence is that data released on several different platforms takes time to be localised (Fisher 2015). Moreover, the communication structure inside the Swarmcast model led to an unclear division between the audience and the content producer, thus once the content is created, it is disseminated by the media mujahedeen rather than by the original producer (Fisher 2015). Given this context, experts observed a new centrality of pro-IS non-institutional media houses, which started to spread IS official propaganda and/or produce pro-IS propaganda content.

During the apex of the self-styled caliphate, Telegram was IS's main messaging platform for both institutional

and non-institutional media houses. However, in late November 2019, the 16th Referral Action Day coordinated by the European Union Agency for Law Enforcement Cooperation (EUROPOL) took place, which was aimed at countering Salafi-Jihadi propaganda material and disrupting the IS propaganda network (EUROPOL 2019). Consequently, IS propaganda operators adopted what was described by Ali Fisher and Nico Prucha as the Multiplatform Communication Paradigm (MCP). Rather than focusing on individual platforms, the adoption of MCP allowed IS, and broadly speaking the Salafi-Jihadi online movement, to develop next-generation approaches to counter online disruption and content removal (Fisher, Prucha, and Winterbotham 2019). Accordingly, IS increased its capacity to create a more resilient network. This was the moment that the Swarmcast model evolved. While the original Swarmcast was enabled largely by the increasing access to mobile technology, Swarmcast 2.0 operates with the emergence of alternative distribution modalities including the growth in Web31 technologies, approaches, and ethos (Fisher and Prucha 2022).

Following the Referral Action Day and the adoption of the MCP, IS has scattered across various platforms, including Rocket.Chat, which became IS's primary launchpad and digital safe haven. Behind that migration towards Rocket.Chat, there are several reasons. The most important is the difficulty of how to reach

[1] Web 3.0, also known as Web3, is the third generation of the World Wide Web. Web 3.0 is meant to be decentralized, open to everyone (with a bottom-up design), and built on top of blockchain technologies and developments in the Semantic Web, which describes the web as a network of meaningfully linked data. Web 3.0 is based on a specific set of principles, technical parameters, and values that distinguish it from earlier iterations of the World Wide Web: Web 2.0 and Web 1.0. Web 3.0 envisions a world without centralized companies, where people are in control of their own data and transactions are transparently recorded on blockchains, or databases searchable by anyone. See https://www.avast.com/c-web-3-0.

Rocket.Chat, the high level of users' personal security, and the absence of a centralised administration, unlike Facebook, Twitter, Instagram, etc. Rocket.Chat thus became IS, and broadly speaking Salafi-Jihadi 'citadel', wherein pro-IS individuals freely disseminate propaganda content and interact (Fisher and Prucha 2022).

The first massive use of AI inside the pro-IS main room on Rocket.Chat

In late March, the first massive use of AI was observed on Rocket.Chat. It was aimed at producing what can be depicted as a video news broadcast in Arabic of IS's wilayat – namely provinces – operations all over the world designed by a pro-IS non-institutional media house. This first video was shared a few days following the Crocus City Hall attack in Moscow on March 22. From that day to the present, the user posted ten different propaganda videos employing the same production techniques, albeit with some graphic and content differences. The first video was entirely focused on the Crocus City Hall attack and it was titled 'Moscow blessed Operation'. Since IS official media houses described the attack as a new beginning, it could be its source of inspiration.

The communication dimension

From the communication point of view, the first feature to emerge was the producer's aim of recalling the style of the Western major television networks. As one can observe from the videos, the producer inserted all the main characteristics of news broadcasts: the opening, the presence of an overlaying text, the place, the official logo, and an anchorman. All of these elements were

created with the support of artificial intelligence and, specifically, three different types of AI were employed: character generation, voice file generation (in this case, a text-to-speech AI was utilised, which, starting from a written text, reads it with pre-selected intonation and language), and lips movement connected to the file audio.

From the second video onwards, two highly interesting new elements emerged. The first one, which was the most significant, was the introduction of a logo that represents the producer's intention of displaying its own spontaneous media house. Specifically, the logo recalls the producer's Rocket.Chat account's name. Additionally, in an interaction with a user of the pro-IS digital ecosystem, after being asked what represents the logo, the producer commented by saying it stands for a spontaneous media house. The second new element refers to the fact that the anchorman wears civilian Arab clothes. This change of clothing could be taken into consideration as a strategy aimed at reducing the distance between the product and the consumers, thereby making the speaker as similar as possible to a TV news presenter. Therefore, it is evident that the producer wanted to create a product to provide a digital press review service. Yet, contrary to the typical modus operandi of pro-IS non-institutional media houses, the videos lack the presence of a digital bay'ah – in other words, a pledge of allegiance – to IS.

The producer intended to share the videos within the primary IS server room on Rocket.Chat represents another important communicative feature. Specifically, the producer reveals his intention to place his product as quickly as possible within the main Rocket.Chat's IS

supporter community, thus seeking bottom-up support from the very beginning. Nevertheless, it should be emphasised that this intention entails the so-called security-efficiency trade-off. On the one hand, the producer places its product within an ecosystem of IS supporters with very high visibility. On the other, it does so within an ecosystem considered extremely secure by the supporters themselves since Rocket.Chat is regarded as a 'fortified digital citadel'. Overall, the user drew inspiration from institutional material and developed a clearly recognisable brand that would resemble an institutional media house as closely as possible.

The content dimension

From a content analysis perspective, while the first video is entirely centred on the Crocus City Hall attack, the others revolve around propaganda material of IS's *wilayat* in the Middle East and Africa. While these videos can be considered a trailblazing product from a technological and propaganda point of view, except for the first one, there is a huge chronological and geographical discrepancy between IS's official propaganda material and what the user wrote in the overlaying text. Some images have been presented as snapshots of recent operations, yet they date back to 2023, 2022, and even 2017. Specifically, in the second video, there are images dated 2017 and 2023, while in the third video 2022 and 2023. For instance, in the second video, the producer poses an image of the Islamic State West Africa Province (ISWAP) with an overlay description of an operation in Nigeria. However, the original image of AMAQ (Callimachi 2016) agency has an overlay description which locates the operation in Mozambique. By delving into the content analysis, it

turned out that this was done on purpose. The user removed the overlay text – which includes some information about the operation, the date, the *wilayah*, and the location – and inserted elements usually used by IS's an-Naba magazine to make the image look authentic.

Concerning the last videos shared by the producer in May, July, and September, initially, the producer re-introduced an anchorman with military clothes, later, in the last two videos, the anchorman was presented with Arab civilian clothes. Moreover, some graphical changes were made. Firstly, the producer inserted a new AI-generated voice. Furthermore, he decided to exclusively use propaganda material from IS official propaganda media houses, namely AMAQ and an-Naba. Assuming it is an utterly new product seeking affirmation and consensus, this change in content can be read as an attempt to endow AI-powered news broadcast videos with more credibility and authenticity.

The pro-IS digital community's reaction

The release of the first videos on Rocket.Chat elicited various positive reactions from the pro-IS digital ecosystem's users. In the beginning, the reactions were highly positive, including encouragement to continue the work, advice regarding some corrections were given, and a suggestion for an English version. Yet, following the sharing of the fifth video, a user started to insistently admonish the producer on several graphic aspects. By quoting some *hadiths* from the Quran, the user hardly reprimanded the producer for creating animated bodies and faces, a practice which is considered *haram* – namely 'forbidden' – by some Islamic Law scholars

(Shayk Muhammad Saalih al-Munajjid 2024). The producer and the user had thus a very interesting exchange of views wherein the latter invited the former to blur the faces of the anchorman. Surprisingly, following its principle of creating a product which was pro-IS 'community friendly', in the following video, the user blurred the face of the anchorman. Thus, once again, it showed the necessity to make the product as acceptable and therefore enjoyable as possible.

What are the advantages of using AI to produce propaganda material? How can we avoid the use of AI for such objectives?

In this section, some assumptions on why this user adopted AI to produce pro-IS propaganda will be addressed. First of all, the producer decided to resort to AI tools to quickly create a product as close as possible to a TV news broadcast. The decision to create a video newscast would surely speed up and facilitate the dissemination of propaganda materials inside the pro-IS digital ecosystem. Moreover, this type of propaganda content, which consists of a 'simple' video, makes it extremely usable by all IS supporters. In addition, a news broadcast can be easily disseminated and is by far more appealing than textual propaganda content. In that way, IS supporters do not need to find *nashir*[2] (Smith 2017) channels that spread IS propaganda, thus they can get a news broadcast in the style of a TV newscast, something that is part of everyday life. Furthermore, the process of creation of the video, once set up, seems to be extremely easy to replicate, leading to the possibility of mass

[2] Nashirs are propaganda channels which simultaneously stream material produced by the Islamic State's central media operation, including its self-styled news agency AMAQ, and are described as being dedicated to distributing official IS news.

propaganda production with a relatively low effort. Finally, it should also be considered that the creation of the videos themselves has the potential to galvanise the users of the pro-IS ecosystem. The application of new technologies to create a cutting-edge product can be considered by some of them as the ability of the group to keep up with technological advancements. Nevertheless, since the use of AI is still shrouded in a halo of perplexity concerning its permissibility in Islam, there are some limitations and/or hesitation by IS supporters. For instance, some Islamic Law scholars consider AI as haram. Notwithstanding that, until now, there have never been admonishments made by IS officials through official media houses about the usage of AI.

Furthermore, some possible countermeasures to limit the creation and diffusion of this type of propaganda material must be delineated. First of all, law enforcement should focus on a precise network disruption strategy to greatly weaken IS network resilience and its multidimensional presence among messaging applications. It is paramount that security agencies and law enforcement adopt strategies with a holistic approach in order to develop a multi-vector intervention attack to strike the whole IS propaganda network. Nonetheless, a 'digital military strategy' is not enough to hardly damage it. The focus of counter-propaganda measures should also be directed to content analysis. First and foremost, AI providers, internal moderators, and access policies should impede the production of terroristic content within AI-providing platforms. To achieve this, it is crucial to study in detail propaganda released by IS and, broadly speaking, by Salafi-Jihadi organisations. The study of propaganda content has enabled us to identify specific recurring elements

(content, visual motifs, logos, and expressions) that can be exploited to train AIs aimed at recognising terrorist patterns and intervening to remove this type of content from digital messaging platforms. Finally, there is a *conditio sine qua non* all these measures cannot be achieved, namely only and only if a synergy of intent and action is established between digital messaging platforms and security and law enforcement agencies. m

Conclusions

To conclude, the further implementation of AI by pro-IS non-institutional media houses could give a huge boost to IS propaganda diffusion by streamlining the chain of transmission. Given the bottleneck structure of the IS propaganda machine, the employment of AI will speed up propaganda diffusion and will reduce the distance between the original producer and the audience. Moreover, it will also accelerate the work of translation made by non-institutional media houses, thus greatly extending the range of IS propaganda's reach in the world. Structure according to the Swarmcast model, media mujahideen could highly benefit from the use of AI, further incrementing their capacities of producing and diffusing IS official material. Consequently, it will be fundamental that security agencies and law enforcement will develop a precise disruptive network strategy as well as detection tools to avoid the further diffusion of propaganda through AI technologies.

Notes:

1. Web 3.0, also known as Web3, is the third generation of the World Wide Web. Web 3.0 is meant to be decentralized, open to everyone (with a bottom-up design), and built on top of blockchain technologies and developments in the Semantic

Web, which describes the web as a network of meaningfully linked data. Web 3.0 is based on a specific set of principles, technical parameters, and values that distinguish it from earlier iterations of the World Wide Web: Web 2.0 and Web 1.0. Web 3.0 envisions a world without centralized companies, where people are in control of their own data and transactions are transparently recorded on blockchains, or databases searchable by anyone. See https://www.avast.com/c-web-3-0.

2. Nashirs are propaganda channels which simultaneously stream material produced by the Islamic State's central media operation, including its self-styled news agency AMAQ, and are described as being dedicated to distributing official IS news.

Literature:

1. Callimachi, Rukmini. 2016. 'A News Agency With Scoops Directly From ISIS, and a Veneer of Objectivity'. The New York Times, 14 January 2016, sec. World. https://www.nytimes.com/2016/01/15/world/middleeast/a-news-agency-with-scoops-directly-from-isis-and-a-veneer-of-objectivity.html.
2. EUROPOL. 2019. 'Referral Action Day against Islamic State Online Terrorist Propaganda'. EUROPOL. 22 November 2019. https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda.
3. Fisher, Ali. 2015. 'Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence'. Perspectives on Terrorism 9 (3). https://www.jstor.org/stable/10.2307/26297378.
4. Fisher, Ali, and Nico Prucha. 2022. 'The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0'. Expert Paper. European Institute for Counter Terrorism and Conflict Prevention. https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf.
5. Fisher, Ali, Nico Prucha, and Emily Winterbotham. 2019. 'Mapping the Jihadist Information Ecosystem Towards

the Next Generation of Disruption Capability'. Paper No. 6. Global Research Network on Terrorism and Technology. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/20190716_grntt_paper_06.pdf.

6. Lynch, Marc, Deen Freelon, and Sean Aday. 2014. 'Syria's Socially Mediated Civil War'. 91. Peaceworks - Blogs and Bullets III.

7. Prucha, Nico. 2011. 'Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors'. ORIENT IV.

8. Shayk Muhammad Saalih al-Munajjid. 2024. 'Is Drawing Faces Prohibited?' Islam Question & Answer (blog). 24 March 2024. https://islamqa.info/en/answers/72915/is-drawing-faces-prohibited.

9. Smith, Laura. 2017. 'Messaging App Telegram Centerpiece of IS Social Media Strategy'. BBC News, 31 May 2017, sec. Technology. https://www.bbc.com/news/technology-39743252.