PT PERSPECTIVES ON TERRORISM

RESEARCH ARTICLE

‘Navigating Beyond the Digital Safe Haven’: Mapping the Course of pro-Islamic State Propaganda on Rocket.Chat through a URL Social Network Analysis

Alessandro Bolpagni* and Ali Fisher

Volume XX, Issue 1
March 2026

ISSN: 2334-3745
DOI: 10.19165/AKBV9789

Abstract: In recent decades, Salafi-Jihadi groups have capitalised on the proliferation of social media to establish a persistent online presence. In that time, their activity has evolved into the so-called Multiplatform Communication Paradigm (MCP), a strategy to establish a presence on multiple online platforms instead of focusing on a single platform. Previous research has examined the digital ecosystem through outlinks from social media platforms such as Twitter and Telegram. On these platforms, Salafi-Jihadis face disruption and account removal. As distribution methods evolve to avoid detection, data collection is often based on availability at a given time. In contrast, this research is the first to present a longitudinal study, spanning almost six years of outline sharing from a Salafi-Jihadi digital safe haven, the IS Rocket.Chat server. Here, IS supporters are free to operate without removal, and thus, the research provides valuable insight into how the ecosystem operates when it is not facing disruption. The research provides an initial overview of the outlink data and demonstrates the continued importance of platforms fulfilling the roles of beacons, aggregators, and content stores within the digital ecosystem. It also emphasises the role of human choices in domain selection, as not all rooms share the same combinations of URL. This suggests a vital new, human-centred avenue for research into terrorist exploitation of the internet.

Keywords: Salafi-jihadi groups, Islamic State, Rocket.Chat, TechHaven, social network analysis

*Corresponding author: Alessandro Bolpagni, Università Cattolica del Sacro Cuore. Email: alessandro.bolpagni@unicatt.it

Introduction

Salafi-Jihadi groups have long understood that their activity revolves around communicating with core supporters in the safe haven controlled by the mujahideen and the contested 'frontier' spaces where they seek to reach a wider audience. Today, within the Multiplatform Communication Paradigm (MCP) adopted by Salafi-Jihadi groups, al-Qaeda (AQ) and the Islamic State (IS) run Rocket.Chat servers, which function as self-hosted digital strongholds intended to be a safe haven for supporters and 'trusted brothers'. While Jihadi safe havens are not as popular a subject of study when compared to the fortunes of groups on the easily accessible digital frontier, the digital strongholds that underpinned the Swarmcast and MCP exhibit a modus operandi that traces back to the core tenets of Salafi-Jihadi online activity.

This research is the first to present a longitudinal study that spans almost six years (December 2018 to October 2024) of outlink sharing from a Salafi-Jihadi digital safe haven, namely the IS Rocket.Chat server TechHaven, within which IS supporters are free to operate without content removal or external moderation. The period chosen coincides with the date (5 December 2018) of the first sharing of a URL within TechHaven and with the date (1 October 2024) at which data collection was terminated. The study thus aims to map out the pro-IS propaganda stream specifically generated by the sharing of URLs inside the pro-IS server TechHaven on Rocket.Chat. Each URL analysed was considered an element of IS propaganda because it either led to a site containing IS propaganda material or to other social media (whether messaging platforms or social networks) where IS propaganda material could be acquired. Moreover, the research provides valuable insight into how the ecosystem operates when it is not facing disruption.

This is distinct from previous studies[1] that have assessed the Salafi-Jihadi ecosystem by analysing outlinks on social media where Salafi-Jihadis face disruption and account removal, such as Telegram, Facebook, Twitter, and YouTube.[2] This means their distribution propaganda methods evolve to avoid detection, and data collection is often based on availability at a given time. Despite its remarkable significance in spreading the Salafi-Jihadi propaganda online, Rocket.Chat has been rarely analysed to understand its role as a propaganda launchpad within the IS online ecosystem and, broadly speaking, the Salafi-Jihadi online information environment. This paper thus shows how and which URLs are shared by a Salafi-Jihadi group, in this case IS, to direct its propaganda stream when it is not seeking to avoid content removal. As such, we can begin to test some of the prior assumptions about URL sharing. For example, are the same domains used consistently when URL sharing occurs in a safe space, and do all channels in a safe space behave in the same way? Are there other explanations for the fluctuation in the use of specific domains, other than Western disruption efforts?

To examine these questions, the paper is divided into the following sections. It will initially discuss the role of the safe haven within Salafi-Jihadi online communication strategies. Afterwards, it will describe the evolution of the IS online ecosystem, which led to the emergence of Rocket.Chat as the IS digital safe haven and the operational utility of such a platform.

Once the communicative strategies and the online environment are outlined, the paper will present the methodology applied for monitoring these strategies and the IS online ecosystem and extracting all the URLs shared within TechHaven in a specific time frame. Data and findings will finally be discussed, representing almost six years of activity within one of the best-known Salafi-Jihadi digital safe havens.

Understanding the Safe Haven

In recent decades, major Salafi-Jihadi groups – AQ and IS – have capitalised on the proliferation of social media to establish a persistent and consistent online presence to conduct a media war in parallel to their military operations, performing *da'wa* (proselytism/missionary work) through sharing propaganda, and recruiting new supporters and operatives. What began with the recognition of the internet as a battlefield for jihad capable of breaking the 'media siege' on AQ has evolved from self-hosted safe spaces on forums to embrace social media and the multiplatform communication paradigm of today.[3] While the technology used for communication has changed over time, certain elements, frequently overlooked by researchers, have remained central elements of strategy. Specifically, the distinction between protected strongholds for mujahideen or core supporters and the contested frontier spaces where Salafi-Jihadi groups could reach wider audiences.

In the late 2000s, Salafi-Jihadi groups were well acquainted with the potential of the internet as a means of promoting jihad and disseminating propaganda material. In 2009, Anwar Al-Awlaki underlined how "The internet has become a great medium for spreading the call of Jihad and following the news of the mujahideen".[4] Following the death of Osama bin Laden in May 2011, in the Arabic manual *Methodology in Acquiring Media Experience*, AQ officially promoted the role of the "media soldier", or "media martyr", and shared guidelines on how to develop "media work" with any "brother stationed on the frontier of the media jihad," whose mission is "to form cells to call for jihad and incite jihad, and to facilitate the means for people to do so by providing them with information, guidance, and programs."[5] Moreover, on May 6th, 2011, in a statement[6] to mark the death of Osama bin Laden, AQ-affiliated 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, dedicating himself, his wealth, and his time for God."[7]

In 2011, Ansar al-Mujahideen created both Twitter and Facebook pages.[8] Early efforts would also be conducted on YouTube and Tumblr.[9] These early steps into social media and distribution of media guides were part of a tipping point towards wider social media engagement.[10] These steps by AQ came at the same time as the increased social media adoption within their primary target audience and the outbreak of the then-Syrian Civil War. This combination of factors created a crucial opportunity for Salafi-Jihadi groups to further evolve their information network and propaganda dissemination strategy. The Syrian conflict thus offered to Salafi-Jihadi groups, in particular the group that would become IS, the potential to expand militarily and territorially, as well as expand the digital frontier of their online ecosystem.[11] This, however, is not a moment where groups abandoned one element in favour of another, but of the evolving relationship between the digital strongholds and contested frontier spaces.

Twitter became the primary tool to disseminate propaganda material, while the content and archives were still stored on 'safe spaces' such as forums and websites.[12] At that time, Twitter was the primary method used by non-violent Syrian activists to expose the atrocities and war crimes committed by the Bashar al-Assad regime. At that time, those who would become known as media mujahideen began to adopt content created by civil society activists into their narrative, exploiting their discontent to promote the Salafi-jihadist perspective and legitimise their presence and actions.[13] Consequently, by focusing on grievances and injustice, Salafi-Jihadi groups exploited the Syrian Civil War to mobilise potential supporters against the al-Assad regime and Western powers involved in the conflict. In the early period of Twitter adoption, authority within these networks was still conferred by connection to specific forums, with links

to longer-form content still directing users to these forums.[14] This followed from earlier practice where forums would rely on distribution through al-Fajr Media to prove the authenticity of the communications shared on their platforms.[15]

Therefore, within the Salafi-Jihadi communications, there was a clear relationship between the safe-haven provided by digital strongholds and the contested media frontier. This was rooted in how Salafi-Jihadi groups understood the use of the internet as a tool to disseminate their theological doctrine to galvanise core supporters, the Mujahid vanguard, and engage in *da'wa* to mobilise a mass movement.[16]

As stated by Ayman al-Zawahiri in 2013 in *General Guidelines for Jihad*, the Salafi-Jihadi groups have to pursue a twofold strategy in what he described as the "propagational field", one of the "two aspects" of jihad alongside the "military."[17] According to al-Zawahiri, on the one hand, Salafi-Jihadi groups have to "educate and cultivate the Mujahid vanguard, which shoulders […] the responsibility of confronting the Crusaders and their proxies."[18] On the other hand, Salafi-Jihadi groups have to "create awareness within the masses, inciting them, and exerting efforts to mobilise them so that they revolt against their rulers and join the side of Islam."[19] This twofold strategy was aimed at shaping a Mujahid vanguard that, according to al-Zawahiri's words, followed the principles of "support, participation, and guidance" to conduct "the revolution of the oppressed against the oppressors," as much in the online dimension as in the physical one.[20] While the mujahideen may receive material on the digital frontier, the continued existence of safe havens in digital strongholds has remained an important part of the strategy, allowing individuals to fall back and regroup when frontier networks are disrupted.

The twofold purpose of propagational activity outlined by Zawahiri emphasised the continued importance of the safe haven provided by digital strongholds. This is where the group could galvanise supporters if other communication channels were disrupted. This has long been an important undercurrent within Salafi-Jihadi media, despite the tendency for research to focus on the contested frontier spaces. For more than a decade, the Salafi-Jihadi movement has been conscious that they would "remain on social media sites as mere guests" and "would always be competing with the owners of the site."[21] Abu Saad al-Amili warned in *Apathy in Jihadist Forums: Causes and Solutions*, that "there must come a day when they will close their doors in our faces."[22] As such, al-Amili argued in 2013 that media mujahideen should "consider these sites to be arenas for spreading our seeds, then we will return to our safe, fortified and original bases, which are these networks [forums] that our brothers created specifically for us, to spread the truth without restrictions, and [where] we practice our duties without restriction, condition or fear of tyrants."[23] In other words, al-Amili was exhorting these earlier media mujahideen not to move permanently to social media platforms with their activity, but to recognise the continued importance of their safe havens that (at that time) were jihadist-administered forums.

Jihadi online activity has expanded from the early experiments with Twitter to the fully fledged Multiplatform Communication Paradigm (MCP).[24] Across the MCP, Salafi-Jihadi groups have forged a stable and doctrinally cohesive presence online to disseminate propaganda aimed at attracting new fighters, fundraising, and encouraging attacks against the far and the near enemy.[25] Since the early 2010s, the activity of media mujahideen – and munasirin, individuals actively engaged in sharing Salafi-Jihadi propaganda online – have been in a state of constant evolution as their multiplatform *zeitgeist* has continued to reconfigure.[26] The ability to reconfigure has relied on a Swarmcast mentality (discussed further below) on the frontier, underpinned by access to the safe haven provided by digital strongholds.[27]

While some of the early jihadist forums have continued to exist online, Rocket.Chat has emerged as the new, self-hosted safe haven of choice for both IS and AQ. As will be discussed later in the paper, Rocket.Chat is a platform that allows Salafi-Jihadi groups to create their own self-managed server, giving them the opportunity to create their own virtual space with forum-like management.

The Evolution of Jihadi Communication Environment

Over more than twenty years, Salafi-Jihadi groups have undertaken a remarkable evolution in their communicative methods and propaganda-sharing strategies in the digital dimension. Moving from the 1990s Web 1.0[28] online forums to use encrypted messaging platforms and decentralised Web 3.0 technology,[29] Salafi-Jihadi groups have developed a remarkable online resilience and a constantly evolving capacity to adapt to new circumstances and technologies.

Among the communication models adopted in the last two decades, one of the most successful in creating a consistent, resilient, and persistent presence online was the creation of a multiplatform propaganda structure always able to adapt itself to disruption attacks, bans, and content removal from law enforcement agencies. Since the early 2010s, Salafi-Jihadi groups started to configure their online presence according to the MCP: rather than focusing on individual platforms, the Salafi-Jihadi online movement has developed next-generation approaches to online disruption and content removal.[30] The MCP has thus created a network of remarkable resilience, far surpassing that which existed during the period when the Salafi-Jihadi online movement was heavily dependent on Twitter (now X) or the initial adoption of Telegram in 2015. Specifically, the adoption of the MCP has produced many levels of redundancy in the network and ensured a persistent presence for the Salafi-Jihadi online movement.[31] Consequently, this approach has made the jihadist network more resilient and has enabled users to reconnect quickly when the network suffers from online disruption attacks. Within the MCP, social media platforms, archive websites, and cloud storage services act respectively as beacons, aggregators, and specific content stores, through which the Salafi-Jihadi online movement can regroup in the event of a break in its activity on a single specific platform.[32] Firstly, beacons provide the 'always on' stream of communication through which information can be rapidly disseminated; content aggregators are sites or social networks that gather a range of jihadist materials and provide users with a collection of links to locations where a specific propaganda material can be downloaded; and content stores are locations where content is uploaded for users to access with a link supplied by content aggregators or beacons.[33]

In the early 2010s, the recognition and approval of the media mujahideen, the decision to engage via social media, and the mediatic exploitation of the increasing violence of the then-active civil war in Syria provided an opportunity for Salafi-Jihadi groups to evolve their online strategies, which became increasingly aligned with the concepts of netwar.[34] Netwar was defined by John Arquilla and David Ronfeldt as an emerging mode of lower-intensity conflicts at societal levels wherein the protagonists consist of dispersed organisations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an 'internetted' manner, often without a precise central command.[35] What distinguishes netwar as a form of conflict is the networked organisational structure of its practitioners – with many groups being leaderless – and the suppleness in their ability to come together quickly in swarming attacks.[36] This emphasis on the strategic use of information, irregularisation, alternate operational structures, the connection between physical battlefield and information-based (or digital) forms of conflict, and the adoption of swarming attacks makes netwar an important conceptual tool for the understanding of jihadist social media described through the concept of the Swarmcast model.[37]

Inspired by swarm behaviour observed in nature, the Swarmcast model is a netwar-inspired concept to demonstrate the persistence of Salafi-Jihadi propaganda material online.[38] It embodied the transformation of Salafi-Jihadi communication online from a mass communication model – usually referred to as 'one-to-many' – to a new, dispersed, and resilient communication network – commonly referred to as 'peer-to-peer'.[39] Furthermore, the communication structure inside the Swarmcast model led to an unclear division between the audience and the content producer; therefore, once the content is created, it is disseminated by the media mujahideen rather than by the original producer.[40] In doing so, media mujahideen connected to form a dispersed network based on loose affiliations, within which users disseminate propaganda content, constantly reconfiguring and reorganising in mid-flight like a swarm of bees or a flock of birds.[41] The Swarmcast model is based on three main features. 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 mujahideen, they needed a solid and long-lasting presence online.[42] The second feature is speed, to wit, the ability to transfer content inside the whole digital network. In other words, even once the initial wave of propaganda content has been removed from one specific social media platform, media mujahideen have already downloaded it and are ready to disseminate it faster and on a variety of other digital platforms.[43] Finally, agility, namely 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.[44]

The Swarmcast model can be applied to describe the Salafi-Jihadi information ecosystem during the era of Web 2.0.[45] In the early 2000s, Web 2.0 was coined as a term to differentiate the post-dotcom World Wide Web (WWW) from that which came before, giving emphasis to social networking, content generated by users, and cloud computing.[46] In Web 2.0, jihadist groups have been able to maintain a persistent online presence by sharing content through a broad network, which has become one of the clearest incarnations of netwar since it was first envisaged.[47] However, the advent of Web 3.0[48] enabled the evolution of the Swarmcast model to Swarmcast model 2.0. The Swarmcast model 2.0 is much more dynamic, secure, encrypted, decentralised, and resilient than the original version.[49] Web 3.0 can be described as a vision of the future of the internet in which people operate on decentralised, quasi-anonymous platforms rather than depending on tech giants like Google, Facebook, and Twitter.[50] Contrary to the centralisation of Web 2.0, Web 3.0 refers to a decentralised online ecosystem based on the blockchain, wherein platforms and apps are not owned by a central gatekeeper but rather by users, who will earn their ownership stake by helping to develop and maintain those services.[51] While the Swarmcast model was enabled largely by the increasing access to mobile technology, the Swarmcast model 2.0 operates with the emergence of alternative distribution modalities, including the growth in Web 3.0 technologies, approaches, and ethos.[52] Therefore, the media mujahideen act according to a multiplatform *zeitgeist* hyper-distributed and massively replicated on multiple servers simultaneously, which combines decentralised network forms on specific platforms with decentralised peer-to-peer networks.

Throughout the period when the Salafi-Jihadi movement has exploited social media, they have also been aware that they were operating in an environment controlled by 'the enemy' and that they would always need a digital safe haven. By recalling al-Amili's words, media mujahideen will always "remain on social media sites as mere guests."[53] Nevertheless, in late 2019, following a series of network disruption interventions led by Europol, Salafi-Jihadi groups managed to find in Rocket.Chat a new digital safe haven to reorganise their online presence and their *da'wa* operations.

From Telegram to Rocket.Chat: the advent of a new digital safe haven

Since 2016, Telegram has been one of the Salafi-Jihadi online movement's core platforms for communication and the dissemination of propaganda material.[54] Between 2015 and 2019, private groups within Telegram also functioned as a form of digital safe haven thanks to encryption, limited disruption efforts, and vetting of users seeking to access particularly well-protected groups. In 2015, the Salafi-Jihadi movement began to move from the heavy emphasis on Twitter, which at the time had a greater user base and presence on mobile devices, to using Telegram for communication within the core of the movement, and Twitter and other social media for outreach.[55] For several years subsequently, Telegram was the core media platform of Salafi-Jihadi online movements. Yet, between 21-22 November 2019, the 16th Referral Action Day coordinated by the European Union Internet Referral Unit (EU IRU) – a team inside the European Union (EU)'s law enforcement agency, Europol – took place at Europol's headquarters in The Hague, which transformed and resized the Salafi-Jihadi's online movement presence. The online propaganda items targeted by Europol included propaganda videos, publications, and social media accounts that supported terrorism and violent extremism. Specifically, an official of the EU IRU reported that the operation was coordinated to conduct a "serious disruption campaign" against IS's online channels and groups, especially directing the efforts towards IS-branded and produced propaganda material.[56] Overall, the initiative led to the flagging or removal of over 26,000 pieces of IS propaganda content, dealing what Europol officials have called a "major blow" to IS's online presence.[57] The 16th Referral Action Day took on a much broader scope than previous ones, with Europol and partner agencies aiming to remove "everything related to Daesh propaganda" across multiple platforms.[58] In particular, Telegram was notably in the spotlight, as many IS and pro-IS channels and chats operated primarily on that platform, since it was their digital safe haven at the time.[59] Alongside Telegram, other tech companies were engaged through the flagging process. According to Europol, partners included Google (for example, YouTube), Twitter, and Facebook services (particularly Instagram), among others.[60] As a result of these concerted efforts, authorities removed a considerable number of key actors associated with IS and, broadly speaking, with the Salafi-Jihadi online movement network from Telegram, briefly disrupting its ability to spread extremist content on the platform. Following the 16th Referral Action Day, Salafi-Jihadi groups have intensified their diversification efforts on various platforms, including Rocket.Chat, which has subsequently functioned as their digital safe haven.

As al-Aza'im Media Foundation outlined to supporters in its magazine Voice of Khorasan (issue 43):

> *Rocket.Chat is an open-source messaging platform often used by organizations for team collaboration. Its privacy policies can differ significantly based on how it is hosted. Organizations that choose to self-host Rocket.Chat have the option to determine their level of logging and data retention, which may include IP addresses and other identifying information. (Voice of Khorasan, Issue 43, p. 47, 2025)*

An earlier guide to the IS Rocket.Chat server, published by pro-IS Qimam Electronic Foundation (QEF) in 2020, promoted TechHaven server as having "All official and supporters' channels of the Islamic State."[61] Moreover, QEF stated that there had been (within TechHaven) "[n]o censorship since December 2018."[62] Apart from a few days for maintenance and a hacking attack, the IS server TechHaven has been online almost continuously since then until the time of writing in August 2025.

The migration towards Rocket.Chat was not a replacement for other platforms, but a necessary diversification to create new digital safe havens, particularly one that was self-administered. By applying the security-efficiency trade-off, it is easy to observe how Salafi-Jihadi groups understood that Rocket.Chat focuses on users' security and anonymisation over its broadcasting capabilities, prioritising security over efficiency. By day-to-day monitoring, authors were able to observe how Rocket.Chat lacks, for instance, Telegram's public broadcast capabilities, a shortcoming visible through TechHaven users' complaints about the functioning of Rocket.Chat. According to C. Morselli, C. Giguère, and K. Petit,[63] a consistent trade-off facing participants in any criminal or terrorist network is that, between organising for efficiency or security, participants collectively pursue an objective while keeping the actions leading to that goal concealed. Which side of the trade-off is prioritised depends on the objective that is pursued by the criminal group or the terrorist organisation. According to C. Morselli *et al.*, on the one hand, since the time-to-task is shorter in money-driven criminal organisations, they therefore prioritise efficiency over security. In other words, criminal organisations focus on efficiency because their actions have a reasonably short time frame and they expect a pay-off for their involvement in the network. On the other hand, since ideologically driven terrorist groups have longer horizons, security is prioritised over the execution of any single attack.[64] Contrary to criminal groups, terrorist organisations pursue common ideological objectives over monetary return, and thus the network objectives influence the incidence of actions by extending the time-to-task.

In the spirit of Web 3.0, Rocket.Chat thus offers users the full capabilities of a mature communication platform without the centralised administration found in Web 2.0 platforms like Telegram, Facebook or Twitter, which often suspend or remove accounts when flagged by users or governments.[65] On Rocket.Chat, the Salafi-Jihadi online movement has thus maintained access through its self-managed installations. Furthermore, the authors observed significant aspects of Rocket.Chat's technical configuration based on the security-efficiency trade-off, specifically impacting its accessibility and attractiveness to the pro-IS ecosystem and, broadly speaking, the Salafi-Jihadi online movement. Firstly, the platform is relatively hard to reach. This is due to several factors, such as the difficulty of finding links to the digital platform, stringent access controls, the need for moderate technical knowledge to join and participate, as well as the limited availability of resources and support for new users. Such barriers reduce the platform's accessibility, making it less appealing for activities intended to reach less invested individuals or mobilise the mass movement. Yet, this could be considered a deliberate tactic by the administrators of the TechHaven server and, broadly speaking, the Salafi-Jihadi movement. They have adopted a high level of security, thus raising their resilience in an environment where they can communicate with existing supporters, namely the Mujahid vanguard.

Secondly, Rocket.Chat was found to have relatively low-level user-friendliness compared to some other platforms. This means that inexperienced users, especially those who may not be technologically savvy, might find it more difficult to navigate the platform, understand its features, or utilise it effectively for communication, content sharing, and coordination purposes. Moreover, since the server is intended to be a 'walled garden' for members, it is hard to broadcast content via links onto other platforms. Overall, Rocket.Chat has thus become one of the main platforms among MCP's beacons and one of the main pillars of the Swarmcast model 2.0, given its role and centrality as the digital safe haven for IS, and broadly speaking, for the Salafi-Jihadi propaganda machine. Within the broad Salafi-Jihadi movement online ecosystem, it is therefore a place primarily for the Mujahid vanguard, with other platforms, such as Telegram, fulfilling the role of outreach.

As a result, since late 2018, the Mujahid vanguard has used Rocket.Chat not only as a safe space for sharing propaganda material but also as the primary launchpad for campaigns to target other digital platforms. These platforms, including Telegram, other messaging applications, and various websites, have become the prime targets of botnets and online recruitment campaigns, highlighting the significant role of Rocket.Chat in the broader digital strategy of the Salafi-Jihadi online movement. For these reasons, Rocket.Chat has turned into the Salafi-Jihadi movement's digital safe haven or 'fortified citadel' thanks to its security features and independence provided by hosting their own self-managed server.

Methodology – Mining Rocket.Chat

The study was developed through the application of intelligence techniques elaborated by the Italian Team for Security, Terroristic Issues & Managing Emergencies (ITSTIME) and data collection tools developed by Human Cognition. Specifically, the authors employed Digital Human Intelligence (Digital HUMINT) methodologies to monitor day by day the active members within the pro-IS server TechHaven. Despite not being directly addressed in this research, the principles at the basis of the Digital HUMINT will be described in this section because they represent fundamental intelligence techniques that allowed the acquisition of the pro-IS server TechHaven in 2018 and were crucial in observing the evolution of the interaction within the servers in the last seven years.

To gather comprehensive insights, the research employed a covert non-participant observation method through the application of Digital Human Intelligence (Digital HUMINT) techniques. Designed by the Italian Team for Security, Terroristic Issues & Managing Emergencies (ITSTIME), the Digital HUMINT is an intelligence method that combines the Human Intelligence (HUMINT) practice and the new-type approach related to the new social media sources.[66] It encompasses a series of socio-anthropological approaches and mimesis tactics to observe and, if necessary, interact within extremist online ecosystems. Digital HUMINT is primarily based on digital ethnography, namely the application of socio-anthropological models to the online dimension. The latter can be described as a contemporary form of ethnography that considers online social environments following the developments in data transmission technology.[67] The ethnological approach appears to be polyvalent, since it encompasses both the socio-anthropological study and the data collection instrument.[68] In the first case, the socio-anthropological study responds to the necessity of observing the digital environment to grasp and understand all the social and relational dynamics happening in the virtual communities.[69] Complementarily, the data collection focuses on the exchange of content and information within a virtual environment.[70] In other words, the second approach represents the 'participative observation' which configures itself as an effective tool for the recollection of data and information useful for future analyses.[71] Overall, these intelligence techniques allowed the researchers to observe the platform's functionalities and user interactions without influencing the behaviour of the pro-IS TechHaven community.

The research thus seeks to delve into how the pro-IS ecosystem has developed on Rocket.Chat and how users are directed to resources outside the digital safe haven, such as other messaging platforms and archive websites. To accomplish this objective, the authors employed covert non-participant observation approaches through the application of Digital HUMINT techniques and digital ethnography to develop deeper insights into the structure of the MCP from Rocket.Chat outwards.[72] The study identified the URLs shared in each channel/group on Rocket.Chat. To accomplish this, the study used a Python script written by Human Cognition to download data from the self-hosted pro-IS server TechHaven on Rocket.Chat. The data scraper extracted every

post from each room available as of 1 October 2024, and extracted any URL present in the post text. URLs from each room are hosted on the Rocket.Chat server TechHaven by systematically sorting the URLs into various categories based on the distinct purposes each link serves.

Following the data collection and classification phase, the authors employed Social Network Analysis (SNA) to systematically map and interpret the relationships between URLs shared inside the pro-IS TechHaven server. SNA is a research perspective used within Terrorism Studies that enables researchers to visualise and analyse the social structural patterns within networks by examining nodes (in this case, URLs) and the connections (edges) between them.[73] From a methodological point of view, through the creation of graphs based on statistical and mathematical calculations, it can measure and analyse features of nodes as well as of their connections.[74]

By applying SNA to the collected data, the authors aim to uncover the underlying network structure formed by these URLs within the pro-IS server TechHaven on Rocket.Chat. This involves identifying central nodes, clusters, and key linkages that facilitate and show the direction of the stream of information. Specifically, the analysis seeks to highlight the significance of specific URLs in terms of their connectivity and influence within the network. Central URLs, which serve as major hubs, can play a crucial role in disseminating content and maintaining the cohesion of the network. The goal of this comprehensive analytical approach is to gain a deeper understanding of how the pro-IS propaganda ecosystem moves outside Rocket.Chat's digital safe haven. By mapping the network of shared URLs, the research intends to reveal the extent to which Rocket.Chat acts as a pivotal digital platform in the broader information ecosystem of pro-IS online content dissemination. This includes assessing how and whether URLs have changed over time and towards where they have been directed, thus outlining the behaviour of the pro-IS online movement.

The findings from the SNA will contribute to the academic discourse on digital extremism by providing empirical evidence on the functionality and significance of Rocket.Chat within the pro-IS digital landscape.

SNA of the URLs stream inside the pro-IS server TechHaven on Rocket.Chat

On Rocket.Chat, the pro-IS digital ecosystem has its own server titled TechHaven. The server consists of rooms which, depending on the settings chosen by the room administrator or administrators, can take the form of a channel (where only certain users can share messages and material) or a chat (where anyone can share messages and material). Specifically, the TechHaven server has a main 'general room discussion' and rooms which focus on news, institutional propaganda, Ansar Production media houses, content arranged by specific themes or geography, and technological issues.[75] While the server has not had a continuously active room for IS's branded media or consistent news channels (akin to the *nashir* channels active on other platforms), the many Ansar Production media houses have their own rooms. The most active are the 'general discussion' room and those dealing with content translated into languages relevant to specific regions (namely IS's *wilayat* locations), with Arabic and English being most common over the almost six-year period. On the date when the data collection process was completed (1 October 2024), there were a total of 430 rooms on the TechHaven server. Yet, analysis showed that messages containing URLs were shared in 290 rooms by 678 users. For security reasons and in order to avoid indirectly disseminating IS or pro-IS propaganda content, the full names of the rooms have been anonymised in all images included in the paper, as well

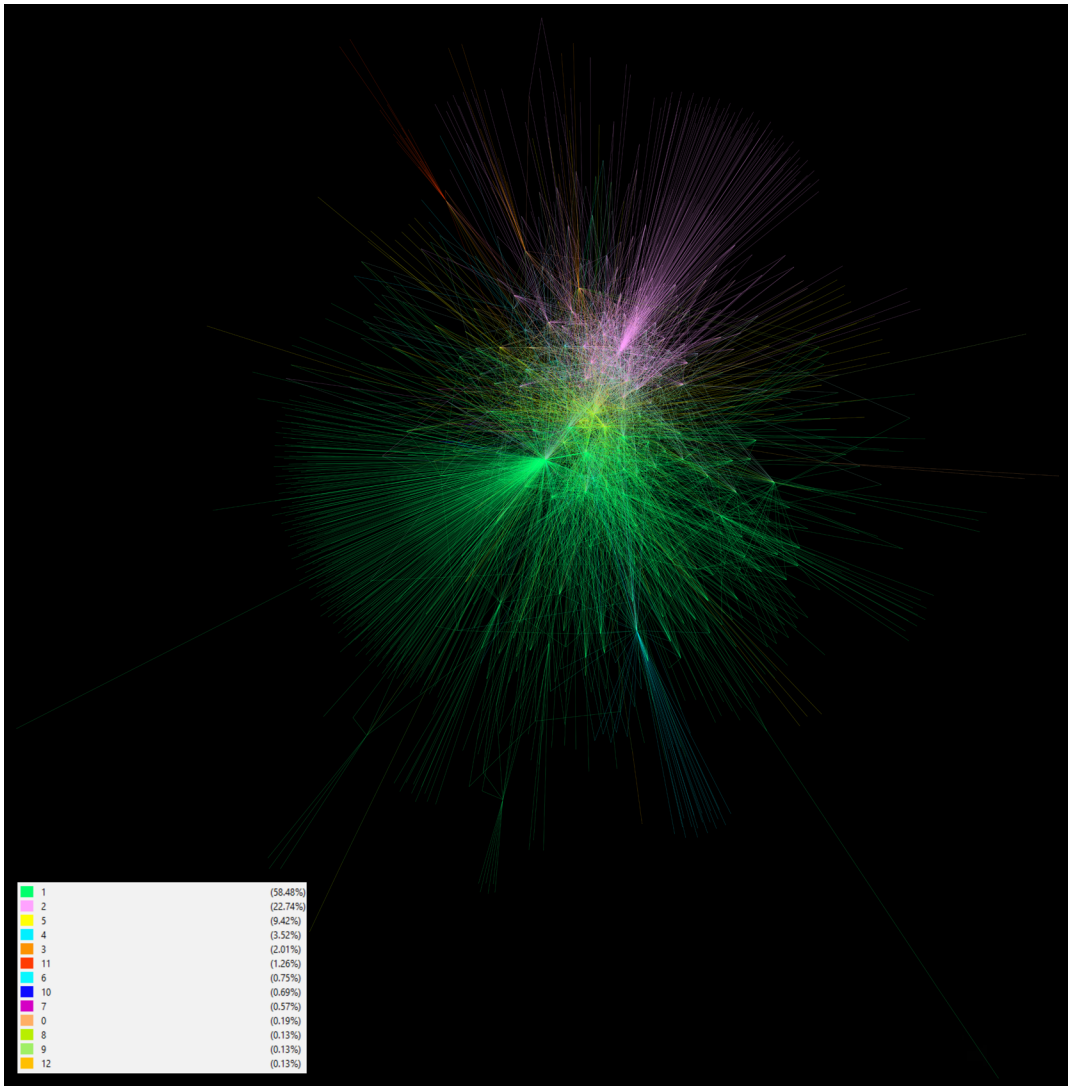
as the URLs, which have been modified from their original form, usually with abbreviations that do not refer back to the reference site.

The following section will present the SNA that examines the stream of propaganda inside the TechHaven server and outlinks to other platforms. Specifically, the SNA aims to map out all the URLs shared (just under ninety thousand) in the message text of the aforementioned 290 rooms of the TechHaven server from 5 December 2018, to 1 October 2024. As mentioned above, the start date of the data collection (5 December 2018) is the day on which the first URL was shared on TechHaven, while the end date of the data collection is the date on which the authors chose to conclude the process. The SNA presents a visual representation of the connections between the domain name (modified) of each URL and the rooms in which they were shared on the TechHaven server. The total number of nodes in the network is 1,592, which are made up of 290 rooms - namely, channels and chats - and 1,302 unique domains and subdomains, which have been shared a total of 89,991 times within TechHaven. Furthermore, 678 users were active in sharing all the URLs through message texts. The representation of the network was developed using the ForceAtlas2 algorithm implemented in Gephi. Specifically, ForceAtlas2 is a force-directed layout: it simulates a physical system to spatialise a network, wherein nodes repulse each other like charged particles while edges attract their nodes like springs, creating a movement that converges to a balanced state.[76]

At the whole network level, it is significant to analyse the density of the network. This metric indicates the overall level of connectivity between the nodes among all its constituent nodes. Moreover, it is obtained by dividing the sum of existing connections by the maximum number of possible connections, namely the ratio of the sum of connections to the maximum possible number of connections. The value obtained ranges from 0 to 1, where 0 represents the absence of connections, and 1 indicates that all possible connections are present within the network. In the SNA shown in Figure 1, the density is 0.002, which indicates a low density of interconnectivity. This means that the rooms on the server do not all share URLs to the same platforms, if they had the density would be much higher. As underlined before, the pro-IS digital ecosystem on Rocket.Chat prioritises security over efficiency by minimising connections and being multi-lingual, not all URLs are relevant to all users. In addition, the almost six-year time period may influence the availability of some services and preferences for specific services amongst the Media Mujahideen and could account for some variation in platform selection.

In subgroup-level analysis, the modularity class identifies the communities or clusters which exist within the network as a whole. In this analysis, thirteen communities were identified, and the modularity score was 0.418 (Figure 1).

Figure 1



Higher modularity scores indicate that the network has clearly distinct clusters. In the case under analysis, the modularity metric does not suggest that the network has a well-defined and distinct community structure,[77] but does show that clusters of rooms sharing URLs on Techhaven tend to have some similar URL sharing patterns. Employing the modularity score shows the size of the groups that adopt similar URL-sharing patterns. The distribution of these communities is shown below in Table 1.

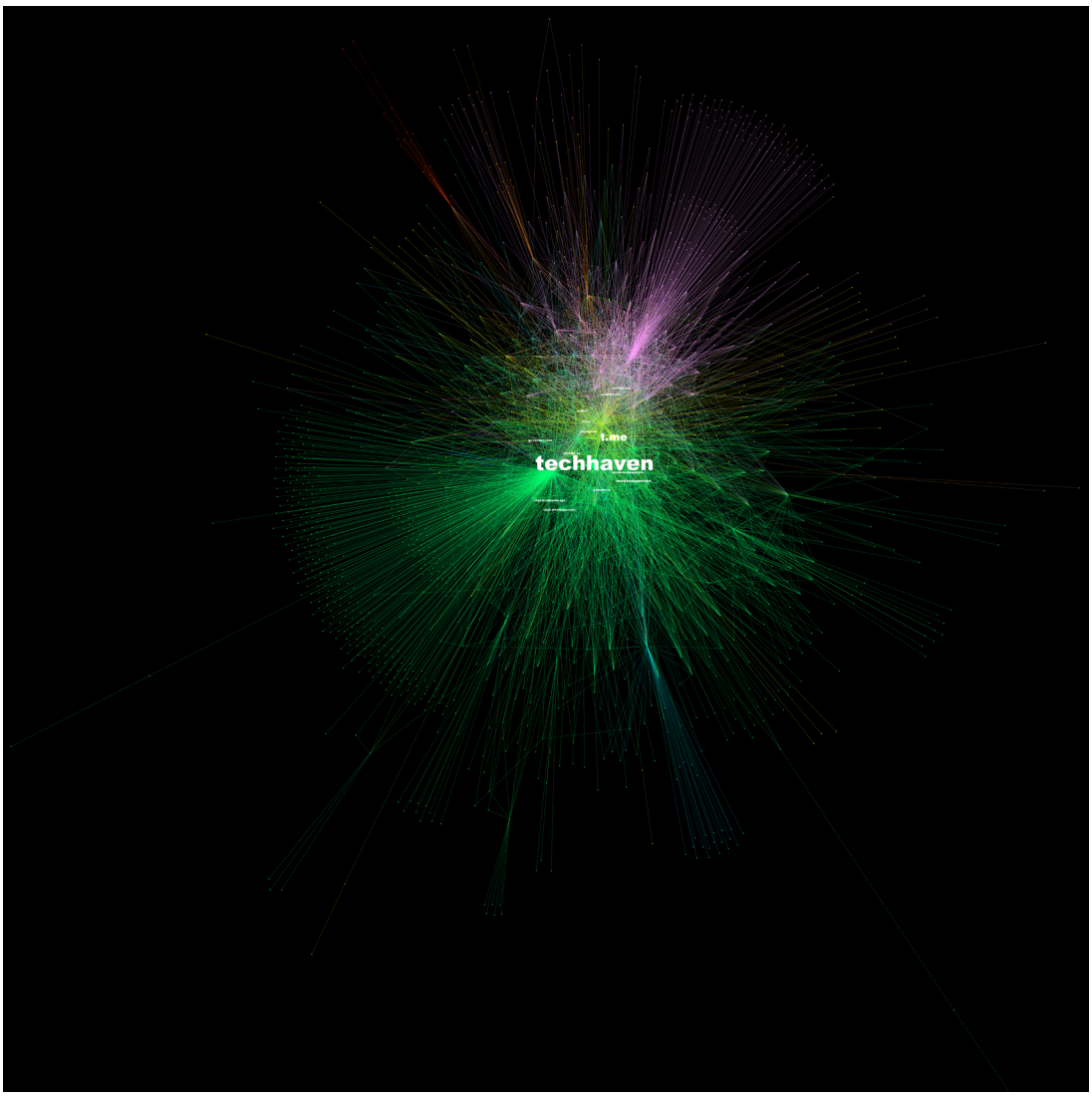
Table 1: Modularity Class

Community number	**Share of nodes**
1	58.48%
2	22.74%
5	9.42%
4	3.52%
3	2.01%
11	1.26%
6	0.75%
10	0.69%
7,0,8,9,12	< 0.60%

Community 1 shares 58.48 percent of the nodes in the network, meaning that more than half of all the nodes in the network are in Community 1. Different communities can be identified in Figure 1 by looking at the legend in the bottom-left corner. For ease of interpretation, the Community number column in Table 1 provides a reference system to identify the position of each community within the network depicted in the SNA in Figure 1, using the colour legend supplied.

At the node level, PageRank is considered (Figure 2). PageRank is a variation of eigenvector-based centrality that measures the influence of a node in a network. PageRank refers to the probability distribution for nodes in a network. In other words, it is a measure of how likely a user is to reach a specific node from other nodes in a network.[78] It is adopted in directed networks because it uses the in-degree – incoming relations – as a metric to estimate the level of influence.

Figure 2



The four domains with the highest PageRank (Table 2) are techhaven (0.033189), t.me (0.016735), matrix.to (0.003609), and obidientsupporters (0.003271).

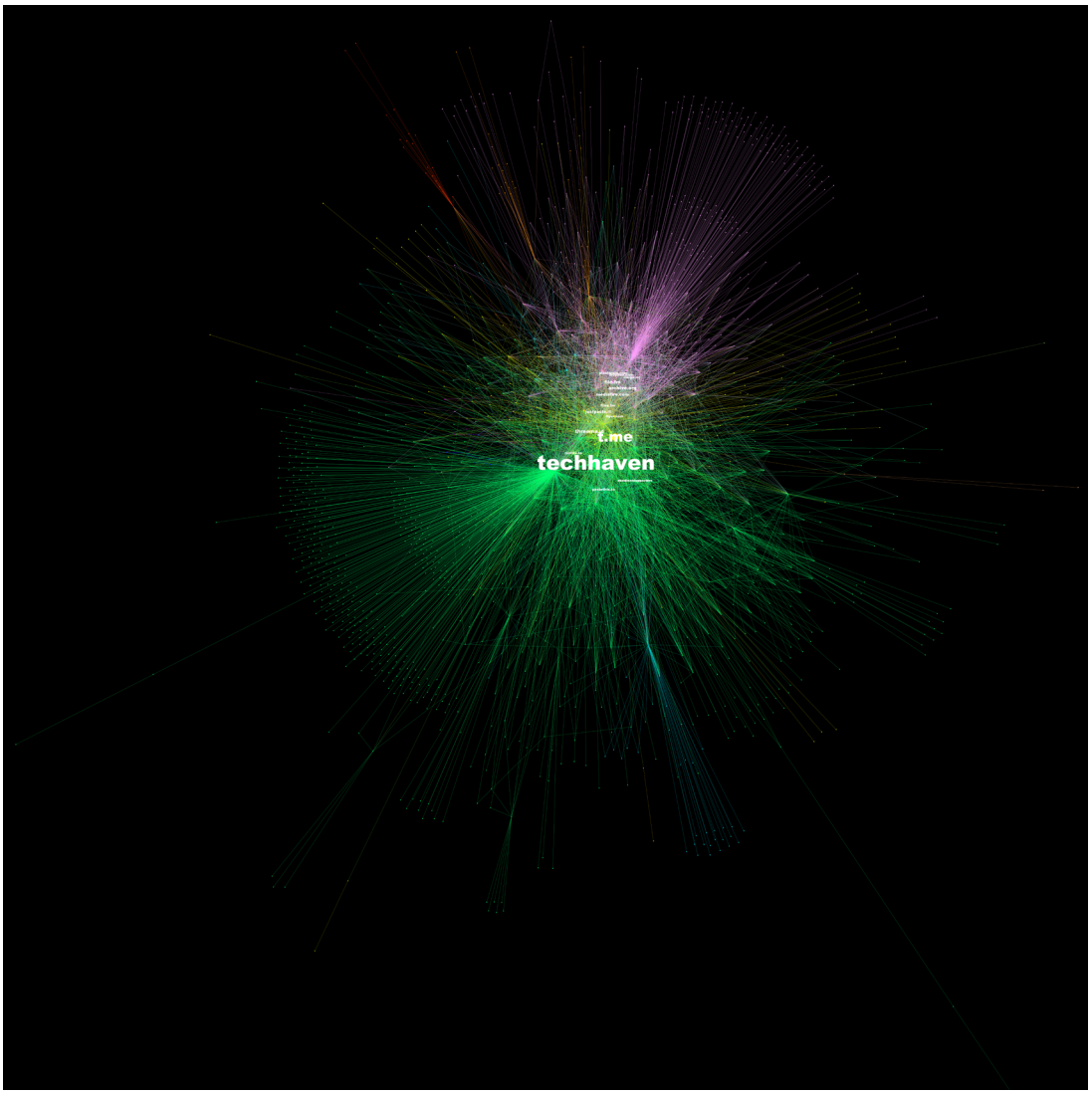
Table 2: PageRank

Domains	PageRank
techhaven	0.033189
t.me	0.016735
matrix.to	0.003609
obidientsupporters	0.003271
archive.org	0.002899
chat.whatsapp.com	0.002825
hoop.page.link	0.002775
obedientsupporters.	0.002746
go.rocket.chat	0.002695
techhaven.xyz	0.002138
file.io	0.002350
pastethis.to	0.002181
threema.id	0.002138
mediafire.com	0.002109
gofile.io	0.001956

These results reflect the structure of the Swarmcast model 2.0. Within it, Rocket.Chat, Telegram, and Matrix are the main pillars, as well as beacons, which supply users with links to direct them to domains where propaganda content is uploaded, namely content stores, such as Obedient Supporters.[79] Moreover, it is noteworthy to underline that, by following the analysis of the PageRank classification, there are several other URLs for archive websites, file-sharing websites, cloud store websites, and messaging platforms.

Moreover, at the node level, centrality metrics investigate the role of each node within a network and attempt to determine whether a node is important in the network. For the present research, degree centrality and betweenness centrality have been considered. Degree centrality is the number of nodes adjacent to a given node and represents the number of direct contacts each node has.[80] Yet, it is important to underscore that a high degree centrality score does not necessarily imply leadership status but rather indicates that the node under consideration has a large number of direct connections with other nodes. By going deeper into analysing degree centrality, it is more relevant to examine the in-degree centrality because the research is intended to identify which URLs are shared most frequently in the rooms of the TechHaven server. To do so, the weighted in-degree was examined, which represents the number of incoming relations of each node (Figure 3).

Figure 3



By looking at the weighted in-degree, the most-shared URLs inside the server TechHaven have been highlighted. Moreover, it can be observed that certain URLs were shared more in rooms belonging to specific modularity classes. For example, the URL techahven was shared more by rooms in modularity class number 2, t.me in modularity class 3 and several archive or cloud store sites in modularity class 1. Consequently, it can be asserted that the URLs of the so-called beacons belong to modularity class 2 and 3 and the content stores to modularity class 1. The URLs (Table 3) with values over 1,500 are techhaven (18,745), t.me (12,798), and threema.id (3,157), followed by several archive websites, file-sharing websites, cloud store websites, and messaging platforms.

Table 3: Weighted in-degree

Domains	Weighted in-degree
techhaven	18,745
t.me	12,798
threema.id	3,157
file.fm	3,022
archive.org	2,867
mediafire.com	2,544
justpaste.it	2,410
mega.nz	1,965
files.fm	1,897
pixeldrain.com	1,855
dropbox.com	1,810
matrix.to	1,778
pastethis.to	1,746
tlgur.com	1,674
obedientsupporters	1,615

Conclusions

The analysis of the SNA of the URLs shared inside the pro-IS server TechHaven has confirmed the centrality of Rocket.Chat and Telegram within the broader IS digital ecosystem. This approach, which maps and quantifies the stream of information within the IS propaganda network, has demonstrated that Rocket.Chat functions as a primary launchpad of the IS propaganda infrastructure online. In addition to providing a safe haven within which users can interact, it serves as a hub directing users to a multitude of pro-IS channels on other platforms, content repositories, and websites that function as aggregators of content, thereby facilitating the group's ability to maintain a resilient and adaptive digital presence.

By examining the URLs shared between December 2018 and October 2024, a clear pattern emerges: the IS online ecosystem has strategically developed and structured the so-called MCP. This model ensures a continuous and persistent presence online by leveraging two key mechanisms. Beacons function as central nodes that provide an always-on stream of information, thus guiding users towards a broader network of pro-IS channels across different platforms. In this case, when considering the stream of propaganda flowing centripetally and centrifugally within IS's digital safe haven, Rocket.Chat (namely the TechHaven server) and Telegram are the main beacons of IS's entire online ecosystem. Alongside content aggregators, they serve as digital waypoints, enabling IS supporters and operatives to navigate an otherwise fragmented online landscape. Content stores serve as digital archives where IS propaganda materials, including videos, magazines, and operational guides, are stored and systematically distributed. The duplication of these repositories ensures that propaganda material remains accessible despite frequent attempts to take down content by law enforcement and tech companies.

The application of SNA techniques in this context enables researchers and analysts to pinpoint the most influential messaging platforms and storage repositories utilised by IS operatives.

The findings highlight how Rocket.Chat and Telegram consistently serve as the main platforms for propaganda content dissemination. Rocket.Chat functions as the primary launchpad, orchestrating the distribution of IS-related material. It plays a pivotal role in directing users to various content repositories and messaging platforms, ensuring that IS propaganda remains accessible even as individual accounts and channels are banned. Alongside Rocket.Chat, Telegram remains the most employed platform for real-time communication and content sharing among IS supporters. Despite ongoing interventions to remove IS content and related users, which between August 2024 and June 2025 increased by around 240 percent,[81] Telegram remains a fundamental communication tool for IS, as underlined by al-Azaim Media Foundation in Voice of Khorasan (issue 43):

> *Even after its recent policy changes, Telegram continues to provide unique benefits that distinguish it from other messaging apps, particularly for users concerned about security and functionality (Voice of Khorasan, Issue 43, p. 53)*

Furthermore, over the almost six years, the domain selection is not uniform across Techhaven, with some rooms displaying the tendency to use different combinations of domains than others. This speaks to the human aspect of communication and fits with the day-by-day monitoring of these platforms, which has shown that IS operatives employ an adaptive approach to content dissemination, frequently rotating URLs and migrating to alternative platforms when faced with takedowns. That users in rooms switch to other domains makes it unlikely they will all make the same choice each time. Furthermore, as some rooms focus on specific geographic or linguistic audiences, their choices of domain may reflect differences in the familiarity with certain domains over others. This indicates that further analysis is warranted into the influence of human habits in propaganda distribution, alongside the presumed impact of content removal strategy as a rationale for changes to the platforms used to share content.

The analysis of the stream of URLs inside TechHaven reiterates the MCP approach of IS, strategically focused on decentralisation and redundancy to continuously increase the propaganda reach and mitigate the effects of counterterrorism measures. Overall, the SNA findings provide insights into how IS continues to exploit several digital platforms for propaganda dissemination. By understanding the structural role of Rocket.Chat and Telegram within this ecosystem, analysts can develop more effective countermeasures focusing on both the shifts in the platforms used to share content over time and a better understanding of the role of human habits in the distribution of terrorist content.

Funding Acknowledgment: This research was supported by the University of Maryland's MPowering the State (MPower) Strategic Partnership programme.

Alessandro Bolpagni is a senior research analyst at the Italian Team for Security, Terroristic Issues, and Managing Emergencies (ITSTIME) and lecturer at Università Cattolica del Sacro Cuore (UCSC). He specialises in OSINT, SOCMINT and Digital HUMINT for monitoring terrorist networks, recruitment tactics in the digital environment, and communication strategies and technologies implemented by terrorist organisations.

Ali Fisher is the lecturer at Università Cattolica del Sacro Cuore (UCSC) in Milan and Explorer of Extreme Realms at Human Cognition Ltd. He is a leading strategist whose work has supported government departments, agencies and military in both Europe and North America by providing actionable insights to counter emerging threats in complex information environments.

Endnotes

1 See Fisher, Prucha, and E. Winterbotham, "Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability", Global Research Network on Terrorism and Technology 6, (2019); M. Frampton, A. Fisher, N Prucha, "The New Netwar: Countering Extremism Online", Policy Exchange, (2017).
2 Macdonald, Stuart, et al. "Who disseminates Rumiyah? Examining the relative influence of sympathiser and non-sympathiser Twitter users", 2nd European Counter Terrorism Centre Advisory Group Conference (2018); Macdonald, Stuart, et al, "A Study of Outlinks Contained in Tweets Mentioning Rumiyah", Global Research Network on Terrorism and Technology: Paper No. 2 (2019); Weimann, Gabriel, and Asia Vellante, "The Dead Drops of Online Terrorism", Perspectives on Terrorism 15.4 (2021): 39-53.
3 Akil N. Awan and Mina al-Lami, "Al-Qa'ida's Virtual Crisis," The RUSI Journal 154, no. 1 (February 2009)
4 Anwar Al-Awlaki, "44 Ways to Support Jihad", Victorious Media, www.anwar-alawlaki, 2009.
5 Al-Yaqeen Media Center (مركز اليقين الإعلامي), "Methodology in Acquiring Media Experience (المنهجية في تحصيل الخبرة الإعلامية)", Al-Yaqeen Media Center (May 2011).
6 Al-Fajr Media Center, "Statement from Al-Fajr Media Center: Condolences and congratulations to the Islamic nation on the occasion of the martyrdom of Sheikh Al-Assad/Osama bin Laden, may God have mercy on him", Al-Fajr Media Center (May 2011).
7 N. Prucha, "Online Territories of Terror – Utilizing the Internet for Jihadist Endeavors", ORIENT IV (2011).
8 Gabriel Weimann, "Terror and the Internet", International Encyclopedia of the Socal & Behavioral Sciences, 2nd edition, Volume 24, 227–236, at 231–232.
9 N. Prucha, "Jihadi Twitter activism – Introduction", Jihadica.net, (2013(; Rüdiger Lohlker, "Tumbling Along the Straight Path – Jihadis on tumblr.com", University of Vienna (2012); 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).
10 N. Prucha, A. Fisher, "The Call-up: The Roots of A Resilient and Persistent Jihadist Presence on Twitter", CTX, Vol 4, No 3 (2014).
11 N. Prucha, A. Fisher, "Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda", Combating Terrorism Center at West Point 6, no. 6 (25 June 2013), https://ctc.westpoint.edu/tweeting-for-the-caliphate-twitter-as-the-new-frontier-for-jihadist-propaganda/.
12 M. Rudner, "Electronic Jihad": The Internet as al-Qaeda's Catalyst for Global Terror", Studies in Conflict & Terrorism, (2016) DOI: 10.1080/1057610X.2016.1157403.
13 N. Prucha, "Jihadi Twitter activism – Introduction", Jihadica.net, (2013).
14 Weimann, Gunnar J, "Competition and Innovation in a Hostile Environment: How Jabhat Al-Nusra and Islamic State Moved to Twitter in 2013–2014", Studies in Conflict & Terrorism 42 (1–2): 25–42 (2018), doi:10.1080/1057610X.2018.1513692.
15 L. Brynjar. "Jihadi web media production: characteristics, trends, and future implications", Norwegian Armed Forces (2007).
16 A. Fisher, N. Prucha, "Online Territories of Terror: The Manipulation Communication Paradigm and the Information Ecology of the Web3 Era", Routledge Handbook of Transnational Terrorism 10 (New York: Routledge, 2023).
17 Ayman al-Zawahiri, "General Guidelines for Jihad", as-Sahab Media (2013).
18 Ibid.
19 Ibid.
20 A. Bolpagni, E. Ristuccia, G. Giardini, "Creating awareness within the masses": mapping the pro-Islamic State (IS) ecosystem on Instagram", Security Terrorism Society 21, 2 (2025).
21 Abu Saad al-Amili, "Apathy in Jihadist Forums: Causes and Solutions", Fursan Al-Balagh Media (2013).
22 Ibid.
23 Ibid.
24 Fisher, Prucha, and Winterbotham, *Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability*, 2019.
25 A. Fisher, "Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence", Perspectives on Terrorism 9, 3 (June 2015), https://www.jstor.org/stable/10.2307/26297378.
26 N. Prucha, A. Fisher, *Tweeting for the Caliphate: Twitter as the New Frontier for Jihadist Propaganda*, 2013.
27 A. Fisher, N. Prucha, "The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0", Expert Paper, European Institute for Counter Terrorism and Conflict Prevention, (July 2022), https://eictp.eu/wp-content/uploads/2022/08/EICTP_Swarmcast2_FINAL.pdf
28 Conceived as a Web of cognition, Web 1.0 Web 1.0 is the first generation of the web, which could be considered the read-only web and also as a system of cognition. Moreover, it began as an information digital space for businesses to broadcast information to people, offering a limited

capacity of interactions among users. Web 1.0 is mainly built on core web protocols and formats, such as HTTP, HTML, and URI. See S. Aghaei, M. A. Nematbakhsh, H. K. Farsani, "Evolution of the World Wide Web: From Web 1.0 to Web 4.0", International Journal of Web & Semantic Technology (IJWesT), Vol. 3, No. 1, January 2012; C. Fuchs, W. Hofkirchner, M. Schafranek, C. Raffi, M. Sandoval, R. Bichler, "Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0. 2.0, 3.0", Future Internet, Vol. 2, No. 1, 41-59, 2010.

29 S. Wan, H. Lin, W. Gan, J. Chen and P. S. Yu, "Web3: The Next Internet Revolution," in *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34811-34825, 1 Nov.1, 2024, doi: 10.1109/JIOT.2024.3432116

A. Ghosh, Lavanya, V. Hassija, V. Chamola and A. El Saddik, "A Survey on Decentralized Metaverse Using Blockchain and Web 3.0 Technologies, Applications, and More," in *IEEE Access*, vol. 12, pp. 146915-146948, 2024, doi: 10.1109/ACCESS.2024.3469193

30 A. Fisher, N. Prucha, and E. Winterbotham, *Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability*, 2019.

31 Fisher, Prucha, *The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0*, 2022.

32 Fisher, Prucha, and E. Winterbotham, *Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability*, 2019.

33 Ibid.

34 Fisher, *Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence*, 2015.

35 John Arquilla and David Ronfeldt, "Networks and Netwars: The Future of Terror, Crime, and Militancy'", RAND - National Defense Research Institute (2001).

36 Ibid.

37 A. Fisher, *Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence*, 2015.

38 Ibid.

39 Ibid.

40 A. Fisher, *Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence*, 2015.

41 Ibid.

42 Ibid.

43 Ibid.

44 Ibid.

45 Web 2.0 represents the second generation of the Web, which is more participatory for users and wherein the latter are important as the content. Web 2.0 is mainly characterised by a higher degree of user participation, a conception of the Web as a medium of communication, and the emergence of social networks. See G. Cormode, B. Krishnamurthy, "Key Differences between Web1.0 and Web2.0", AT&T Labs-Research, February 2008; E. Constantinides, S. Fountain, "Web 2.0: Conceptual foundations and marketing issues", J Direct Data Digit Mark Pract 9, 231–244, 2008.

46 Berube L., Web 2.o ethos: hive mind and the wisdom of the crowd, Candos Publishing (2011), 21-31.

47 A. Fisher, *Swarmcast: How Jihadist Networks Maintain a Persistent Online Presence*, 2015.

48 Web 3.0 represents the third generation of the Web. It is mainly characterised by its decentralised structure, emphasising user control, security, and data encryption based on blockchain technology. Moreover, it is based on the principle of the semantic web sense, namely the desire to decrease humans' tasks and decisions, leaving them to the machine by providing machine-reliable content. See S. Aghaei, M. A. Nematbakhsh, H. K. Farsani, "Evolution of the World Wide Web: From Web 1.0 to Web 4.0", International Journal of Web & Semantic Technology (IJWesT), Vol. 3, No. 1, January 2012; J. Xiangjuan, F. Xinwei, Z. Yijie, Y. Heng, C. Xiaofeng, G. Wenfei, L. Weinan, H. Fanglei, "Integration and innovation of blockchain in Web3.0: current status and standardization prospects", World Wide Web (2025), Vol. 28, No. 7, 2024.
Carly Burdova, "What Is Web 3.0 (Web3 Definition)?", Avast, 8 December 2022, https://www.avast.com/c-web-3-0.

49 Fisher and Prucha, *Online Territories of Terror: The Manipulation Communication Paradigm and the Information Ecology of the Web3 Era*, 2023.

50 Bobby Allyn, "People Are Talking about Web3. Is It the Internet of the Future or Just a Buzzword?", National Public Radio (2021), https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision?t=1639411948920.

51 G. Edelman, "The Father of Web3 Wants You to Trust Less", Wired (2021), https://www.wired.com/story/web3-gavin-wood-interview/.

52 Fisher, Prucha, *The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0*, 2022.

53 Abu Saad al-Amili, *Apathy in Jihadist Forums: Causes and Solutions*, 2013.

54 N. Prucha, "IS and the Jihadist Information Highway - Projecting Influence and Religious Identity via Telegram", Perspectives on Terrorism 10, 6 (2016): 48–58.

55 Fisher and Prucha, *The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0*, 2022.

56 A. Amarasingman, "A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit", CTC Sentinel 13, 2 (February 2020), https://ctc.westpoint.edu/view-ct-foxhole-interview-official-europols-eu-internet-referral-unit/.

57 Arab News, "EU police deal 'severe blow' to Daesh online propaganda", Arab News (November

2019), https://www.arabnews.com/node/1589606/session_trace/page_view_timing/aggregate#:~:text=THE percent20HAGUE percent3A percent20European percent20police percent20said,land percent20in percent20Syria percent20and percent20Iraq.
58 A. Amarasingman, *A View from the CT Foxhole: An Interview with an Official at Europol's EU Internet Referral Unit, Issue 2, Volume 13*, 2020.
59 Ibid.
60 J. Stone, "European police remove 26,000 pieces of Islamic State content from social media", Cyberscoop, (November 2019), https://cyberscoop.com/eu-police-islamic-state-takedown/#:~:text=Google percent2C percent20Twitter percent2C percent20Instagram percent20and percent20Telegram,out percentE2 percent80 percent9D percent20content percent20of percent20this percent20kind.
61 Qimam Electronic Foundation (QEF), "Rocket Chat قيبطت", 2020.
62 Ibid.
63 C. Morselli, C. Giguère, K. Petit, "The Efficiency/Security Trade-Off in Criminal Networks", Social Networks, 17 (November 2016).
64 Ibid.
65 Fisher, Prucha, *The Salafi-Jihadi Online Ecosystem in 2022 - Swarmcast 2.0*, 2022.
66 A. Burato, M. Maiolino, M. Lombardi, "Dalla SOCMINT alla Digital HUMINT. Ricomprendere l'uso dei Social nel ciclo di intelligence", Sicurezza Terrorismo e Società 2, 5 (2015): 95-108.
67 V. D'Auria, A. Delli Paoli, "Digital Ethnography: A Systematic Literature Review", Italian Sociological Review, (January 2021): 243.
68 F. Borgonovo, M. Ziliani, "Strumenti di OSINT, SOCMINT e Digital HUMINT", in M. Lombardi, "Intelligence C4", BTT Editore (2022): 69.
69 Ibid.
70 Ibid.
71 Ibid.
72 Borgonovo, Ziliani, *Strumenti di OSINT, SOCMINT e Digital HUMINT*, 2022.
73 Basu, Aparna. "Social network analysis: A methodology for studying terrorism." Social Networking: Mining, Visualization, and Security. Cham: Springer International Publishing, 2014. 215-242.
74 Saxena, Sudhir, K. Santhanam, and Aparna Basu. "Application of social network analysis (SNA) to terrorist networks in Jammu & Kashmir." Strategic Analysis 28.1 (2004): 84-101.
Medina, Richard M. "Social network analysis: a case study of the Islamist terrorist network." *Security Journal* 27.1 (2014): 97-121.
75 Bolpagni, Ristuccia, Giardini, *Creating awareness within the masses": mapping the pro-Islamic State (IS) ecosystem on Instagram*, 2025.
Perliger, Arie, and Ami Pedahzur. "Social network analysis in the study of terrorism and political violence." *PS: Political Science & Politics* 44.1 (2011): 45-50.
76 J. Mathieu et al., "ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software", PLOS ONE 9, 6 (2014), https://doi.org/10.1371/journal.pone.0098679.
77 E. Mark, J. Newman, M. Girvan, 'Finding and Evaluating Community Structure in Networks', Physical Review E 69, no. 2 (2004).
78 S. Brin, L. Page, "The Anatomy of a Large Scale-Hypertextual Web Search Engine", Computer Networks and ISDN Systems 30, 1–7 (1998): 107–17.
79 Fisher, Prucha, and E. Winterbotham, *Mapping the Jihadist Information Ecosystem Towards the Next Generation of Disruption Capability*, 2019.
80 L. C. Freeman, D. Roeder, R. R. Mulholland, "Centrality in Social Networks: Ii. Experimental Results", Social Networks 2, 2 (1980-1979).
81 The data refers to the number of data provided by the Telegram channel ISIS Watch, analysing the number of Telegram channels and bots banned each month. In the period indicated, August 2024 and June 2025, the total number of Telegram channels and bots removed for sharing IS or pro-IS material amounts to 208,689.

About

Perspectives on Terrorism

Established in 2007, *Perspectives on Terrorism* (PT) is a quarterly, peer-reviewed, and open-access academic journal. PT is a publication of the International Centre for Counter-Terrorism (ICCT), in partnership with the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

Copyright and Licensing

Contact

E: pt.editor@icct.nl
W: pt.icct.nl

Universiteit Leiden

HANDA CSTPV