

RESEARCH ARTICLE

# In Mapping Digital Jihad: Understanding the Structure and Evolution of al-Qaeda's Information Ecosystem on the Surface Web

Miron Lakomy\*

Volume XVIII, Issue 2  
June 2024

ISSN: 2334-3745  
DOI: 10.19165/2024.6272

**Abstract:** This article, which combines social network analysis and open-source intelligence, discusses the functions, structure, and evolution of al-Qaeda's (AQ) information ecosystem on the surface web in the second half of 2023. It argues that despite preferring Rocket Chat as a primary communication channel, this terrorist organisation developed an extensive and robust propaganda distribution network detectable from the surface web. The pro-AQ ecosystem on this Internet communication layer relied primarily on standalone websites, message boards, and blogs, interconnected with a broad range of file-sharing services and channels on encrypted communication apps. Aside from them, the group manifested limited activity on mainstream social media. In the second half of 2023, the group demonstrated resilience to content takedowns, as most of its key domains used to disseminate propaganda continued to be active under the same or changed URLs. This study shows that, in contrast to the Islamic State, al-Qaeda's information ecosystem was largely decentralised, which was primarily caused by the differentiated approaches of its branches to maintaining their presence in this environment. The lack of centralisation of AQ's propaganda distribution network may be considered both an advantage and a disadvantage. On the one hand, it potentially increases its resilience to content takedowns. On the other hand, however, it also demonstrates a lack of coordination between branches, which decreases their media operations' potential efficiency and reach.

**Keywords:** Al-Qaeda, propaganda, networks, information, jihad

---

\* Corresponding Author: Miron Lakomy, University of Silesia, email: miron-lakomy@wp.pl

## Introduction

Al-Qaeda (AQ) is one of the first terrorist organisations that started to use the Internet to radicalise, inspire, and recruit followers. Its activities in this regard, dating back to the 1990s, evolved significantly over time. During the War on Terror, AQ spearheaded the development of terrorist online propaganda in many aspects.<sup>1</sup> Among others, it introduced new forms of influencing online audiences, as demonstrated by Abu Musab al-Zarqawi of al-Qaeda in Iraq (AQI).<sup>2</sup> It was also one of the first to experiment with new channels of propaganda dissemination.<sup>3</sup>

Due to these features, al-Qaeda's online strategic communication has been the subject of significant interest from the academic community. Since the beginning of the 21<sup>st</sup> century, researchers representing diverse fields have analysed this phenomenon from multiple angles. Many scholars focused on understanding what AQ published and how these productions radicalised and inspired online audiences.<sup>4</sup> Others were more inclined to explore the workforce behind its propaganda machine.<sup>5</sup> Noticeable attention was also devoted to understanding some distinctive types of AQ's propaganda, such as its terrorist manual series<sup>6</sup> and e-magazines.<sup>7</sup> However, in a plethora of publications on AQ's strategic communication, relatively few publications have focused on understanding the structure, core features, and evolution of its propaganda distribution networks. While such works were published in the pre-Islamic State era,<sup>8</sup> only a few significant studies have attempted to do so in recent years. This contrasts with the amount of attention in the subfield of online terrorism and political violence dedicated to, for instance, mapping information ecosystems maintained by far-right violent extremist organisations (VEOs) and the Islamic State (IS).<sup>9</sup> Effectively, we have only a limited understanding of how exactly al-Qaeda distributes its propaganda today and how to curb it.

This study aims to fill this gap in research and has three scientific objectives. First, to identify communication channels exploited by AQ and its followers on the surface web in the second half of 2023 and understand their main functions. Second, to map the structure of the pro-AQ information ecosystem in this environment and explore its crucial elements responsible for propaganda distribution. Third, to understand the evolution of the detected AQ's propaganda dissemination network over a period of six months, which enables its vitality and resilience to be measured. To reach these objectives, this study exploits a combination of open-source intelligence, social network analysis (SNA), and comparative analysis. It focuses on communication channels available on – or detectable from – the surface web, as this layer of Internet communication potentially offers the easiest and broadest access to terrorist propaganda. The data discussed in this paper was collected between 1<sup>st</sup> July and 31<sup>st</sup> December 2023.

This research article is divided into five sections. The first briefly overviews the most critical studies on AQ's exploitation of the surface web for propaganda distribution. The second covers in detail the methodology of this research project, including open-source intelligence methods utilised and approaches used in social network analysis. The third section discusses fundamental quantitative data collected by this study in a comparative perspective. It provides information on the quantity and types of the identified propaganda distribution channels in July and December 2023. The fourth part explores the structure and interconnectedness of al-Qaeda's information ecosystem on the surface web uncovered in July 2023. The final section highlights crucial changes introduced to this ecosystem throughout a period of six months.

## What Do We Know About al-Qaeda's Use of the Surface Web?

Al-Qaeda's propaganda dissemination networks were the subject of scientific analyses primarily at the apogee of the War on Terror. One of the first to do so was Weimann, who listed and investigated communication channels used by the group at the beginning of the 21<sup>st</sup> century. His analyses covered popular webpages run by AQ at the time, such as *alned.com*, *jihadunspun.net*, *aloswa.org*, *islammemo.com*, and *jehad.net*.<sup>10</sup> In the following years, various recognised scholars, such as Riedel,<sup>11</sup> Zelin,<sup>12</sup> Awan,<sup>13</sup> and Conway,<sup>14</sup> have studied various aspects of al-Qaeda's exploitation of standalone websites and message boards. The scale of the Salafi-jihadist information ecosystem – dominated by al-Qaeda – was estimated to reach 4,000 domains between 2000 and 2005.<sup>15</sup> Unfortunately, due to the lack of publicly accessible databases from this period, we know little about how this network exactly functioned, its accurate scale at a given time, its accessibility, and how it responded to content takedowns. In time, due to the belief that traditional websites were in decline,<sup>16</sup> scholars' attention started to shift increasingly toward exploring al-Qaeda's migration to social media platforms. The papers of Weimann,<sup>17</sup> Klausen,<sup>18</sup> West,<sup>19</sup> and Torres-Soriano<sup>20</sup> described various aspects of this notable process.

Since 2014, the scientific community working on online terrorist communication has paid visibly less attention to analysing al-Qaeda's media operations on the Internet. This was primarily caused by the launch of the Islamic State's "shock and awe" propaganda campaign.<sup>21</sup> Effectively, the academic discourse in this subfield was dominated for several years by studies exploring different aspects of IS's activities online. These studies that included al-Qaeda frequently compared its operations on the Internet to those carried out by Islamic State.<sup>22</sup> After the fall of IS as a territorial organisation, online terrorism and political violence research started to be dominated by studies concentrating on the far-right violent extremists' use of various online platforms, including primarily messaging apps and services used by video gamers.<sup>23</sup>

Effectively, al-Qaeda's online operations drew relatively little attention from the academic community in the last decade. We know little about the scale, structure, and evolution of its information ecosystem since the launch of Islamic State's propaganda campaign. This is especially visible regarding AQ's presence on the surface web, which has remained under-researched for years. This trend was accurately summarised by Conway and Looney, who argued that "terrorist websites never really went away, they were just overlooked for a decade by researchers and others due to a not unwarranted narrowing of focus to social media platforms and, latterly, messaging applications and adjacent online spaces".<sup>24</sup>

In this context, there is just a handful of more recent academic papers published in recognised journals that touch upon al-Qaeda's presence on the surface web and beyond. In 2017, Rudner published a paper that attempted to understand how this terrorist organisation exploited various Internet platforms, ranging from message boards to *Facebook* and *Twitter*. His study noticed the Salafi-jihadist migration from the World Wide Web towards social media but still emphasised the importance of terrorist-operated websites.<sup>25</sup> In 2021, Nsaibia and Lyammouri published a valuable analysis of al-Qaeda's propaganda distribution strategy, although it focused primarily on encrypted communication apps like *WhatsApp* and *Rocket Chat*. They noted that "while al-Qaeda groups are certainly present on Telegram, WhatsApp, Riot, and Minds, the number of subscribers on these platforms is only a fraction of the number of users on Rocket Chat".<sup>26</sup> Insightful reports on various aspects of AQ's online propaganda were also recently published by Taneja and Thakkar. Taneja compared al-Qaeda's and Islamic State's propaganda related to the Hindu-Muslim tensions.<sup>27</sup> Thakkar, on the other hand, focused on the development

of al-Qaeda's capabilities in carrying out global propaganda campaigns. She also noticed that AQ has profited from "the efforts of intelligence and security agencies to evict Islamic State's media constellations from encrypted and social media platforms."<sup>28</sup> In this context, while all these studies provided valuable insights, none allowed for a better understanding of the scale, structure, and functions of al-Qaeda's information ecosystem on the surface web.

## Methodology

As stressed above, this study aims to fill this gap in research by providing a detailed picture of al-Qaeda's information ecosystem discoverable on and from the surface web in the second half of 2023.<sup>29</sup> To do so, it was founded on the combination of open-source intelligence, comparative analysis, and social network analysis.<sup>30</sup> Open-source intelligence means were primarily based on the so-called "Google dorks," which is a set of methods allowing for maximisation of search results based on the use of advanced options and operators in the *Google* search engine.<sup>31</sup> Other capable search engines, including *Bing*, *Yahoo*, *Baidu*, *Yandex*, and *DuckDuckGo*, were used in a similar manner.

There were several distinct ways of carrying out advanced searches for al-Qaeda-associated URLs.<sup>32</sup> To begin with, this part of the investigation used specific keywords related to AQ, its branches, media offices, or titles of individual propaganda productions. They were combined with advanced operators, allowing the uncovering of communication channels operated by terrorists. The study used search queries utilising terminology in multiple languages popular in AQ's propaganda, including Arabic, English, Bengali, and Somali. Aside from the terminology itself, advanced search methods exploited addresses of the detected websites of al-Qaeda, which allowed the identification of link directories and hotspots of networking used by its followers. Aside from search engines, the study also utilised alternative methods of detecting such content, including reverse image search platforms and software, such as *TinEye*, *Yandex Image Search*, or *Google Lens*. Image-based search queries used the most popular pieces of content or logotypes published by al-Qaeda. Subsequently, detected links were verified regarding their association with this terrorist organisation.<sup>33</sup>

Positively verified and available URLs were subject to subsequent website intelligence (WEBINT) gathering,<sup>34</sup> mainly comprising various forms of data scraping. It primarily aimed to discover information, allowing learning locations of other interconnected communication channels used by al-Qaeda. To do so, the study used several distinct methods, including those focused on extracting out links leading to other associated AQ domains. Aside from them, the study focused on other relevant pieces of data, such as websites co-hosted on the same server or information included in the website's code. For this purpose, several types of software were used, including *SpiderFoot* and *Recon NG*. In this context, it must be noted that data scraping was not carried out on communication channels falling beyond the surface web unless they could be accessed with an ordinary browser and without the need for additional registration. In other words, the study collected deep web and dark web links available from the surface web, as well as information about channels on messaging apps, but in most cases, they were not subject to additional data scraping.

All identified Internet addresses were registered in the database under multiple categories. First, each URL was coded in terms of its type, namely: Web 1.0 (surface web domains, such as standalone websites, blogs, and message boards), Web 2.0 (social networks, file-sharing services), communication apps (*Telegram*, *Rocket Chat*, *Threema*, *WhatsApp*, etc.) and dark web (mainly .onion domains). Second, the availability of all detected URLs that could be accessed with an ordinary browser was verified and registered in the database at regular intervals. This

verification occurred at the beginning and end of each month.<sup>35</sup> Internet addresses were coded as “positive” if their content was accessible for at least one day a month. Third, monthly changes in accessibility were also registered separately. Fourth, approximate dates of takedowns and creation were included wherever possible. Fifth, all URLs associated with a given domain (for instance, through out links) were registered for social network analysis. In this context, it must be noted that multiple external links from one URL to a single file-sharing platform were treated in the database as one record.<sup>36</sup> Exceptions were made only in these cases where pro-AQ media operatives treated file-sharing domains as separate communication ecosystems. This attitude mainly applied to accounts active on the Internet Archive. Finally, each detected and accessible domain was subject to online observation, focusing on understanding its predominant function in propaganda dissemination.

This cumulative database, compiled and updated monthly,<sup>37</sup> was subject to subsequent social network analysis, primarily done with *Gephi*.<sup>38</sup> To do so, detected URLs were given unique IDs and treated as “nodes” in SNA.<sup>39</sup> Each node was assigned additional variables, including availability in a given month and the cumulative number of mirrors detected during the investigation. This allowed a “node list” to be created. A second database – an “edge list” – was also compiled, which included interconnectedness between the nodes based on the detected external links in the pro-AQ communication channels. This approach effectively allowed the structure of the al-Qaeda information ecosystem to be mapped.

Both databases combined were subject to social network analysis from multiple angles, including:

- degree – related to the number of connections to a given node;
- modularity class – a method allowing showing internal subdivisions (“communities”) in a network, based on the comparison of densities of edges within a group;<sup>40</sup>
- page rank – calculated based on the links directed to a node from other nodes.<sup>41</sup>

Effectively, six monthly graphs portraying the interconnectedness and specific features of al-Qaeda’s information ecosystem on the surface web were generated. A comparative analysis of the monthly databases was carried out at the final stage. Both quantitative and qualitative approaches were adopted. The quantitative analysis focused on monthly changes in all coded variables – including, for instance, the number of standalone websites or social media profiles detected and their availability. This facilitated learning how this propaganda distribution network evolved over time. The qualitative approach, on the other hand, focused more on the changes in the features of the ecosystem as a whole, as well as the changes in the functions of individual communication channels over a six-month period.

This study has one limitation that must be discussed in detail. As mentioned above, this project prioritised exploring the surface web. This approach allowed for the detection of parts of al-Qaeda’s information ecosystem located on the deep and dark web, as well as in encrypted communication apps. However, these environments were usually not subject to additional data scraping, similar to surface web locations. Such an approach was adopted because the surface web, aside from being under-researched, still plays a crucial role in Salafi-jihadist propaganda dissemination.<sup>42</sup> Terrorist-operated websites (TOWs) are less ephemeral compared to alternative communication channels, accessible with ordinary web browsers, and usually do not require additional registration.<sup>43</sup> Thus, violent extremist organisations tend to use them to maximise the efficiency of their strategic communication. Moreover, there are certain legal constraints in exploring encrypted environments used by terrorists in the territory of the European Union member states where this project was conducted. Effectively, there is a limited risk that this study does not provide a complete picture of al-Qaeda’s information ecosystem in the second

half of 2023 due to the lack of data scraping of, for instance, the *GeoNews* platform. Still, the data gathered in this project allowed for portraying the core of its propaganda dissemination network, which was available on (or detectable from) the surface web at the time.

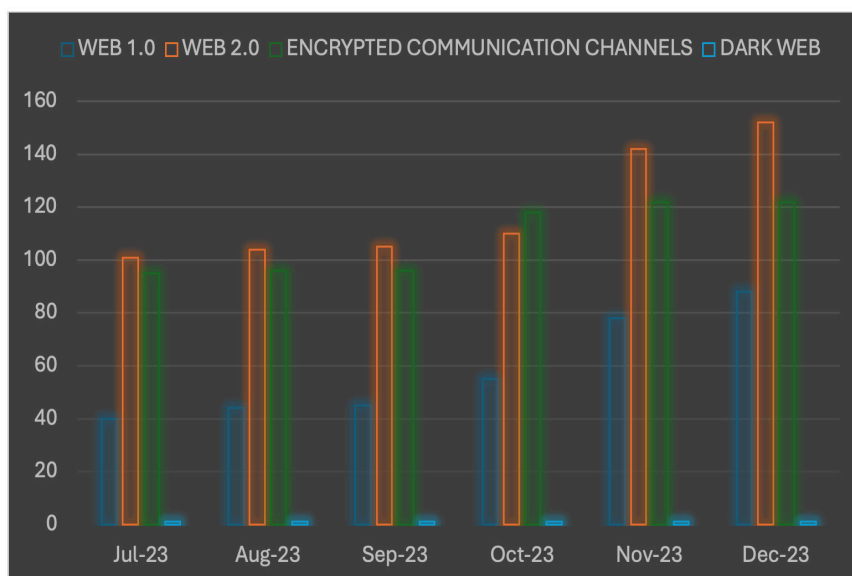
There are also two caveats. First, due to research ethics reasons, this study avoided collecting or processing any data that could be related to individual people. It consisted of no activities defined as profiling natural persons with online identifiers.<sup>44</sup> Second, for counter-terrorism reasons, this paper does not provide exact URLs of the detected communication channels used by al-Qaeda and its followers. Instead, it uses labels adopted in social network analysis.

## Evolution of al-Qaeda's Propaganda Dissemination Networks on the Surface Web in the Second Half of 2023: A Quantitative Perspective

In July 2023, the study detected 237 individual Internet addresses associated with al-Qaeda. This number comprises 40 standalone webpages, 101 Web 2.0 addresses (social media or file-sharing services), 95 channels on communications apps, and one .onion domain. Six months later, the identified ecosystem proved to be 53.1 percent bigger, consisting of a cumulative number of 363<sup>45</sup> Internet addresses. It consisted of 88 standalone websites and blogs,<sup>46</sup> 152 Web 2.0 addresses, 122 communication applications, and one webpage located on the dark web (Figure 1).<sup>47</sup> This data shows how dynamic al-Qaeda's ecosystem was, as it regularly established new ways of communicating with online audiences.

It must be noted that throughout the second half of 2023, proportions in the structure of this ecosystem changed. The most significant change could be seen in the use of TOWs, as the cumulative number of standalone websites and blogs increased by 120 percent compared to July. It is indicative of their importance for al-Qaeda's propaganda distribution. Moreover, while in the summer of 2023, the share of messaging apps and Web 2.0 in the whole network was almost equal, it shifted in favour of the latter six months later. In December, the number of detected Web 2.0 URLs increased by 50.4 percent, compared to only a 28.4 percent rise in the use of encrypted communication apps. No new developments in the use of the dark web were detected.

Figure 1. Structure of pro-AQ information ecosystem between July and December 2023



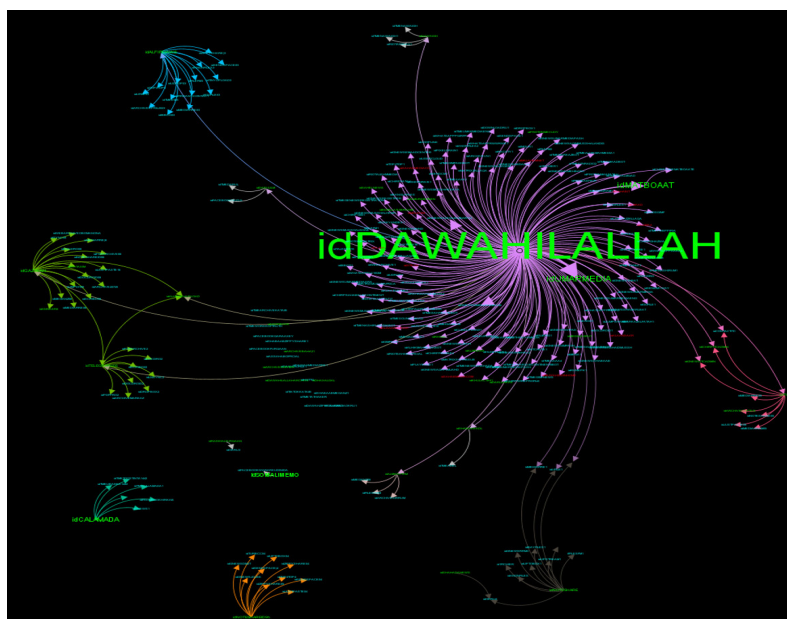
Source: The VEOMAP project

The most significant quantitative change in the number of detected Internet addresses occurred in October (37 new channels identified) and November (59 URLs). These changes were, at least partially, caused by the October 7<sup>th</sup> terrorist attack against Israel and its subsequent military operation in Gaza, which significantly engaged al-Qaeda's strategic communication.<sup>48</sup> In effect, its media offices launched many publication series dedicated exclusively to events in Palestine, which were distributed through a set of new blogs and file-sharing services. However, at the time, the group also advertised a large number of new *Telegram* and *Rocket Chat* channels, run by such media cells as Markaz al-Fatah, al-Sindh Media, Thabat News Agency, and al-Firdaws Media. In December 2023, AQ's activity in establishing new communication channels slightly dropped.

## Mapping al-Qaeda's Surface Web Propaganda Ecosystem on the Surface Web in July 2023

Looking at al-Qaeda's information ecosystem, as of July 2023, through the lens of social network analysis, allows for identifying some of its features that are critical to understanding the group's propaganda distribution strategy. First of all, as demonstrated by Figure 2, a large part of the detected network was concentrated around the *Dawahilallah* message board, which stands out in terms of its SNA degree level, maintaining 168 connections as of July 2023. This domain, active since at least 2017, proved to be a primary communication hotspot for online communities and media offices supporting al-Qaeda in the Indian Subcontinent (AQIS), although its everyday audience was somewhat limited.<sup>49</sup> It was utilised predominantly by the group's Bengali-speaking supporters for networking, exchanging ideas, and gathering information. It constituted a link directory, allowing followers to reach active AQ communication channels available on the messaging apps, as well as the surface, deep, and dark web. Aside from these functions, *Dawahilallah* served multiple pro-AQIS media centres as a propaganda aggregator. Such entities as al-Firdaws Media, al-Hikmah Media, Islamic Translation Centre, and an-Nasr Media used this board's "sticky threads" function to share their productions regularly. On top of this, this domain provided AQ supporters a platform to debate the most important international events, interpret religious texts, and discuss various aspects of jihad.

Figure 2. AQ information ecosystem in July 2023 through the lens of social network analysis<sup>50</sup>



Source: The VEOMAP project

*Dawahilallah* proved to be interconnected with several important parts of the pro-AQ ecosystem. First, as of July 2023, it shared links to 84 channels on encrypted communication apps. Most of them redirected users towards the *Rocket Chat*-based *GeoNews* platform, utilised by prominent al-Qaeda media offices, ranging from the al-Kata'ib Foundation – which supports Harakat al-Shabaab al-Mujahidin (HSM) – to al-Andalus Media, producing propaganda for al-Qaeda in the Islamic Maghreb (AQIM). This confirms the previously mentioned AQ's preference to exploit *Rocket Chat*, which offers open-source architecture and owner-operated servers.<sup>51</sup> However, aside from *GeoNews*, the board's members published information on the whereabouts of pro-AQ content on other encrypted messaging platforms like *Chirpwire*<sup>52</sup> and Telegram.

Second, *Dawahilallah* redirected users towards a broad range of file- and text-sharing services, including mega.nz, noteshare.id, jumpshare.com, mediagram.me, file.fm, gofile.io, and justpaste.it. Overall, the webpage contained links to 49 different Web 2.0 platforms as of July 2023. They were predominantly used as short-term storage for individual pieces of content released by al-Qaeda. However, the same file-sharing role was also fulfilled by multiple WordPress blogs that were advertised on the board, mostly by an-Nasr Media. They lacked any content on the main page, but their subdomains were exploited to store individual propaganda items for periods ranging from several weeks to several months. This approach to using blogs is relatively uncommon among other violent extremist organisations.<sup>53</sup>

Third, *Dawahilallah* redirected its users to other standalone websites and blogs that played important roles in al-Qaeda's information ecosystem. The board's members prioritized publicising links to a broad range of websites targeting online audiences from Southern and Southeastern Asia, including, for instance, *Matboaat*, *Gazwah*, or an-Noor Media's home page, all of which published a variety of pro-AQ propaganda in Bengali. *Gazwah* stood out in terms of the quantity and quality of the published content. It was a standalone website that published translations of various types of propaganda associated with al-Qaeda. It maintained a significant propaganda distribution network by itself, sharing its publications through thirteen different file-sharing services, including mega.nz, *Internet Archive*, noteshare.id, and justpaste.it. It was also interconnected with several blogs. Other communities in the region were also targeted. Among others, *Dawahilallah* shared links to a webpage dedicated to influencing the Rohingya community or to the *Nawaigh* domain, which targeted Hindi-speaking Internet users. Aside from them, this message board advertised these parts of the surface web ecosystem that was maintained by al-Qaeda's Arabic-speaking core. These websites included, among others, the *Sahelnews*, which stored various types of propaganda in its subdomains. More in-depth analysis of its content was impossible, as the webpage required a signing-up procedure. In July 2023, the message board also shared links to – inactive at the time – URLs used by al-Malahem Media and al-Zallaqa Media. On top of this, the board's members distributed links to a constellation of loosely associated domains, such as the *Umarmedia*, which constitutes a primary communication channel utilized by the AQ-aligned Tehreek-E-Taliban Pakistan (TTP).<sup>54</sup> *Dawahilallah* lacked significant connectivity with websites exploiting Western languages. One notable exception was the *al-Minara* blog in English, which remained accessible in 2023 but was not updated for some time.

Two Internet addresses stood out among all websites interconnected with this message board. The first was run by al-Firdaws Media Foundation, a pro-AQ office publishing content in Bengali. While it predominantly focused on the Indian Subcontinent, al-Firdaws Media frequently shared productions released by other branches of al-Qaeda. Compared to other standalone websites linked with *Dawahilallah*, it proved to have the most professional structure and was updated regularly. For instance, it released a series dedicated to highlighting "crimes" committed against Muslims globally, articles publicizing successful operations of al-Qaeda in Africa and the Middle

East, or pieces positively framing the Taliban's rule over Afghanistan. Al-Firdaws domain was also a central point of a separate propaganda distribution network consisting of twelve Web 2.0 platforms, such as anonfiles.com, top4top.io, tinyupload.com, gofile.io, and file.fm, sendspace.com, zippyshare.com, and udrop.com. Al-Firdaws website also redirected all visitors towards its official channel on *Telegram*.

The second exceptional website was run by the Islamic Translation Centre (ITC), a media office dedicated to boosting the multilingual campaign of al-Qaeda similarly to the Islamic State's I'lam Foundation or Fursan al-Tarjuma.<sup>55</sup> As of July 2023, the ITC domain published content in 34 languages, including English, Albanian, Persian, Pashto, Arabic, and Tamil. Aside from the website itself, translated propaganda items were stored on a constellation of external file-sharing platforms, including mediagram.me, mediafire.com, noteshare.id, and the *Internet Archive*. Aside from propaganda aggregation, ITC's webpage focused on redirecting all visitors to its official channels at *GeoNews* and *Chirpwire*.

In this context, there were other parts of the pro-AQ information ecosystem detected in July 2023 that maintained no evident links with the network discussed above, which shows the lack of coordination between different branches. These parts mainly comprised websites associated with Harakat al-Shabaab al-Mujahidin.<sup>56</sup> Among those, *Calamada*, *Shahadanews*, *Radio al-Furqaan*, and *Somalimemo* stood out. *Calamada* proved to be the primary communication channel that disseminated content in Somali, produced by all official and unofficial media bureaus associated with HSM, including al-Kata'ib Foundation, Idaacadda Andalus, and Radio al-Furqaan. This domain stood out primarily regarding the regularity of the published content. Every day, it released between three to five radio broadcasts alongside various other productions, including combat videos, photo reports, and standalone articles. They covered a broad spectrum of topics ranging from international relations to highlighting HSM's victories in Eastern Africa. *Calamada* also maintained a small network of interconnected propaganda distribution channels, consisting of (among others) ok.ru or *Telegram*. *Shahadanews*, run by HSM-aligned Shahada News Agency, fulfilled a similar function but released content in Arabic. It focused on a relatively narrow set of topics, including promoting HSM operations in Somalia and Kenya, in particular.<sup>57</sup> In contrast to *Calamada*, aside from ok.ru, it maintained no relevant links to other platforms as of July 2023. Radio al-Furqaan's webpage published regular audio broadcasts. Its content was organized into several sections, such as internal news, international news, reports, the history of Islam, special programs, and more (photos, videos, and literature). Similarly to *Shahadanews*, the only relevant external link led to the ok.ru webpage, which HSM-aligned media offices preferred. The last relevant standalone website aligned with al-Shabaab – *Somalimemo* – had a history of supporting this organisation since 2011. It generally fulfilled similar functions to *Shahadanews*, although it primarily shared content in Somali. It stood out mainly in terms of the highest number of parallel mirrors active simultaneously on the surface web.

There were two eye-catching features of the al-Shabaab-related propaganda dissemination network. In contrast to the rest of the mapped ecosystem supporting al-Qaeda on the surface web, it attempted to exploit mainstream social media platforms. This tendency was already noticed in 2022 by Ayad, Harrasy, and Abdullah A.<sup>58</sup> *Somalimemo* advertised itself on and was supported by a *Facebook* profile, although its reach was limited to only 34 followers as of July 2023. *Calamada* exploited the same platform, although in a slightly different manner – mostly for file-sharing purposes. Lastly, al-Kata'ib Media also ran a popular *TikTok* profile consisting of more than 30 videos in the summer of 2023. This shows that al-Shabaab media operatives wanted to capitalise on the popularity of this platform in a similar manner to, for instance, far-right violent extremist organisations.<sup>59</sup> Aside from these attempts, it should be stressed that, surprisingly, none of these HSM-related websites and profiles contained links leading to other

parts of the al-Shabaab's ecosystem. No attempt was, therefore, made to mutually reinforce their traffic with out links, which contrasts with the approach frequently adopted by other VEOs.<sup>60</sup>

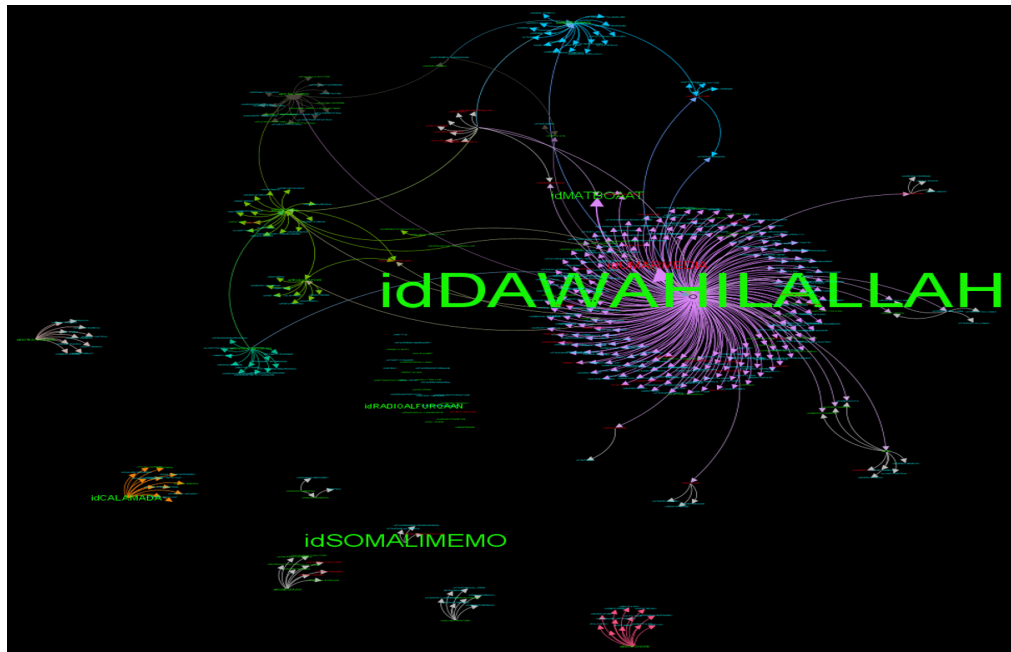
Other Internet addresses in AQ's information ecosystem played secondary roles and lacked substantial interconnectedness with the communication channels discussed above. Judging from their content, they were probably manifestations of al-Qaeda's followers' attempts to support the group's presence on the surface web. This is hinted at by the fact that many constituted link directories, rerouting online audiences to AQ-affiliated communication channels.

## A Structure of al-Qaeda's Surface Web Information Ecosystem in December 2023

At the end of 2023, the accessibility and functions of primary surface web communication channels utilised by al-Qaeda remained generally unchanged. After six months, those websites that aimed to influence online audiences in Southern and Southeastern Asia used similar addresses and remained active. This refers, among others, to *al-Firdaws*, *Gazwah*, *Matboaat*, and ITC web pages. The only exception was the TTP-aligned *Umarmedia*, which was temporarily unavailable but eventually reestablished an active URL. No significant changes in accessibility and functions could also be registered in the network associated with Harakat al-Shabaab al-Mujahidin. They were not subject to any content takedowns.<sup>61</sup> The most important SNA data related to the core nodes in the ecosystem are provided in Appendix 1.

Still, during the second half of 2023, five quantitative and qualitative changes were introduced in AQ's information ecosystem (Figure 3). To begin with, the propaganda distribution network concentrated around the *Dawahilallah* message board developed significantly. The number of Web 1.0 URLs advertised on this message board grew from 35 to 62 Internet addresses as of December 2023. They predominantly consisted of *WordPress* blogs used mainly by an-Nasr Media to store its productions. Moreover, compared to July 2023, *Dawahilallah* gained nine new links (up to a cumulative number of 58) to Web 2.0 platforms. They mainly consisted of new file-sharing services like *drive.internxt.com*, *backblazeb2.com*, and *k00.fr*. It also gained multiple links to new channels on messaging apps, including *WhatsApp*, *GeoNews*, *Matrix*, and *Telegram*. Most of them seemed to be new versions of the channels banned by law enforcement agencies, as over time, the study registered several new channels run by the same bureaus. Overall, in December 2023, the degree level of *Dawahilallah* increased to 228, compared to 168 in July 2023, which constituted a 35.7 percent rise. This change manifests that aside from aggregating propaganda and networking, this message board played an important role in sharing information on the whereabouts of AQ-affiliated propaganda. However, this function was partially mitigated by its relatively low popularity, narrowed down predominantly to Bengali speakers. While the board consisted of propaganda published by multiple branches of the group, only AQIS-aligned media offices used it to disseminate propaganda. Effectively, despite its high degree level in SNA, caused by its interconnectedness with other pro-AQ addresses, it could hardly be considered a cornerstone for the whole information ecosystem maintained by this terrorist organisation.

Figure 3. AQ information ecosystem in December 2023 through the lens of social network analysis



Source: The VEOMAP project

Secondly, al-Firdaws Media, the most active media office supporting AQIS, made attempts to expand beyond its traditional environment during the second half of 2023. It was manifested by the fact that the group created and exploited a *YouTube* account. Its primary function was to release a news series summarising the most important topics covered by this group each week. Such content was usually published in a way that allowed it to be disguised as non-partisan journalism. Al-Firdaws avoided the most controversial topics and often used images and videos originating from mass media or social networks. Still, this account was subsequently blocked by the platform.

Thirdly, a number of new standalone websites that supported al-Qaeda's ideology were identified. Some of them were active for a long time, although they were not initially detected. One of the most important was a website that focused on the history of jihadism. This domain, apparently associated with the pro-AQ community in the Caucasus, featured numerous videos and images highlighting the most important Salafi-jihadist leaders during the War on Terror, including Osama bin Laden and Ayman al-Zawahiri. This webpage maintained a well-developed propaganda distribution network consisting of several channels on *Telegram* and *Chirpwire*, an *Internet Archive* account, and two *Discord* groups. It was the only recorded case of a pro-al-Qaeda media office exploiting *Discord*, which as other researchers have noted is a common strategy among far-right groups.<sup>62</sup>

Another relevant webpage focused on publishing fatwas on issues related to jihad.<sup>63</sup> It was advertised by the *Dawahilallah* message board as a relevant and accurate source of theology-related information on an armed struggle against disbelievers. However, similarly to al-Firdaws Media, this domain avoided posting content directly associated with al-Qaeda. Thanks to this strategy, it was present on multiple mainstream platforms, allowing it to increase its resonance with the online audience. They included *Twitter/X*, *Facebook*, and *YouTube* profiles and an *Internet Archive* account. Its *YouTube* profile had 61 videos and 513 subscribers as of November 2023. On top of this, it utilised several file-sharing services, including *mymegacloud.com*, *top4top.io*, and *megaup.net*.

During the second half of 2023, several new pro-AQ blogs emerged online. Among others, the *Shohayeb* blog featured a number of official al-Qaeda propaganda productions. For instance, it published Osama bin Laden's *Letter to America*, which was seemingly AQ's response to the fact that it went viral on American social media.<sup>64</sup> It must be noted that similar actions at the time were carried out also by other AQ-aligned communication channels. Another new URL, located on the *Site123* platform, constituted a high-quality news webpage on al-Qaeda's activities. Aside from these two, there were also some blogs that promoted both AQ and Taliban agendas simultaneously. On top of this, many websites consisted of the group's propaganda, which were still accessible but remained inactive for several years.

Lastly, the study detected several new communication channels exploited by those branches of al-Qaeda that manifested little interest in maintaining a significant presence on the surface web, notably Jama'at Nusrat al-Islam wa al-Muslimeen (JNIM) and al-Qaeda in the Arabian Peninsula (AQAP). Media offices representing those branches, al-Zallaqa Media and al-Malahem Media, moved their websites to new URLs. However, they remained temporarily unavailable in the second half of 2023 and lacked technical quality compared to domains maintained by pro-AQIS bureaus. Furthermore, they were visibly treated by both branches as secondary communication channels. This was proven by the distribution of one of the most important al-Qaeda propaganda productions in recent years, the video *Inspire – What America and the West Do Not Expect: Open Source Jihad*,<sup>65</sup> published by al-Malahem Media in December 2023. This high-quality bomb-making manual was not released through its official website but only through *Rocket Chat* and *Telegram*. In this context, aside from standalone domains, this study found that al-Zallaqa Media's *Chirpwire* channel was exploited to disseminate its propaganda and advertise other al-Zallaqa channels located on other platforms, such as *Telegram*. Effectively, it demonstrated that this platform was still considered a gateway to attract online audiences from the surface web and reroute them deeper into the encrypted part of the AQ ecosystem.

## Conclusion

This study allows several conclusions to be drawn. First of all, the information ecosystem maintained by al-Qaeda in the second half of 2023 proved to be stable, holding a high degree of accessibility. The vast majority of standalone websites that served as primary communication channels for al-Qaeda remained available during this period, which shows that its propaganda distribution network was generally resilient to relatively infrequent content takedowns. Over six months, it also grew significantly and tended to rely more on terrorist-owned domains and blogs.

The overall scale of AQ's information ecosystem on the surface web during this period was relatively large and similar to the one supporting the Islamic State in mid-2021.<sup>66</sup> It also relied on a similar set of Web 2.0 platforms, as well as messaging apps (*Telegram*, *Rocket Chat*). However, the structure of these networks was different in many aspects. This difference primarily refers to the fact that the Islamic State's propaganda distribution network in this environment was more centralised, founded on the so-called "Index" (*Fahrmas*) webpage that served as a central link directory, rerouting its followers to all relevant communication channels associated with this terrorist organisation.<sup>67</sup> This strategy contrasts with al-Qaeda's information ecosystem mapped by this study, which lacks a similar cornerstone of the whole propaganda dissemination network. The *Dawahilallah* message board is closest to providing such a function. Still, it cannot be considered central due to its limited traffic, focus on digital jihad in South and Southeastern Asia, and the lack of connectivity with networks maintained by al-Shabaab.

The lack of a central communication channel dedicated to aggregating propaganda and redirecting followers to other relevant parts of the ecosystem seems to be primarily caused by the specific internal structure of al-Qaeda. This study confirms the recent findings indicating that AQ as a whole prioritised the use of *Rocket Chat* through its *GeoNews* platform.<sup>68</sup> However, its branches adopted differentiated – and sometimes opposing – strategies to utilise the potential offered by the surface web. In this context, such groups as JNIM, AQIM, and AQAP attached relatively little importance to maintaining a prolonged presence in this environment. While they manifested some activity in this regard, their websites remained inaccessible for long periods and lacked significant connectivity with other parts of AQ’s networks. Moreover, as manifested by al-Malahem Media, they sometimes used the surface web to publish only less important propaganda pieces, while the essential productions were released elsewhere. This contrasted with the approach adopted by HSM and AQIS, which attached significant importance to reaching online audiences through standalone websites, message boards, and blogs. These contrasting attitudes explain the eye-catching lack of solutions introduced by most AQ websites to reinforce the traffic in other parts of the ecosystem through out links, which is a common feature present in Islamic State domains.

It should also be stressed that pro-AQ media offices manifested great interest in using platforms that were considered successful in detecting and removing terrorist content. This was proven by the fact that they regularly exploited *Facebook*, *TikTok*, and *YouTube* to reach online audiences. They were also interested in introducing innovations in propaganda dissemination strategy, as they tested *GitHub* and *Discord*, which Salafi-jihadist media operatives have not frequently used in recent years.<sup>69</sup> While these activities were relatively short-lived, they hinted at the capability to learn from others – namely far-right, violent extremist organisations – and test new ways of radicalising online audiences.

To summarise, the mapped information ecosystem of al-Qaeda shows that this group adopted a well-balanced but generally uncoordinated approach to online propaganda distribution, relying on multiple Internet layers at the same time. While all AQ branches prioritised encrypted messaging apps, including primarily the *GeoNews* platform, most established at least some presence on the surface web. In this context, the aforementioned decentralisation and lack of coordination of al-Qaeda’s propaganda distribution network may be considered both an advantage and disadvantage from the viewpoint of countering violent extremism on the Internet. On the one hand, the lack of coordination potentially decreases the connectivity and traffic on al-Qaeda’s communication channels, which lowers their potential efficiency. On the other, however, it may increase the resilience of the whole ecosystem to content takedowns. These features must, therefore, be taken into consideration in initiatives aiming to counter al-Qaeda’s strategic communication on the Internet.

*Miron Lakomy is a Professor at the Institute of Political Sciences, the University of Silesia, Poland and a visiting fellow at the ITSTIME research centre in Milan, Italy, within the NAWA Bekker programme (2023-2024). His research primarily focuses on various aspects of political violence and terrorism on the Internet, as well as military conflicts. He is author of Islamic State’s Online Propaganda: A Comparative Analysis (London-New York, Routledge, 2021) and has published five monographs and more than 60 scientific papers in several countries.*

*Acknowledgement: This study was supported by the Polish National Agency for Academic Exchange (NAWA – Narodowa Agencja Wymiany Akademickiej) under the Bekker programme (grant no.: BPN/BEK/2022/1/00002/U/00001).*

## Appendix

*Social network analysis statistics on the top 20 nodes in al-Qaeda's information ecosystem  
(December 2023)*

LABEL	MIRRORS	AVAILABILITY*	IN-DEGREE	OUT-DEGREE	DEGREE	PAGERANK
idDAWAHILALLAH	3	1	4	224	228	0.004162563
idGAZWAH	1	1	5	18	23	0.004178349
idALFIRDAWS	1	1	3	18	21	0.002911913
idFATWAAORG	1	1	7	12	19	0.010621654
idARRIBATMEDIA123	1	1	0	13	13	0.002256761
idOFFDOCPICTURES1	1	1	0	12	12	0.002256761
idCALAMADA	2	1	0	12	12	0.002256761
idNOTESHARE	1	1	0	12	12	0.002256761
idTELEGRAPH05	1	1	2	9	11	0.002469742
idNOTESHAREID9h	1	1	0	10	10	0.002256761
idITC	1	1	1	8	9	0.002272547
idALMIRSAAD	1	1	0	9	9	0.002256761
idISLAMICHISTORY	1	1	0	7	7	0.002256761
idAFNYOUTUBE	1	0	2	4	6	0.002410011
idCHIRPAZZALLAQA	1	2	1	4	5	0.002272547
idNAWAIGH	1	0	1	3	4	0.002272547
idALMAKHTUM	1	0	1	3	4	0.002272547
idGITHUBFAHADHUSSAIN	1	2	0	4	4	0.002256761
idDARULILM	1	1	2	1	3	0.002752071

\*Availability: 0 – inaccessible, 1 – accessible; 2 – not monitored

## Endnotes

- 1 Gabriel Weimann, "www.terror.net. How Modern Terrorism Uses the Internet," *United States Institute of Peace Special Report*, no. 116 (2004), pp. 10-11.
- 2 AQI was one of the first groups to massively utilize execution recordings in online propaganda. Al-Qaeda as a whole was also a pioneer in exploiting other means of radicalizing online audiences, such as video games and e-radios. See, for instance: Martin Harrow, "Video-recorded Decapitations – A seemingly perfect terrorist tactic that did not spread," DIIS Working Paper, no. 8 (2011); Rosanna E. Guadagno et al., "Social Influence in the online recruitment of terrorists and terrorist sympathizers: Implications for social psychology research," *Revue Internationale de Psychologie Sociale*, vol. 23, no. 1 (2010).
- 3 AQ was a pioneer in exploiting social media. See Gabriel Weimann, "Terror on Facebook, Twitter, and YouTube," *The Brown Journal of World Affairs*, vol. 16, no. 2 (2010), pp. 45-54.
- 4 Manuel R. Torres Soriano, "Spain as an Object of Jihadist Propaganda," *Studies in Conflict & Terrorism*, vol. 32, no. 11 (2009).
- 5 See Agnes Hankiss, "Behind the Scenes of Al-Qa'ida's Media Strategy," *Journal of Strategic Security*, vol. 12, no. 2 (2019).
- 6 See Sara Zeiger and Joseph Gyte, "Prevention of Radicalization on Social Media and the Internet," in *Handbook of Terrorism Prevention and Preparedness*, ed. Alex P. Schmid (The Hague: ICCT, 2021).
- 7 See, for instance: Xander Kirke, "Violence and Political Myth: Radicalizing Believers in the Pages of Inspire Magazine," *International Political Sociology*, vol. 9, no. 4 (2015), pp. 283-298; Alastair Reed and Haroro J. Ingram, "Exploring the Role of Instructional Material in AQAP's *Inspire* and ISIS' *Rumiyah*," *EUROPOL*, 26 May 2017, [https://www.icct.nl/sites/default/files/import/publication/reeda\\_ingramh\\_instructionalmaterial.pdf](https://www.icct.nl/sites/default/files/import/publication/reeda_ingramh_instructionalmaterial.pdf).
- 8 Daniel Kimmage, "The Al-Qaeda Media Nexus," *An RFE/RL Special Report*, March (2008).
- 9 Stephane J. Baele, Lewys Bryce, Travis G. Coan, "Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda," *Studies in Conflict & Terrorism*, vol. 46, no. 9 (2023).
- 10 Gabriel Weimann, "www.terror.net. How Modern Terrorism Uses the Internet," *United States Institute of Peace Special Report*, no. 116 (2004), pp. 10-11.
- 11 Bruce Riedel, "Al Qaeda Strikes Back," *Foreign Affairs*, May-June (2007), pp. 24-41.
- 12 Aaron Y. Zelin, *The State of Global Jihad Online. A Qualitative, Quantitative, and Cross-Lingual Analysis* (New York: New America Foundation, 2012).
- 13 Akil N. Awan, "Radicalization on the Internet? The Virtual Propaganda of Jihadist Media and Its Effects," *The RUSI Journal*, vol. 152, no. 3 (2007).
- 14 Maura Conway, "Terrorism and New Media: the cyber battle-space," in *Countering terrorism and insurgency in the 21<sup>st</sup> century*, ed. James Forest (Westport: Greenwood Publishing Group, 2007); Maura Conway, "From al-Zarqawi to al-Awlaki: The Emergence of the Internet as a New Form of Violent Radical Milieu," *Combating Terrorism Exchange*, vol. 2, no. 4 (2012).
- 15 Akil N. Awan, "Radicalization on the Internet? The Virtual Propaganda of Jihadist Media and Its Effects," *The RUSI Journal*, vol. 152, no. 3 (2007), p. 76.
- 16 Alexander Meleagrou-Hitchens, Audrey Alexander, Nick Kaderbhai, "The Impact of digital communications technology on radicalization and recruitment," *International Affairs*, vol. 93, no. 5 (2017), pp. 1233-1249.
- 17 Gabriel Weimann, "Terror on Facebook, Twitter, and YouTube," *The Brown Journal of World Affairs*, vol. 16, no. 2 (2010), pp. 45-54; Gabriel Weimann, "Al-Qa'ida's Extensive Use of the Internet," *CTC Sentinel*, vol. 1, no. 2 (2008).
- 18 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, vol. 38, no. 1 (2015).
- 19 Levi J. West, "#jihad: Understanding Social Media as a Weapon," *Security Challenges*, vol. 12, no. 2 (2016).
- 20 Manuel R. Torres-Soriano, "The Caliphate Is Not a Tweet Away: The Social Media Experience of Al Qaeda in the Islamic Maghreb," *Studies in Conflict & Terrorism*, vol. 39, no. 11 (2016).
- 21 Asma Shakir Khawaja and Asma Hussain Khan, "Media Strategy of ISIS," *Strategic Studies*, vol. 36, no. 2 (2016).

- 22 *Jihadism Transformed: Al-Qaeda and Islamic State's Global Battle of Ideas*, eds. Simon Staffel and Akil Awan (Oxford: Oxford University Press, 2016); Haroro J. Ingram, "Learning from ISIS's Virtual Propaganda War for Western Muslims: A Comparison of Inspire and Dabiq," *NATO Science for Peace and Security Series*, vol. 136 (2017).
- 23 See, for instance: Aleksandra Urman and Stefan Katz, "What they do in the shadows: examining the far-right networks on Telegram," *Information, Communication & Society*, vol. 25, no. 7 (2022).
- 24 Maura Conway and Sean Looney, *Back to the Future? Twenty First Century Extremist and Terrorist Websites* (Luxembourg: Publications Office of the European Union, 2021), p. 3.
- 25 Martin Rudner, "Electronic Jihad: The Internet as Al Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism*, vol. 40, no. 1 (2017).
- 26 Héni Nsaibia and Rida Lyammouri, "The Digital Transformations of Al-Qaeda and Islamic State in the Battle Against Online Propaganda," *Global Network on Extremism & Technology*, 19 May 2021, <https://gnet-research.org/2021/05/19/the-digital-transformations-of-al-qaeda-and-islamic-state-in-the-battle-against-online-propaganda/>.
- 27 Kabir Taneja, "Al Qaeda, Islamic State, and Targeted Online Propaganda Around India's Domestic Political Discourse," *Global Network on Extremism & Technology*, 28 June 2022, <https://gnet-research.org/2022/06/28/al-qaeda-islamic-state-and-targeted-online-propaganda-around-indias-domestic-political-discourse/>.
- 28 Mona Thakkar, "Islamic Translation Centre (ITC): Taking al-Qaeda's Media Jihad Global," *Global Network on Extremism & Technology*, 14 November 2022, <https://gnet-research.org/2022/11/14/islamic-translation-centre-itc-taking-al-qaedas-media-jihad-global/>.
- 29 Data discussed in this paper was collected between 1<sup>st</sup> of July 2023, and 31<sup>st</sup> of December 2023.
- 30 OSINT is usually defined as "intelligence produced by collecting, evaluating and analyzing publicly available information". See Ritu Gill, "What is Open-Source Intelligence," *SANS Institute*, 23 February 2023, <https://www.sans.org/blog/what-is-open-source-intelligence/>.
- 31 See Star Kashman, "Google dorking or legal hacking: From the CIA compromise to your cameras at home, we are not as safe as we think," *Washington Journal of Law, Technology & Arts*, vol. 18, no. 2 (2023).
- 32 URL stands for Unified Resource Locator, which is a reference to an address on the World Wide Web.
- 33 Verification of already unavailable Internet addresses was founded on two separate methods: the use of either Wayback Machine or the Google "cache" command.
- 34 Unavailable websites were not subject to WEBINT but were still included in the database in order to gain as much historical perspective as possible. However, old websites that were inaccessible for years were not considered.
- 35 Due to the adopted way of coding out links to file-sharing services in the database, their availability was not verified. This approach was explained in endnote 36.
- 36 For instance, if a given website consisted of five different links leading to five propaganda items located at mega.nz, they were counted in the database as one record. This approach was adopted because a single website sometimes consists of dozens or hundreds of links leading to a single file-sharing platform, most usually active only for brief periods. Including them as a whole in social network analysis would, therefore, bring no additional value and, at the same time, would negatively impact the clarity of SNA results.
- 37 It means that the database compiled for December 2023 consisted of all URLs collected from July 2023, although updated monthly regarding changes in their accessibility and interconnectedness.
- 38 Gephi is a leading open-source and free social network analysis software that allows exploring and visualizing different types of networks. See: *Gephi – The Open Graph Viz Platform*, Github, <https://gephi.github.io/>.
- 39 It must be stressed that the number of URLs and nodes discussed in the paper is not identical. This is because the quantitative statistics described in the third section include all URLs detected, while individual nodes in SNA could represent more than one Internet address if they were mirrors of the same domain. For instance, the idDAWAHILALLAH node consisted of three URLs, being mirrors of this message board.
- 40 Martin Grandjean, *Gephi – Introduction to network analysis and visualization*, MartinGrandjean, <http://www.martingrandjean.ch/wp-content/uploads/2015/10/Gephi-introduction.pdf>.
- 41 Alan Shaw, *How a Page Rank is calculated in Gephi*, *Strategic Planet*, 31 March 2019, <https://www.strategic-planet.com/2019/12/how-a-page-rank-is-calculated-in-gephi/>.

42 See Ali Fisher, Nico Prucha, and Emily Winterbotham, "Mapping the Jihadist Information Ecosystem. Towards the Next Generation of Disruption Capability," *Global Research Network on Terrorism and Technology*, no. 6 (2019); "Terrorist-Operated Websites," *Tech Against Terrorism*, <https://techagainstterrorism.org/terrorist-operated-websites>. Accessed 22 February 2024.

43 See more in: Arthur Bradley and Deeba Shadnia, *Examining Online Migration to Terrorist and Violent Extremist-Owned Domains* (Washington D.C.: George Washington University, 2022).

44 Lee A. Bygrave, "Article 4(4). Profiling," in *The EU General Data Protection Regulation (GDPR): A Commentary*, eds. Christopher Kuner et al. (New York: Oxford Academic, 2020), pp. 127-131.

45 This is a cumulative amount, including all communication channels, available and unavailable, detected throughout a six-month investigation.

46 This number includes mirrors of AQ's websites.

47 It should be mentioned, however, that al-Qaeda used more websites on The Onion Router. They were just not advertised in their surface web ecosystem. See Miron Lakomy, "Dark web jihad: Exploring the militant Islamist information ecosystem on The Onion Router," *Behavioral Sciences of Terrorism and Political Aggression* (2023). DOI: <https://doi.org/10.1080/19434472.2022.2164326>.

48 Rohan Gunaratna, "Al Qaeda's Stance in the Gaza War," *RSIS Commentary*, 22 February 2024, <https://www.rsis.edu.sg/rsis-publication/rsis/al-qaedas-stance-in-the-gaza-war/>.

49 On AQIS propaganda narratives see: Shafi Md Mostofa, "A Study of Al-Qaeda's Propaganda Narratives in Bangladesh," *Counter Terrorist Trends and Analyses*, vol. 11, no. 2 (2019).

50 Green labels mark accessible websites; red labels mark inaccessible ones. IDs with light blue color were not subject to regular accessibility verification. It should be stressed, however, that most Web 2.0 links were active upon their detection. The size of the labels on the diagram is based on their degree level as well as on the number of detected mirrors. It should also be stressed that the number of nodes in this SNA is slightly different from the statistical data provided above. This is because the SNA treated mirrors of the same website as one node.

51 "Rocket.Chat Remains One of the Most Resilient Platforms for Jihadists," *Flashpoint*, 20 December 2020, <https://flashpoint.io/blog/rocket-chat-remains-resilient-platform-for-jihadists/>.

52 ChirpWire is an encrypted messaging platform that offers increased anonymity for its users. Among others, it does not require a phone number or e-mail address to sign in. It is also known for not exchanging any information about its users with third parties, such as authorities. See "ChirpWire: A virtual safe haven for Bangladeshi extremists," *Dhaka Tribune*, 13 September 2021, <https://www.dhakatribune.com/bangladesh/258292/chirpwire-a-virtual-safe-haven-for-bangladeshi>.

53 See Stuart Macdonald, Connor Rees, Joost S., *Remove, Impede, Disrupt, Redirect: Understanding & Combating Pro-Islamic State Use of File-Sharing Platforms* (Washington D.C.: RESOLVE Network, 2022).

54 On TTP media operations see: Joshua Bowes, "Telegram's Role in Amplifying Tehreek-e-Taliban's Umar Media Propaganda and Sympathiser Outreach," *Global Network on Extremism & Technology*, 30 January 2024, <https://gnet-research.org/2024/01/30/telegrams-role-in-amplifying-tehreek-e-talibans-umar-media-propaganda-and-sympathiser-outreach/>.

55 Mona Thakkar, "Islamic Translation Centre (ITC): Taking Al-Qaeda's Media Jihad Global," *Global Network on Extremism & Technology (GNET)*, 14 November 2022, <https://gnet-research.org/2022/11/14/islamic-translation-centre-itc-taking-al-qaedas-media-jihad-global/>.

56 See more in: Evan Matos, "Al-Shabaab: Information Operations Strategy Overview," *Small Wars Journal*, 29 August 2019, <https://smallwarsjournal.com/jrnl/art/al-shabaab-information-operations-strategy-overview>.

57 More on operations of Shahada News Agency in: "Inside Al-Shabaab's digital propaganda machine," *Disinfo Africa*, 23 November 2023, <https://disinfo.africa/inside-al-shabaabs-digital-propaganda-machine-05cbdb04ed4f>.

58 Moustafa Ayad, Anisa Harrasy, Mohammad Abdullah A., *Under-Moderated, Unhinged and Ubiquitous: Al-Shabaab and the Islamic State Networks on Facebook* (Washington D.C.: Institute for Strategic Dialogue, 2022).

59 See Gabriel Weimann, Natalie Masri, "Spreading Hate on TikTok," *Studies in Conflict & Terrorism*, vol. 46, no. 5 (2023).

60 Stuart Macdonald, Daniel Grinnell, Anina Kinzel and Nuria Lorenzo-Dus, "A Study of Out links Contained in Tweets Mentioning Rumiya," *Global Research Network on Terrorism and Technology*, no. 2 (2019).

- 61 Takedowns of some of these addresses took place at the end of January 2024. However, all HSM-aligned websites were quickly reestablished under new Internet addresses. See “Somalia’s Intelligence Agency shuts down 14 news websites linked to al-Shabab,” *Hiiraan*, 1 February 2024, [https://www.hiiraan.com/news4/2024/Feb/194839/somalia\\_s\\_intelligence\\_agency\\_shuts\\_down\\_14\\_news\\_websites\\_linked\\_to\\_al\\_shabab.aspx](https://www.hiiraan.com/news4/2024/Feb/194839/somalia_s_intelligence_agency_shuts_down_14_news_websites_linked_to_al_shabab.aspx).
- 62 Aofie Gallagher et al., *The Extreme Right on Discord* (Washington D.C.: Institute for Strategic Dialogue, 2021).
- 63 On e-fatwas, see: Gary R. Bunt, *Islam in the Digital Age. E-Jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Press, 2003).
- 64 Amit Chaturvedi, “Osama bin Laden’s ‘Letter to America’ Goes Viral Amid Israel-Hamas War,” *NDTV World*, 17 November, 2023, <https://www.ndtv.com/world-news/explained-osama-bin-ladens-letter-to-america-controversy-and-why-its-viral-4581487>.
- 65 Federico Borgonovo, Giulia Porrino, Silvano Lucini, Alessandro Bolpagni, “Debunking Al Qaeda new Inspire productions,” *ITSTIME*, 1 February 2024, <https://www.itstime.it/w/debunking-al-qaeda-new-inspire-productions-by-f-borgonovo-g-porrino-s-lucini-a-bolpagni/>.
- 66 Islamic State maintained 386 unique communication channels on the surface web at the time. See Miron Lakomy, “The virtual ‘Caliphate’ strikes back? Mapping the Islamic State’s information ecosystem on the surface web,” *Security Journal*, vol. 36 (2023), pp. 791-811.
- 67 See *Online Jihadist Propaganda. 2021 in review* (Luxembourg: Publications Office of the European Union, 2022), p. 23.
- 68 Héni Nsaibia and Rida Lyammouri, “The Digital Transformations of Al-Qaeda and Islamic State in the Battle Against Online Propaganda,” *Global Network on Extremism & Technology*, 19 May 2021, <https://gnet-research.org/2021/05/19/the-digital-transformations-of-al-qaeda-and-islamic-state-in-the-battle-against-online-propaganda/>.
- 69 There are some known cases of Islamic State supporters utilizing Discord, but they have been relatively rare. See “ISIS Supporters Communicate, Compete On Encrypted Discord Channel; TikTok Account Which Promoted Server Recently Suspended,” *MEMRI*, 1 February 2024, <https://www.memri.org/cjlab/isis-supporters-communicate-compete-encrypted-discord-channel-tiktok-account-which-promoted>.