



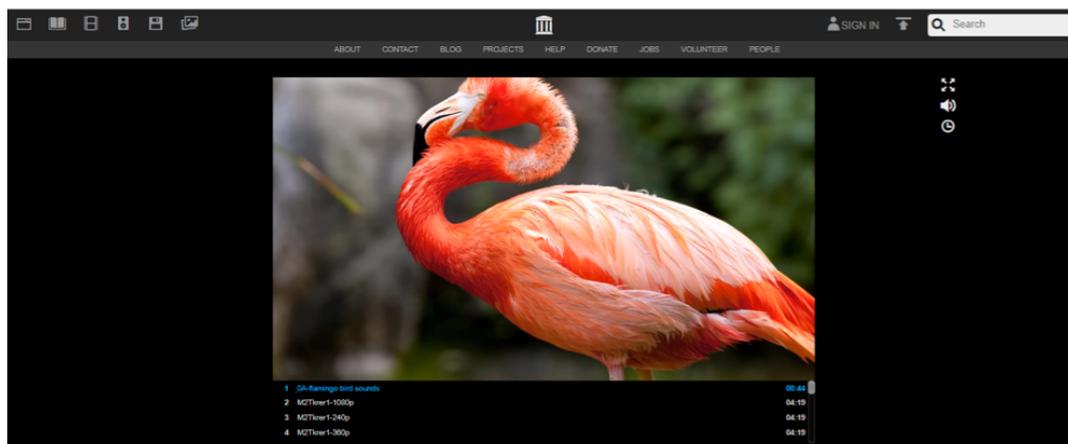
Archive as a Platform for Storing and Disseminating the Propaganda Materials of Al Qaeda and its Supporters

Dr. Michael Barak and Nadine Liv

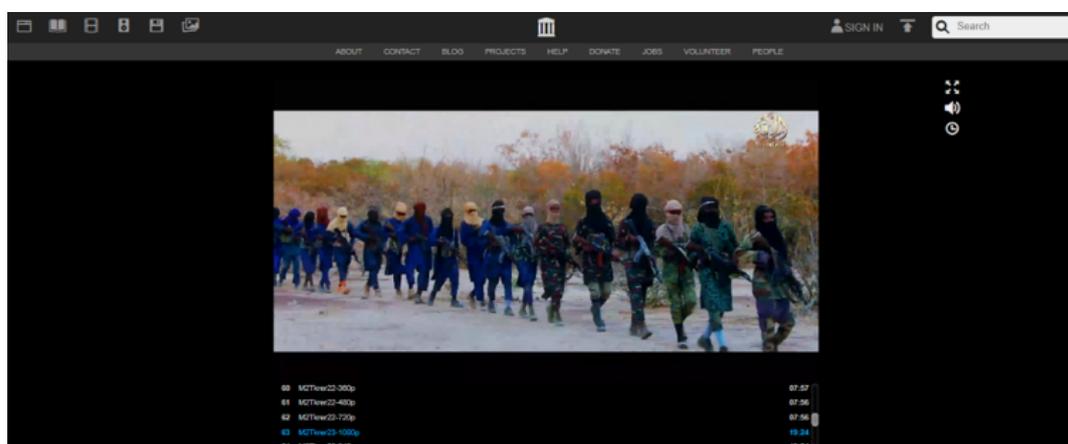
Archive as a Platform for Storing and Disseminating the Propaganda Materials of Al Qaeda and its Supporters

In recent years, social networks have concentrated efforts on removing incitement content following international criticism that they have become an area of activity and a platform for terrorist organizations, such as the Islamic State and Al-Qaeda. However, it is apparent that terrorist organizations are finding ways to overcome the difficulties facing them and are succeeding in outwitting sharing platforms, as recently reflected by the American sharing site, Archive.

In March 2019, propaganda materials related to Al-Qaeda, Hayat Tahrir al-Sham and other terrorist organizations were uploaded to the Archive site, including a series of videos, the transcription of videos into Arabic and audio clips (102 incitement materials).¹ In order to prevent the site's management from identifying them as incitement materials, the terrorist operatives chose to give them a misleading headline, taken from the world of nature: “Flamingo Bird Sounds”. Indeed, the opening film in the series focuses on flamingo bird sounds but it is followed by the organization’s other videos as well as the rest of the incitement materials.



Flamingo Bird Sounds

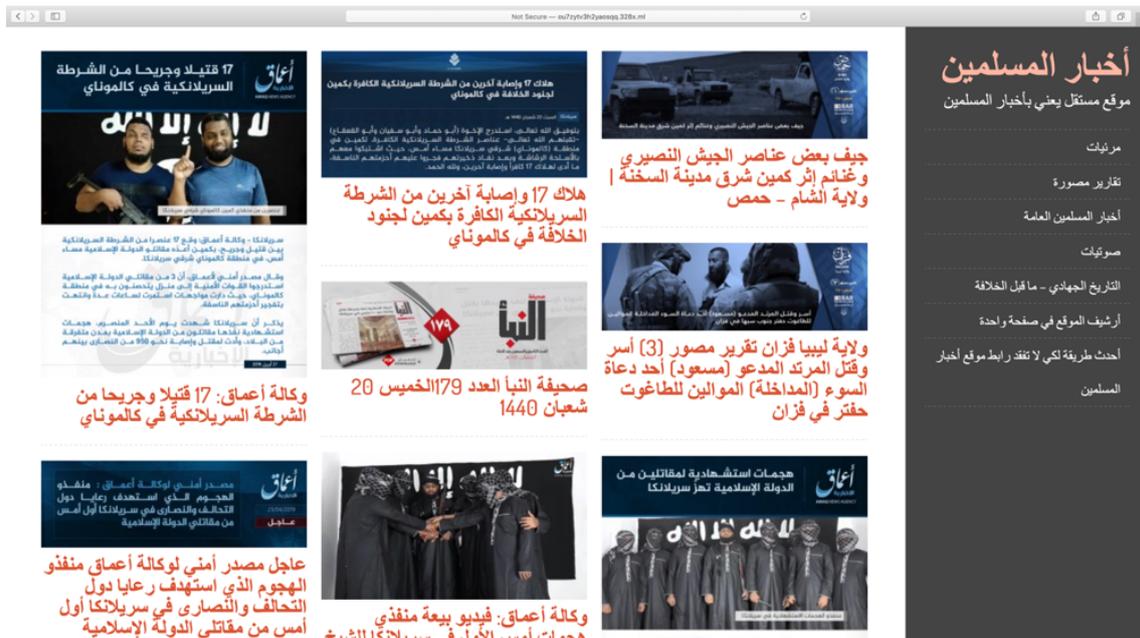


Flamingo Bird Sounds

Top: The opening video, “Flamingo Bird Sounds”; Bottom: A video by Jamaat Nusrat al Islam wal Muslimin, a Salafi-jihadist umbrella organization associated with Al-Qaeda in the Mali region

¹ <https://archive.org/details/elsaharee2>

This is not the first time that terrorism supporters on the Internet have used misleading names to disguise the real purpose of a website. The Akhbar al-Muslimeen website is a supporter of the Islamic State that publishes news about the Caliphate and even raises funds for this purpose. Like many other jihadist websites, this site is also periodically periodically shut down and re-launched. In November 2017, Akhbar al-Muslimeen operated under the address: <http://ou7zytv3h2yaosqq.stopisis.top>; the address bar at the time read "Stop ISIS". Since this is a well-known and significant Islamic State-supporting site, it is reasonable to assume that the use of the term "Stop ISIS" was intended to disguise the real purpose of the site and make it difficult to detect. As of this writing, the Akhbar al-Muslimeen website is active on the darknet and has a site on the visible Web (address in footnotes).²



Screenshot from the Akhbar al-Muslimeen website (April 28, 2019)

While the Akhbar al-Muslimeen domain is privately owned,³ Internet Archive, which operates at archive.org, is a non-profit organization that serves as a platform for uploading user-content that allows people to store information and web pages so that they are not removed from the network. Attempts by various countries to deal with the question of platforms' liability for harmful or illegal content advertised on them have created three types of legal liability models. 1. The absolute immunity model customary in the United States. 2. The strict liability model customary in China and Thailand. 3. The safe harbor model customary in European countries. According to this approach, the agent is protected against liability for user behavior provided that it meets certain criteria. A central but controversial feature of safe harbor doctrines is the creation of "notice and takedown" mechanisms. Under these mechanisms, content hosts remove specific materials when they receive a message claiming that it is illegal.⁴

² As of today (April 28, 2019), the Akhbar al-Muslimeen website is active at the onion address: <http://ou7zytv3h2yaosqq.onion/> and on the visible Web at: <http://ou7zytv3h2yaosqq.328x.ml>

³ According to the Whois registry, the domain of Akhbar al-Muslimeen is registered under the name of the organization, Mali Dili B.V. Point ML administrator from Amsterdam. The domain is defined as a Free Domain and the user information for this domain name is prohibited for distribution or publication. See <https://www.whois.com/whois/328x.ml>

⁴ Eitan Azani & Nadine Liv (2018): A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks, Studies in Conflict & Terrorism, DOI: 10.1080/1057610X.2018.1494874

One example of the safe harbor model is the European E-Commerce Directive, which offers different levels of immunity to a platform determined by the nature of the agent’s activity.⁵ Another example of this model is the German Network Enforcement Act.⁶ Germany passed an innovative law imposing fines of up to five million Euros (which could accumulate to 50 million Euros) on Internet service providers that do not remove illegal content uploaded to their platforms by users. The law is designed to improve enforcement on social networks and it states that providers must remove content within 24 hours of being reported, in parallel to their obligation to create user-friendly reporting mechanisms; its disadvantage is that it applies only to providers that operate on a for-profit basis, meaning that it does not apply to Archive. *Both the E-Commerce Directive and the German law reflect a passive stance, since they do not obligate providers to locate for themselves content that they allow to be published;* the laws rely on user-reporting mechanisms.

Since the current voluntary mechanism does not adequately address the phenomenon of online terrorist propaganda, the European Commission published a bill in September 2018 to require Internet service providers to remove content within one hour of receiving a report of its illegality. An Internet provider that does not comply with the new law will face penalties of up to 4% of its annual turnover,⁷ similar to the established sanction of non-compliance with GDPR regulations.⁸ The main points of the bill are: the duty to remove content within one hour; the formulation of a clear definition of pro-terrorist content; the obligation to use proactive means to locate pro-terrorist content; increased cooperation between Internet service providers and countries, and the establishment of contact points for the implementation of the Notice and Takedown mechanism 24/7; the establishment of strong judicial mechanisms to protect against unwarranted reports; increased transparency and accountability; the imposition of deterrent financial penalties.⁹



One hour takedown



A clear definition



Proactive measures



Increased cooperation



Strong safeguards



Transparency and accountability



Financial penalties

⁵ <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>

⁶ Act to Improve Enforcement of the law in social networks (Network Enforcement Act). (2017). Available online: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

⁷ <https://www.theguardian.com/media/2018/sep/13/social-media-firms-could-face-huge-fines-over-terrorist-content> ; <https://www.theverge.com/2019/3/21/18274201/european-terrorist-content-regulation-extremist-terreg-upload-filter-one-hour-takedown-eu>

⁸ <https://eugdpr.org/the-regulation>

⁹ http://europa.eu/rapid/press-release_IP-18-5561_en.htm

In response to the publication of the bill, the Internet Archive team published a blog stating that at the beginning of April, the site received 550 unwarranted reports of pro-terrorist content being published on the site. The reports, which were received by the French Internet Referral Unit (IRU) using Europol's reporting platform, inadvertently identified content as pro-terrorist propaganda, while the Archive team presents the blog as innocent content. This included the reporting of academic articles, US government reports and user-generated content. One specific report that demanded the removal of pro-terrorist content within the "Notice and Takedown" mechanism referred to content that interpreted the Quran as "incitement to commit acts of terrorism." The blog team claims that these reports came from European law and enforcement agencies, demonstrating that the bill violates freedom of expression.¹⁰

The European bill follows GDPR regulations, which came into force in May 2018,¹¹ and it reflects dual tension. One level is the tension between American culture, which respects individual rights, especially freedom of expression and property, and the more conservative European culture. A second level is the tension between nation-states and non-state actors, such as corporations and international organizations. On both levels, there is a trend of restraint on the part of Europeans in the global Internet arena.

¹⁰ <https://blog.archive.org/2019/04/10/official-eu-agencies-falsely-report-more-than-550-archive-org-urls-as-terrorist-content/>

¹¹ <https://eugdpr.org/the-regulation/>