The Digital Battlefield: How Terrorists Use the Internet and Online Networks for Recruitment and Radicalization

Aaron Y. Zelin
Gloria and Ken Levy Senior Research Fellow
Washington Institute for Near East Policy

Testimony before the House Committee on Homeland Security, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence Subcommittee
March 4, 2025

Thank you Mister Chairman and members of the committee for giving me the opportunity to testify today on how terrorists use the internet and online networks for recruitment and radicalization. This is an important topic in light of the recent New Years Eve attack in New Orleans. On that day, Shamsud-Din Jabbar was killed in a shootout with police after driving a Ford pickup truck with an Islamic State (IS) flag through a New Year's crowd on Bourbon Street, killing fourteen and injuring fifty-seven. Prior to the attack, he visited New Orleans twice, on October 31 and November 10 last year. During his October trip, he recorded a video of the French Quarter using smart glasses from Meta. Jabbar also expressed support for IS in videos posted to Facebook, researched the December 2016 car attack at a Christmas market in Germany, and pledged allegiance to the group shortly before the attack.[1]

The following week, the Islamic State wrote an editorial in its weekly newsletter called *al-Naba*, titled "We Were There!," where it gloated over Jabbar's attack.[2] In the editorial, it highlighted the group's influence and incitement capabilities. The piece also boasted that the perpetrator used American technology, referring to the Meta smart glasses he employed to conduct reconnaissance. The piece concluded by once again urging Muslims in Europe and the United States to carry out more terrorist attacks. Highlighting how IS uses one attack to push for a new one and creates a virtuous cycle from its perspective. That is why it is not surprising that Jabbar himself, prior to his own attack, researched a prior IS attack: the December 2016 Christmas Market car ramming attack in Berlin that killed twelve and injured forty-eight.[3]

Jabbar's attack also falls in line with Islamic State instructional attack planning. In particular, in mid-November 2016, in IS's English language magazine at the time called *Rumiyah*, it released an article titled "Just Terror Tactics" that provided guidance on the best way to kill as many of their enemies as possible.[4] It says "the type of vehicle most appropriate for such an operation is a large load-bearing truck." Jabbar did this with the pickup truck. The article also highlights that if one doesn't have the wealth, it suggests renting a vehicle, again Jabbar did this as well. Further, it suggests specific targets, with one of them being pedestrian-congested streets, again something

---

[1] "IS-Inspired Attacker Killed After Driving Through Crowd in New Orleans," *Islamic State Worldwide Activity Map*, January 1, 2025, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/4029.
[2] The Islamic State, "al-Naba' Newsletter Issue #477," January 9, 2025, https://jihadology.net/2025/01/09/new-issue-of-the-islamic-states-newsletter-al-naba-477.
[3] "Attack on Berlin Christmas Market," *Islamic State Worldwide Activity Map*, December 20, 2016, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/989.
[4] The Islamic State, "Rome Magazine Issue #3," November 11, 2016, https://jihadology.net/2016/11/11/new-release-of-the-islamic-states-magazine-rome-3.

Jabbar followed. The article also suggested that an attacker can use a secondary weapon. In this case, Jabbar placed two coolers with explosive devices at two other locations in the city's French Quarter. Finally, the article tells prospective attackers to find "an appropriate way… for announcing one's allegiance to the Caliphate." Not only did Jabbar do this with his pledge of allegiance on Facebook, but also by raising the Islamic State flag on the truck he used during the attack. This all shows that while this attack occurred in 2025, in many ways examples and guidance literature from almost a decade ago that remains accessible online has a long shelf life and that not enough is still being done to make sure that potential attackers do not have access to such content online.

Background

Unfortunately, none of this is new. Since the commercial internet came about, jihadis have been there in parallel. The first known jihadi presence on the Internet can be traced back to 1991, with the Islamic Media Center (IMC). al-Qaeda's official debut dates to February 2000, with the creation of maalemaljihad.com. This was followed in March 2001 by alneda.com, which was active through mid-July 2002.[5] In the summer of 2001, al-Qaeda created a media arm, al-Sahab Media Production Establishment, and released its first video, "The Destruction of the American Destroyer [USS] Cole." Several other websites at the time were not directly connected with al-Qaeda, but sympathized with its jihadi worldview, including Azzam Publications, al-Tibyan Publications (which had one of the earliest jihadi-leaning, English-language, interactive forums), and Sawt al-Qawqaz.[6]

Since then, the jihadi movement has taken advantage of new online technologies at every turn to spread its message, recruit individuals to fight abroad, incite or help plan attacks, and raise money. For example, the onset of interactive forums in the mid-2000s, concurrent with the rise of Abu Mus'ab al-Zarqawi and the Iraq jihad, shattered the elitist nature of jihadi communications. Web forums still offered administrators (who were often directly connected with al-Qaeda) extensive influence over what was posted because they could delete threads or ban members. But individual forum members, not directly connected to al-Qaeda, could not only view what was posted by administrators, but also comment and post their own content as well.[7] Mustafa Setmariam Nasir, better known by his nom de guerre Abu Mus'ab al-Suri, called for producing jihadi media in languages other than Arabic, including English, and devising messages that appealed more to the masses. The popularization of the online jihadi movement empowered organizations dedicated to translating material, most of which was still produced in Arabic. The Global Islamic Media Front (GIMF), established in August 2004, was a key innovator in this regard, and could trace its roots all the way back to June 2001.[8]

After this, Web 2.0 innovations and the creation of social media platforms (blogging, Facebook, YouTube, and Twitter) flattened control over the production of online jihadi media. Social media

---

[5] Abdel Bari Atwan, The Secret History of al-Qaeda, London: Saqi Books, 2006, pp. 127; Patrick Di Justo, "How Al-Qaida Site Was Hijacked," Wired Online, August 10, 2002, http://www.wired.com/culture/lifestyle/news/2002/08/54455.

[6] For more see: Hanna Rogin, "Al-Qaeda's online media strategies- From Abu Reuter to Irhabi 007," Norwegian Defence Research Establishment (FFI), January 12, 2007, http://rapporter.ffi.no/rapporter/2007/02729.pdf

[7] Gordon Corera, "Al-Qaeda's 007," The Times, January 16, 2008, https://www.thetimes.com/article/al-qaedas-007-c2sx2r5bdgc.

[8] Rogin, "Al-Qaeda's online media strategies," pp. 56.

platforms enabled global jihadi entrepreneurs to share news items, original articles and essays, tribute videos, and anashid (Islamically-sanctioned a cappella music). The newer technologies, at that time, lowered the bar for participation, making the involvement of low-level or non-jihadis in online conversation a new feature of the global jihadi movement. Those so inclined could talk about jihad all day on the Web, even if they were geographically dispersed. This was not possible beforehand.[9]

As a consequence, when the Islamic State eclipsed al-Qaeda in the mid-2010s they used this to deadly effect.[10] To further their message they would create innocuous hashtag aggregators yet only post their propaganda, create hashtag targeting bots, have multiple backup accounts in case they were taken down, and build the Fajr al-Basha'ir app.[11] The latter let members and supporters connect to it and thereby whenever the app tweeted something it would automatically be posted by those that signed up for it onto their own account. The breadth of IS's online Twitter campaign was unprecedented. However, this would not last, due to massive complaints by countries reeling from the Islamic State's on-the-ground successes in Iraq and Syria and tens of thousands of foreign fighters being recruited to join their ranks.[12]

That led Twitter (and all the other main technology companies) to originally establish their Trust and Safety teams. This led to a crackdown on IS networks in 2015 by going after IP addresses and those within their follower networks.[13] This helped also establish the Global Internet Forum to Counter Terrorism (GIFCT), which established a consortium of Western technology companies to work together to take down terrorist content by sharing digital fingerprints (or hashes) of different types of content (pictures, audio, videos, etc.).[14] As a consequence, IS and the jihadi movement shifted to the encrypted messaging application Telegram in August/September 2015, which also had a broadcast feature that allowed anyone to follow official IS and other groups' channels.[15] Telegram never had the same utility as Twitter since it couldn't just reach anyone randomly as Twitter had, one had to know where to go ahead of time to find the content. This takedown cycle eventually happened again on Telegram when Europol convinced the company to go after jihadi accounts, which led to a huge purge in November

---

[9] Aaron Y. Zelin, "The State of Global Jihad Online," *New America Foundation*, February 2013, https://www.newamerica.org/future-security/policy-papers/the-state-of-global-jihad-online.

[10] Aaron Y. Zelin, "Picture Or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism*, Volume 9, Number 4, August 2015, https://www.jstor.org/stable/26297417?seq=1.

[11] J.M. Berger, "How ISIS Games Twitter," *The Atlantic*, June 16, 2014, https://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856.

[12] Michael Isikoff, "Twitter under pressure to act more aggressively against terrorists," February 18, 2015, https://www.yahoo.com/news/amphtml/politics/twitter-under-pressure-to-act-more-aggressively-114435221601.html.

[13] "An update on our efforts to combat violent extremism," *Twitter*, August 18, 2016, https://blog.x.com/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.

[14] "Global Internet Forum to Counter Terrorism: an update on our efforts to use technology, support smaller companies and fund research to fight terrorism online," June 18, 2018, https://gifct.org/2018/06/18/global-internet-forum-to-counter-terrorism-an-update-on-our-efforts-to-use-technology-support-smaller-companies-and-fund-research-to-fight-terrorism-online.

[15] "IS exploits Telegram mobile app to spread propaganda," *BBC News*, October 7, 2015, https://www.bbc.com/news/technology-34466287.

2019.[16] As a consequence, both IS and AQ networks established their own decentralized forums using block chain technology on RocketChat to make it more difficult for content to be taken down. To this day, both RocketChat forums remain online.[17]

Harnessing The Internet Today

While al-Qaeda still operates its RocketChat forum, the Islamic State's online ecosystem and infrastructure is far more diverse and sophisticated than only its own RocketChat forum. In addition to that, IS also established its own Cloud-based archive of its historical propaganda called Obedient Supporters.[18] Moreover, in recent years, it has also established a number of traditional websites. In some ways, a return to the beginning of the internet in the 1990s and early 2000s since it was much harder to operate on mainstream social media platforms. To make these websites more difficult to take down, they jump domain names often using different country codes to hide in plain sight. To make it even more complicated, they have also developed mirrored versions of these websites on the Dark Web, which can only be accessed using a Tor browser and an Onion router link. Each website also provides a specific purpose to try and break up where all the content is so as to disperse it to make their online network more resilient over time. They do this by having a repository website called Fahras al-Ansar, which is based in South Africa right now at least, that shares the last links for each site that are currently available online on the surface web and on the Dark Web.[19] The main website that has been most active recently is called Sah al-Wagha, which shares the latest IS attack claims of responsibility, videos, and weekly newsletter *al-Naba*.[20]

The latter website is where one would find official media content from IS, which comes directly from its Central Media Diwan (Administration), which today includes al-Furqan Media, Amaq News Agency, Provincial Media Centers, among other lesser used outlets today. Other websites and the RocketChat forum also disseminate "unofficial" auxiliary propaganda. These are not created by the Central Media Diwan, but by members of the group in their own capacity and work with online supporters of the group. These include media outlets such as al-Batar Media, al-Saqri Media, al-Dir'a al-Sunni Media, Sirat al-Khilafah, al-'Adilat Media, etc. The next layer under this is IS's translation collective, called Fursan al-Tarjuma, which helps disseminate all of its official propaganda into dozens of languages.[21] Again, this is "unofficial" insofar as the Central Media Diwan is not involved, but rather members of the group in their own capacity and online supporters take part in it. These outlets today include Halammu (English), Nida al-Haqq

---

[16] "Europol and Telegram take on terrorist propaganda online" *Europol*, November 22, 2019, https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.

[17] Peter King, "Analysis: Islamic State messaging on RocketChat still online after seven months," *BBC Monitoring*, August 9, 2019, https://monitoring.bbc.co.uk/product/c200zjhz; "Veteran jihadist outlet uses RocketChat for al-Qaeda propaganda," *BBC Monitoring*, December 6, 2019, https://monitoring.bbc.co.uk/product/c201akwr.

[18] Miron Lakomy, "In the digital trenches: Mapping the structure and evolution of the Islamic State's information ecosystem (2023–2024)," *Media, War & Conflict*, August 24, 2024, https://journals.sagepub.com/doi/10.1177/17506352241274554.

[19] Ibid.

[20] "Briefing: New archive of official IS material appears online," *BBC Monitoring*, October 28, 2024, https://monitoring.bbc.co.uk/product/b0002o3c.

[21] Lucas Webber and Daniele Garofalo, "Fursan al-Tarjuma Carries the Torch of Islamic State's Media Jihad," *Global Network on Extremism and Technology*, June 5, 2023, https://gnet-research.org/2023/06/05/fursan-al-tarjuma-carries-the-torch-of-islamic-states-media-jihad.

(Urdu), al-Aza'im (Pashto, Uzbek, Tajik, Farsi), Markaz al-Nur (French), al-Tamkin (Bengali, Indonesian), Arshad (Russian), al-Bahiriyah (Hausa), al-Basha'ir (Dhivehi), Maydan (Turkish), Rastara (Kurdish), Fakhr al-Ummah (Albanian), Sawt al-Andalus (Spanish), and al-Qital (Hindi). Illustrating the breadth of languages IS has access to for spreading its message, ideology, and incitement all across the world. At the height of IS's territorial control in Iraq and Syria a decade ago, they translated their content into even more languages, illustrating that even if it is relatively weaker today, it is still quite resilient and there are enough people interested in its worldview to assist in these endeavors.

Emerging Tech: Crypto, Live Streaming, and AI

Beyond traditional propaganda efforts to recruit and incite, due to the greater reach and ease of use of cryptocurrencies, there has been a huge uptick in its use by jihadi groups, its supporters, and those involved in attacks abroad. For example, on an official level, beginning in December 2023, the Islamic State's Khurasan Province (ISKP), based out of Afghanistan and Pakistan, began promoting its own wallet for the Monero cryptocurrency to help fund its efforts locally and also as a conduit to pay for external operations abroad. These promotions for ISKP's Monero wallet first appeared in its official English-language magazine the *Voice of Khurasan*.[22] The utility of a cryptocurrency like Monero is that it is more difficult to track the movement of money through the wallet like other cryptocurrencies. Thus making it more secure, which in of itself for normal activity, on the surface, would be fine, but for a terrorist group, not ideal. Since then, ISKP has promoted a number of different wallets in subsequent issues of its *Voice of Khurasan* magazine. This is not theoretical either, back in April 2024, the FBI arrested eighteen-year-old Alexander Scott Mercurio who pledged allegiance to the Islamic State and plotted to attack churches in Coeur d'Alene, Idaho. As part of this plot, he confided in an undercover agent that he wanted to donate his money ($11,000) ahead of this attack to ISKP using Monero.[23] A similar case in the UK occurred as well with an even larger donation attempt of £16,000.[24] Based on data collected for my Islamic State Worldwide Activity map, since 2015, there have been 36 arrest cases globally related to jihadi use of cryptocurrency, with 13 of them happening in 2024 alone, illustrating a huge uptick in only the past year. And these cases are only known cases that have come through judicial manners, not those that were not detected.

Beyond traditional American social media platforms, there has also been a rise in use of TikTok by supporters of IS. This is not surprising since it has become ubiquitous amongst Gen Z individuals. While the trend likely began earlier, based on data from my Islamic State Worldwide Activity map, there have been 15 arrest cases that began in 2023 that have shown the arrestee to have been involved in one way or another with IS propaganda on TikTok, either sharing it themselves or watching it. Just last week, Minneapolis resident Abdisatar Ahmed Hassan was arrested and charged for attempting to provide material support to the Islamic State. As part of the investigation, he actually praised the perpetrator of the IS-inspired attack in New Orleans on

---

[22] The Islamic State's Wilayat Khurasan, "Voice of Khurāsān Magazine Issue #31," *al-Aza'im Media*, December 22, 2023, https://jihadology.net/2023/12/22/new-magazine-issue-from-the-islamic-states-wilayat-khurasan-voice-of-khurasan-31.

[23] "Idaho Teen Arrested For Plotting Church Attacks," *Islamic State Worldwide Activity Map*, April 6, 2024, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/3228.

[24] "Luton Man Arrested for Sending Cryptocurrency to ISKP," *Islamic State Worldwide Activity Map*, March 13, 2024, https://www.washingtoninstitute.org/islamicstateinteractivemap/#view/4191.

TikTok on January 1, 2025.[25] Highlighting how one attack could inspire others to either plot their own attack or to try and travel abroad to fight with IS in a warzone, as Hassan attempted to do with IS in Somalia.

There are also other technological related issues that terrorists could attempt to exploit, including live streaming their attack. It could have had much more of a psychological effect nationally, if the New Orleans attacker had live streamed his attack on his Meta glasses through Facebook instead of only using it for reconnaissance purposes. However, such use is not unprecedented. Back in June 2016, Islamic State attacker Larossi Abballa, broadcast the aftermath of his attack on a French police captain and his partner, in real time on Facebook Live and remained online for almost 12 minutes.[26] A copy of the recording was downloaded and later reposted via IS's official media outlet Amaq News Agency, since it was taken down from Facebook 11 hours after its recording.

In addition to that, there are also worries that Generative Artificial Intelligence (AI) could be exploited by terrorists. However, thus far, at least among jihadis, there has not been much evidence that they have used it yet to deadly ends. However, that does not necessarily mean they couldn't in the future. For now, it has mainly been used by followers to create online graphics to promote the same kind of content they would have previously using Photoshop. Even if this appears to have less stakes, it does lower the bar for those to make content and interact more deeply with the ideology and worldview since one doesn't need the same level of skill set as someone that knows how to use Photoshop, something which takes training and a lot more time. However, there have been inchoate conversations by IS supporters on Rocketchat beginning a few weeks ago, related to the Chinese application Deepseek and how they could potentially exploit it. It is too soon, however, to know how that might evolve.[27]

Moderation Backsliding

Beyond the specifics of how terrorists might exploit technology, policies related to technologies and platforms also have a role in providing space or making it very difficult to use. As noted above, beginning in 2015, there was a much greater focus by major technology companies to moderate their platforms so that terrorists couldn't exploit them. While the moderation was in no way perfect vis-a-vis jihadis online, overall, it curbed usage on mainstream platforms at a good enough rate that it was not noticeably affecting random people as it easily had in the 2013-15 time period. However, in recent years, due to controversies related to alleged censorship within the West politically, there has been a backlash to moderating content even if it is extremist in nature. As a consequence, beginning with Elon Musk's purchase of Twitter, which is now X, the level of content moderation in general, and related to the jihadi movement specifically has

---

[25] "Minneapolis Man Arrested for Attempting to Provide Material Support to ISIS," *Department of Justice*, February 28, 2025, https://www.justice.gov/usao-mn/pr/minneapolis-man-arrested-attempting-provide-material-support-isis.

[26] Caitlin Dewey and Sarah Parnass, "For the first time, an alleged terrorist has broadcast a confession in real time on Facebook Live," *Washington Post*, June 14, 2016, https://www.washingtonpost.com/news/the-intersect/wp/2016/06/14/for-the-first-time-an-alleged-terrorist-has-broadcast-a-confession-in-real-time-on-facebook-live.

[27] "Users on pro-IS chat group begin discussing DeepSeek," *BBC Monitoring*, February 19, 2025, https://monitoring.bbc.co.uk/product/b0003e3h.

backslid.[28] It should not be overblown, however, since it is not as widespread as it was in 2015 prior to the offensive policies against jihadis, but in a relative sense, there is greater space for jihadis to exploit platforms in recent years.[29] It should be noted that this is not just an issue with X, but has Mark Zuckerberg's Meta social media platforms as well, including Facebook, Instagram, and WhatsApp as well as the aforementioned TikTok. Yet unlike a decade ago, much of these relative capabilities by IS networks online are by supporters of the group and not at the official level.[30]

Recommendations

- The U.S. government should urge technology companies and social media platforms to redouble their efforts at content moderation related to the jihadi movement. In particular, beyond only Arabic and English content, these platforms need to beef up their moderation in languages that are increasingly used as the center of gravity of the jihadi movement online such as multiple languages in Africa and Central Asia for example.
- Although there have been recent calls to cut funding and jobs across the U.S. government, cutting ones related to tracking online jihadi recruitment and attack plotting could undermine future security and lead to greater risks at home and abroad. At a time, when greater resources are put toward power competition and less resources are given to counterterrorism, eliminating even more resources in this field could provide more opportunities for adversarial jihadis and entrepreneurial supporters of the movement to take advantage and attack the homeland more easily.
- While there have been many discussions about the utility of using AI in terrorism investigations and content moderation online, it still does not replace human expertise and contextual clues on these issues whether within tech companies or the U.S. government.
- The U.S. government should also urge GIFCT to establish a whitelist for researchers that work on these sensitive issues so that their accounts do not get mistakenly taken down while actual terrorist accounts are targeted. This has been a problem in the past and should be resolved.[31]

---

[28] "Musk admitted to firing 80% of Trust and Safety Engineers at Twitter," January 12, 2024, https://sarajevotimes.com/musk-admitted-to-firing-80-of-trust-and-safety-engineers-at-twitter; "Musk's Twitter has dissolved its Trust and Safety Council," *Associated Press*, December 12, 2022, https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk.

[29] Moustafa Ayad, "Islamic State Supporters on Twitter: How is 'New' Twitter Handling an Old Problem?," *Global Network on Extremism and Technology*, November 18, 2022, https://gnet-research.org/2022/11/18/islamic-state-supporters-on-twitter-how-is-new-twitter-handling-an-old-problem.

[30] Moustafa Ayad, "Teenage Terrorists and the Digital Ecosystem of the Islamic State," *CTC Sentinel*, Volume 18, Issue 2, February 2025, https://ctc.westpoint.edu/teenage-terrorists-and-the-digital-ecosystem-of-the-islamic-state.

[31] Aaron Y. Zelin, ""Highly nuanced policy is very difficult to apply at scale": Examining researcher account and content takedowns online," *Policy & Internet*, Volume 15, Issue 4, December 2023, https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.374.