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

Aaron Y. Zelin,
Levy Senior Fellow,
The Washington Institute for Near East Policy

Testimony submitted to the U.S. House Committee on Homeland Security,
Subcommittee on Counterterrorism and Intelligence

March 4, 2025

Thank you Mr. 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 Year's 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 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, IS wrote an editorial in its weekly newsletter *al-Naba* bearing the title "We Were There!" and gloating over Jabbar's attack.[2] The editorial highlighted the group's influence and incitement capabilities. It 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. This is why it is not surprising that Jabbar himself 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 IS instructional attack planning. In particular, in mid-November

[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] Islamic State, *al-Naba* newsletter, issue no. 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.

2016, in an English-language IS magazine called *Rumiyah*, the group released an article titled "Just Terror Tactics"[4] that provided guidance on the best way to kill as many enemies as possible:

- It advised that "the type of vehicle most appropriate for such an operation is a large load-bearing truck," similar to Jabbar's pickup.
- It noted that if attackers do not have sufficient wealth to buy such a vehicle, they can rent one instead; Jabbar did this as well.
- It suggested specific targets such as pedestrian-congested streets; Jabbar followed suit.
- It suggested that an attacker can use a secondary weapon. In Jabbar's case, two coolers with explosive devices were placed at two other locations in the city's French Quarter.
- It told prospective attackers to find "an appropriate way…for announcing one's allegiance to the Caliphate." Jabbar did so not only with his pledge of allegiance on Facebook, but also by raising the IS flag on his truck during the attack.

All of these findings show that although the attack occurred just weeks ago, in many ways it stemmed from examples and guidance literature from almost a decade ago, which remains accessible online and has a long shelf life. Not enough is 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, jihadists have been there in parallel. The first known jihadist 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 summer 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 jihadist worldview, including Azzam Publications, al-Tibyan Publications (which had one of the earliest jihadist-leaning, English-language interactive forums), and Sawt al-Qawqaz.[6]

Since then, the jihadist 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 Musab al-Zarqawi and the Iraq jihad, shattered the elitist nature of jihadist 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 Musab al-Suri, called for producing jihadist media in languages other than Arabic, including English, and devising messages that appealed more to the masses. The popularization of the online jihadist movement empowered organizations dedicated to translating material, most of

---

[4] Islamic State, "Rome Magazine Issue #3," November 11, 2016, https://jihadology.net/2016/11/11/new-release-of-the-islamic-states-magazine-rome-3.

[5] Abdel Bari Atwan, *The Secret History of al-Qaeda* (London: Saqi Books, 2006), p. 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.

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 jihadist media. Social media platforms enabled global jihadist entrepreneurs to share news items, original articles and essays, tribute videos, and *nashid* (religiously sanctioned a cappella music). The newer technologies also lowered the bar for participation, making the involvement of low-level or non-jihadists in online conversation a new feature of the global jihadist 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 IS eclipsed al-Qaeda in the mid-2010s, the group used these innovations to deadly effect.[10] To further their message, members created innocuous hashtag aggregators for their propaganda, activated hashtag targeting bots, established multiple backup accounts in case they were taken down, and built the Fajr al-Bashair app.[11] Whenever the app tweeted something, it would automatically be reposted by the individual accounts of members who signed up for it. Indeed, the breadth of the IS Twitter campaign was unprecedented.

This would not last, however, due to massive complaints by countries reeling from the group's on-the-ground successes in Iraq and Syria and the tens of thousands of foreign fighters being recruited to join its ranks.[12] That led Twitter (and all the other main technology companies) to establish their original "trust and safety" teams. This in turn led to a 2015 crackdown on IS networks that went after IP addresses and those within their follower networks.[13] It also helped establish the Global Internet Forum to Counter Terrorism (GIFCT), which organized 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 jihadist 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

---

[8] Rogin, "Al-Qaeda's online media strategies," p. 56.
[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*, vol. 9, no. 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," Yahoo News, February 18, 2015, https://www.yahoo.com/news/amphtml/politics/twitter-under-pressure-to-act-more-aggressively-114435221601.html.
[13] Twitter/X, "An update on our efforts to combat violent extremism," 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.

find the content. This takedown cycle eventually happened again on Telegram when Europol convinced the company to go after jihadist accounts, which led to a huge purge in November 2019.[16] As a consequence, both IS and al-Qaeda networks established their own decentralized forums using blockchain technology on Rocket.Chat to make it more difficult for content to be taken down. To this day, both Rocket.Chat forums remain online.[17]

Harnessing The Internet Today

While al-Qaeda still relies substantially on its Rocket.Chat forum, the Islamic State's online ecosystem and infrastructure is far more diverse and sophisticated. In addition to Rocket.Chat, IS also established its own cloud-based archive of historical propaganda called "Obedient Supporters."[18] Moreover, the group established a number of traditional websites in recent years after it became much harder to operate on mainstream social media platforms —in some ways, a return to the beginning of the internet in the 1990s and early 2000s. To make these websites more difficult to take down, IS jumps domain names, often using different country codes to hide in plain sight. To make tracking even more complicated, the group has 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 fulfills a very specific purpose—a tactic intended to break up the group's content and make its online network more resilient over time. IS manages this network via a repository website called Fahras al-Ansar. Based in South Africa as of this writing, this repository shares the last links for each IS site that is currently available on the surface web and the dark web.[19] The site that has been most active recently is called Sah al-Wagha, which shares the latest IS attack claims and videos along with the weekly newsletter *al-Naba*.[20] Sah al-Wagha is where one would find official media content directly from the Islamic State's Central Media Diwan (administration), which today includes al-Furqan Media, Amaq News Agency, Provincial Media Centers, and various lesser-used outlets.

Other websites and the Rocket.Chat forum also disseminate "unofficial" auxiliary propaganda. These are created not by the Central Media Diwan, but by members of the group in their own capacity and in tandem with online supporters. These include outlets such as al-Batar Media, al-Saqri Media, al-Dira al-Sunni Media, Sirat al-Khilafah, al-Adilat Media, and so forth.

The next layer under this is the Islamic State's translation collective, 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; members of the group conduct this activity in their own

---

[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.

capacity, and online supporters take part in it. Illustrating the breadth of languages that IS can access to spread its message, ideology, and incitement all across the world, these translation outlets include Halammu (English), Nida al-Haqq (Urdu), al-Azaim (Pashto, Uzbek, Tajik, Farsi), Markaz al-Nur (French), al-Tamkin (Bengali, Indonesian), Arshad (Russian), al-Bahiriyah (Hausa), al-Bashair (Dhivehi), Maydan (Turkish), Rastara (Kurdish), Fakhr al-Ummah (Albanian), Sawt al-Andalus (Spanish), and al-Qital (Hindi). At the height of the group's territorial control in Iraq and Syria a decade ago, IS translated its content into even more languages. Yet even today when it is relatively weaker, IS still has enough people interested in its worldview to assist in these wide-ranging media and translation endeavors.

Emerging Tech: Crypto, Live Streaming, and AI

Beyond traditional propaganda efforts to recruit and incite, the greater reach and ease of use of cryptocurrencies has led to a huge uptick in their use by jihadist groups, supporters, and those involved in attacks abroad. For example, beginning in December 2023, the Islamic State's Khorasan Province (ISKP), based out of Afghanistan and Pakistan, began promoting its own wallet for the Monero cryptocurrency to help fund its efforts locally and provide a conduit to pay for external operations abroad. These promotions first appeared in ISKP's official English-language magazine *Voice of Khorasan*.[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 is fine for normal activity but problematic when used by a terrorist group.

Since then, ISKP has promoted a number of different wallets in subsequent issues of *Voice of Khorasan*. The operational use of such wallets for terrorist attacks is not theoretical, either. In April 2024, the FBI arrested eighteen-year-old Alexander Scott Mercurio, who had pledged allegiance to IS 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 $11,000 of his money to ISKP in advance using Monero.[23] A similar case occurred in the United Kingdom, involving an even larger donation attempt of 16,000 euros.[24] Based on data collected for my Islamic State Worldwide Activity map, there have been 36 arrest cases globally related to jihadist use of cryptocurrency since 2015, with 13 of them happening in 2024 alone, illustrating a huge uptick in only the past year. And these are only the known cases that have come through the judicial system; many others may have gone undetected.

Beyond traditional American social media platforms, IS supporters have also made growing use of TikTok. This is not surprising since the platform has become ubiquitous among Gen Z. Although the trend likely began earlier, data from my Islamic State Worldwide Activity map shows that 15 arrest cases since 2023 have involved IS propaganda on TikTok, with suspects either sharing it themselves or watching it. Just last week, when Minneapolis resident Abdisatar Ahmed Hassan was arrested and charged for attempting to provide material support to IS, the investigation showed that he had praised the perpetrator of the New Orleans attack on TikTok on January 1.[25] Again, this highlights

---

[22] The Islamic State's Wilayat Khorasan, "Voice of Khorasan Magazine Issue #31," al-Azaim 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.

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

how one attack can inspire others to plot their own attacks or travel abroad to fight alongside IS in a war zone, as Hassan attempted to do in Somalia.

Terrorist might also attempt to exploit other technological options such as live streaming their attacks. For example, the New Orleans attack could have had an even greater psychological effect nationally if the perpetrator had live streamed the incident on his Meta glasses through Facebook instead of using the technology solely for reconnaissance. Yet such tactics are not unprecedented. Back in June 2016, when IS adherent Larossi Abballa attacked a French police captain and his partner, he broadcast the aftermath of the incident in real time on Facebook Live and remained online for almost twelve minutes.[26] The footage was taken down from Facebook eleven hours after it was recorded, but a copy was downloaded and later reposted via the official IS media outlet Amaq News Agency.

In addition, there are worries that terrorists could exploit Generative Artificial Intelligence (AI). Thus far, little evidence has emerged of jihadists attempting to use this technology for deadly ends, but that does not necessarily mean they won't do so in the future. For now, it has mainly been used by jihadist followers to generate online propaganda graphics that previously had to be created manually using software like Photoshop. This use of AI may appear to have lower stakes, but it has the important effect of lowering the bar for individuals to interact more deeply with IS ideology and produce extremist content, since auto-generating potent AI images doesn't require the same amount of skill, training, and time as crafting them in Photoshop. Moreover, a few weeks ago, IS supporters on Rocket.Chat began holding inchoate conversations about how they might exploit the Chinese AI application DeepSeek, though it is still too soon to speculate how that might evolve.[27]

Moderation Backsliding

Beyond the specifics of how terrorists might exploit technology, policies related to these platforms also have a role in providing space—or making it very difficult to use. As noted above, beginning in 2015, major technology companies made a much greater effort to moderate their platforms so that terrorists could not exploit them. While this moderation was in no way perfect in terms of curbing jihadists' online presence, it did decrease their usage of mainstream platforms to a degree that their propaganda was not noticeably reaching random people as easily as it had in 2013-15.

However, in recent years, due to political controversies related to alleged censorship in the West, there has been a backlash to moderating content even if it is extremist in nature. As a consequence, beginning with the shift from Twitter to X, the level of content moderation in general—and content moderation related to the jihadist movement specifically—has backslid.[28] This point should not be overblown, since jihadist content is not as widespread as it was in 2015 prior to the tech crackdown. Nevertheless, jihadists have gained relatively greater space to exploit such platforms in recent

---

[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.

[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.

years.[29] This is not just an issue with Twitter/X, but also with Meta platforms (including Facebook, Instagram, and WhatsApp) and the aforementioned TikTok. And unlike a decade ago, many of these capabilities are wielded by online networks of IS supporters, not at the group's 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 jihadist movement. In particular, beyond 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 jihadist movement online, including multiple languages in Africa and Central Asia.
- Although there have been recent calls to cut funding and jobs across the U.S. government, cutting ones related to tracking online jihadist recruitment and attack plotting could undermine future security and lead to greater risks at home and abroad. At a time when more resources are being put toward power competition and fewer toward counterterrorism, eliminating even more resources in this field could provide more opportunities for adversarial jihadists 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 who work on these sensitive issues so that their accounts do not get mistakenly taken down when actual terrorist accounts are targeted. This has been a problem in the past and should be resolved.[31]

---

[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*, vol. 18, no. 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*, vol. 15, no. 4, December 2023, https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.374.