Coalition for a
Safer Web

For Immediate Release:
February 3, 2025

Contact:
Amb. Marc Ginsberg, President
ambginsberg@coalitionsw.org
Adam Dubitsky, VP Communications
adam@coalitionsw.org, Tel: 202-922-6300

REPORT: ISIS AND AL-QAEDA DEPLOYING NEW AI PROGRAMS TO SURGE LONE WOLF ATTACKS AGAINST U.S. JEWISH COMMUNITY

INTRODUCTION

In the historic global competition for jihadi allegiance and supremacy waged between ISIS and Al Qaeda (AQ) the American Jewish community is a new battleground. Each terrorist group is surging web-based antisemitic incitement onto U.S. social media platforms frequented by Americans protesting Israel's Gaza campaign to incite terrorist attacks against Jews.

The Coalition for a Safer Web (CSW), a Washington-based nonprofit whose mission is to interdict and dismantle online radicalization and antisemitic incitement as well as their funding sources, penetrated these terrorist web media operations in recent weeks to assess the magnitude of the threat and to develop countermeasures.

Since mid-2024 ISIS and AQ have upgraded their propaganda operations by incorporating generative artificial intelligence (G-AI) programs. Readily accessible G-AI programs enhance and "superstylize" this inciting extremist web content. The G-AI programs also enable the terrorist groups to manipulate algorithms enabling each to breach existing social media content moderation barriers barring antisemitic incitement.

This emerging foreign-sourced antisemitic threat landscape along with recommendations to counter them are detailed in the CSW report published today.

CSW President Marc Ginsberg, a former US ambassador and noted cyber counter extremism expert stated:

> *"As if the American Jewish community does not have enough to worry from the antisemitic incitement of domestic far-left and far-right extremist groups, the flood of online AI-driven foreign radical Islamist terrorist group incitement specifically targeting Jews adds yet another ominous threat source that must be countered."*

REPORT

G-AI PROGRAMS HIJACKED BY ISIS & AL QAEDA TARGETING U.S. JEWS

Following the first anniversary of October 7 CSW researchers have discovered a mother lode of ISIS and Al Qaeda websites and accompanying splashy G-AI videos, programs, and memes, (many fictitious) of Gaza's destruction and injured Palestinians. The content is being manipulated to appeal to potential U.S. lone wolf recruits incited by videos and memes of Palestinian casualties to exact retribution against Israel's U.S. supporters (i.e., the Jewish community).

It should come as no surprise that open-source G-AI software is being hijacked by extremist and terrorist groups to professionalize and more precisely target their social media operations to reach their intended audiences. After all, the G-AI programs – including the newly minted Chinese DeepSeek AI program is freely available on app stores and AI programs' content-enabling guardrails are virtually non-existent.

CSW uncovered from both ISIS and AQ accounts what amount to "help wanted" ads to recruit AI software developers, AI video producers, and open-source AI experts. We have also intercepted an ISIS tech support guide on how to covertly use G-AI tools.

The off-the-shelf, readily available AI programs employed by ISIS and AQ have also enabled each group to produce G-AI-generated, western audience attuned news programs in Americanized English using voice cloning software from Eleven Labs, an AI-audio generation company. The videos created represent state-of-the-art production values for AI-sourced current event programs geared toward a younger, more persuadable demographic with the goal of inciting resentment by potential lone wolf terrorist attacks to avenge Gaza's Hamas terrorist and civilian casualties.

Unlike earlier Islamist online media used to incite violence and radicalize followers this G-AI content often has no identifiable ISIS or AQ branding or digital fingerprints. The advanced technology deployed also enables the terrorist groups to reach audiences via a human-like experience without the involvement of actual group members, thus protecting the on-line identities of operatives and freeing up live terrorists to undertake other missions.

Consequently, much of the content evades efforts to detect and block violent and terrorism-related content and allow extremists to create targeted propaganda, radicalize and target specific individuals for recruitment, and to incite violence.

Visit www.coalitionsw.org for examples of content identified by CSW researchers.

There are several reasons for the timing and targeting of the U.S. Jewish community:

1. Growing international anger against Israel and its supporters stemming from Israel's prosecution of the Gaza war provides a new U.S. recruiting ground and endless amounts of press and social media footage and and images of the conflict

for ISIS or AQ-inspired lone wolf attacks. Outbreaks of antisemitic violence in the West, particularly on campuses, have also become a fertile recruiting grounds for radical Islamic terror groups desiring to reach a new audience of potential U.S. recruits.

2. After the destruction of the ISIS-declared Syrian/Iraqi physical caliphate in 2018 and 2019, the group successfully reconstituted its franchise cells across the Middle East and sub-Saharan Africa. Currently, it is emboldened and better resourced to increase its global digital operations beyond the Middle East to promote terror attacks on Western targets.

3. Social media algorithms and content blocking technologies have not been retooled to intercept content disseminated and translated into English from the new regional dialects where ISIS operates.

4. The highly criticized withdrawal of U.S. forces from Afghanistan in 2021 emboldened the Afghan affiliate known as ISIS Khorsan, or ISIS-K, enabling it to "go global." This included ISIS-K's claimed responsibility for the March 2024 Moscow concert hall attack and the October 2024 FBI-foiled ISIS-K plot to stage a mass shooting on Election Day in Oklahoma, in which a 27-year-old Afghan migrant was arrested (see below).

5. "Honey Trap" social media platforms; namely TikTok, Instagram, X, and YouTube and others have slashed their content moderation efforts enabling ISIS and AQAP to upload and more easily vector their antisemitic incitement.

This "version 2.0" of the G-AI-enabled jihadi global ecosystem represents a "soup to nuts" enhanced cyber conveyor belt responsible for inciting a surge of terror plots against the U.S. Jewish targets since late 2024, most of which were thwarted, including:

- September 4, 2024 - The FBI and Canadian authorities arrested Muhammad Shahzeb Khan, 20, a Pakistani citizen residing in Canada on route, according to the FBI, to a planned a mass shooting in support of ISIS at a Jewish center in Brooklyn to coincide with the anniversary of the Hamas October 7 attack on Israel.

- October 8, 2024 – Federal agents in Oklahoma City arrested Nasir Ahmad Tawhedi, a 27-year-old Afghanistan national who, along with an unnamed juvenile, were reported to have been incited by ISIS online operatives to execute a terror attack on Election Day at an unspecified "mass gathering." Tawhedi saved ISIS propaganda on his iCloud and Google account, participated in pro-ISIS Telegram groups, and contributed to a charity which fronts for and funnels money to ISIS.

- October 18, 2024 – An Arizona teen, Marvin Aneer Jalo, 17, was arrested and charged as an adult for plotting an ISIS-inspired drone attack on the Phoenix Pride Festival parade, possibly as it passed by a Jewish community center. The

Maricopa County formal accusation stated his motive was to "further the goals" of the Islamic State.

- October 26, 2024 - Chicago police arrested a 22-year-old Sidi Mohammed Abdullahi for shooting a Jewish man on his way to synagogue and then turned his weapon on first responders. A Mauritanian national, Abdullahi had illegally entered the U.S. in 2023. He committed suicide in his jail in December.

- November 8, 2024 - The Houston FBI Counterterrorism Task Force arrested Anas Said, a 28-year-old Houston native, for conspiring with ISIS web designers to plot a mass casualty attack against a Houston Jewish installation.

- December 18, 2024 – An 18-year-old student at George Mason University in Virginia, Abdullah Ezzeldin Taha Mohamed Hassan, was arrested in connection with a plot inspired by ISIS content on X to stage a mass attack against the Israeli Consulate in New York City, and to prepare a "martyrdom video" and a live stream of the attack.

CAMOUFLAGING ISIS and AQ CYBER FINGERPRINTS

The camouflaged cyber content is also posted by ISIS and Al Qaeda media operatives onto "honeytrap" platforms -- so-designated to attract sympathizers from "bait" social media sites, including TikTok and Telegram. CSW researchers intercepted over a dozen TikTok accounts, notably that of an Abu Zajaawi that were "recommended" to us by TikTok on our TikTok account linking CSW to an ISIS Channel Al Ansar replete with anti-Israel and anti-Zionist content.

CSW researchers also uncovered what amount to "target identification packages," several videos containing geospatial photos of Jewish centers in New York, Miami, Chicago, and Detroit, as well as Sydney, Melbourne, and Toronto.

These ISIS and AQ sites fly under the radar of public and private U.S. content moderator watchdogs. With the assistance of G-AI the extremist sites obscure their identities and use AI to translate content from Arabic and Muslim world dialects into English and pushed onto English-language web platforms and chatbots with inciteful antisemitic content such as:

- ***RocketChat.com***: "RC" is a highly respected encrypted chat messaging platform with global public and private multinational clients. It provides seamless conferencing, messaging, and file sharing, etc. That ISIS has latched on to RC under a disguised front organization is no fault of RC. However, ISIS is using it to reach multi-lingual audiences with the aid of the encrypted Telegram app – a favored web waystation for users and radical Islamic groups.

- **JustPaste.I**t: JustPaste.It is another global web platform favored by the al-Saqri Foundation for Military Sciences, a notorious "how to commit terror" digitized library operated by ISIS. Al Saqri specializes in chemical and biological weapons instructions, bomb-making manuals, and ways to disable CCTV cameras. Although JustPaste. Its management is responsive to human flagging, it is not a social media platform, per se, but a web service and has no algorithmic capacity to keep pro-ISIS groups off it.

Al-Saqri has been successful in evading government efforts to shut down its web operations. Its digital operatives have mastered the art of bouncing from one stand-alone web operation to another without missing a beat. It maintains a stand-alone web archive to which prospective lone wolves are provided guided access. Encrypted Telegram "chatbots" amplify the content.

- **The ISIS *Ashhad Media Company* and the Sunni Shield Foundation**: CSW located its antisemitic content on a deep ISIS Telegram channel connected to these pro-ISIS content creation enterprises.

- **Doat al-Falah media organization**: "Doat" is an offshoot of ISIS's main media organization (Al Naba) concentrating on chatbot English engagement with popular gaming platforms such as Discord. Doat specializes in weapons training for would-be jihadists, such as how to construct a suppressor (silencer) on AR-15s. Doat content has been located by CSW on gaming sites such as Discord and its competitors, including Chanty, Slack, and Flock.

- **GazaTigers.net**: A media production outfit operated by Hamas out of Qatar. It provides media to various TikTok influencers. CSW located an on-line manual released by the site containing info how to fire a sniper rifle from a reinforced tailgate of a pickup truck as well as aerial maps of locations of the largest Jewish synagogues in the U.S.

- **GemSpace:** A new competitor to Telegram, is an encrypted call-to-call mobile phone application that is a "go-to" alternative to Telegram for ISIS and AQ.

- **Halummu**: The international Al Qaeda propaganda translation channel, has its own website and maintains a presence on Telegram, RC, Chipwire, and Scribd. Halummu often places content on the AQ-affiliated aligned Geo-News web platform into often encrypted, but penetrable terrorist archives. In November 2023, a Halummu graphic in English "Practical Ways to Support the Muslims in Palestine," called for the following:

  - "Target Jews living in America Europe and Rest of the World"
  - "Attack the Jewish and Crusader Embassies with fire and rain"
  - "Target Jewish temples synagogues spread everywhere"
  - "Attack Jewish nightclubs and their visitors with death"
  - "Target Jewish economic interests spread throughout the world"

ISIS & AQ UNVEILING NEW, SLICK ENGLISH-LANGUAGE PUBLICATIONS DESIGNED TO INCITE LONE WOLF ATTACKS

Several relatively unknown and anonymously published yet impactful G-AI enhanced innovations are offering how-to guides and tips for this new and improved cyber propaganda spear. These publications are tailored to appeal to a new, younger generation of disaffected western youth who have no direct and discernible ties to either terrorist group:

1. **THE WOLVES OF MANHATTAN**: A web publication created by a group of Al Qaeda in the Arabian Peninsula (AQAP) sympathizers called the ELECTRONIC BATTLE ARMY. Breaking from AQ custom, its latest edition offered bitcoin bounties to anyone who perpetrated an attack in the U.S., particularly Jews.
2. **MUJAHIDEEN IN THE WEST**: A web publication created by an AQAP sympathizer Abu Yahya al Kurasani intended to incite attacks in the U.S., and lately, against supporters of Israel. It regularly prints instructions on how to commit "low grade" terror attacks including vehicle rammings, kitchen table napalm formulas, tear gas formulas, and instructions how to print 3D guns.
3. **VOICE OF KHURASAN**: An English language ISIS publication advocating terrorist attacks in the west which provides detailed instructions from the ISIS Inspire publication how to commit various attacks.

CSW PROPOSALS TO COUNTER THIS THREAT

There are several public and private sector technology and policy measures that can be deployed to confront and neutralize this antisemitic offensive from jihadist terrorist groups.

Public Sector

The White House New Antisemitism Executive Order: The Trump Administration's very timely new Executive Order marshaling more federal resources to combat antisemitism should be interpreted by the White House to enable relevant agencies to undertake more targeted cyber content moderation due to the dangerous foreign sourced AQ and ISIS cyber threat targeting American Jews. CSW intends to leverage the Order's directives to work with the Trump Administration and Congress to compel relevant agencies re-establish intelligence-gathering web content programs focused on foreign-sourced antisemitic incitement.

Amend the definition of Terrorist "Material Support" Under U.S. laws it is illegal to provide "material support" to a foreign terrorist organization. Congress should consider amending existing legislation to expand the definition of "material" to include technology and software support enabling extremist and terrorist groups to incite domestic terrorism when U.S. and European vendors are notified their services are being used by US designated terrorist organizations but fail to terminate their relationship upon adequate notice from the U.S. government.

Congressional Investigation into U.S. Corporate Servicing ISIS & AQ: Congress should be encouraged to investigate U.S. corporate support of antisemitic and terrorist groups to "name and shame" companies to terminate these services leveraging anti-terrorism laws and regulations as a cudgel.

Private Sector

CSW also proposes several initial reasonable and cost-effective private sector-supporting measures to counter the growing threat:

Counter AI Programming Technology: Developing effective countermeasures to prevent and detect the misuse and abuse of G-AI supported platforms by terrorists and violent extremists need to be included in the national toolbox to enhance the security of the American Jewish community. CSW recommends forming a new ad-hoc partnership with state-of-the-art G-AI "jailbreak" experts associated with the Combating Terrorism Center of West Point, the Global Internet Center to Combat Terrorist (GIFCT), MIT, and The University California/Berkeley School of Electrical Engineering and Computer Sciences. CSW is particularly eager to collaborate with G-AI scientists to develop antisemitic cyber "Jailbreaks."

In cyber parlance "jailbreaks" are computer code-generated phrases developed by counterterrorism experts that attempt to bypass an AI model's ethical safeguards and elicit prohibited information. It uses creative prompts in plain language to trick G-AI systems into releasing information that their content filters would otherwise block. This initiative would enable counter-antisemitism web watchdogs to keep testing and proposing upgrades to G-AI embedded safeguards against antisemitic plots.

As best as CSW can tell there is no public or private G-AI enterprise whose principal mission is to fill the gap created by the severe curtailment of content moderation programs by popular social media platforms to counter antisemitism and jihadist terror incitement.

No legacy Jewish organization, not the ADL, the AJC, or the Community Security Network, maintain in-house capabilities to adequately identify, interdict, and act against the antisemitic, jihadi-inspired G-AI content.

Social Media Early Warning Center: The dangerous erosion of cyber threat monitoring is a challenge that must be filled. CSW recommends creating an antisemitism-focused *Social Media Early Warning Center*, a privately-run fusion center, to monitor in real time and act against cyber threats to the Jewish community. Ceding the web battlefield to terrorist groups which have seized upon sophisticated AI is, simply put, an unnecessary and reversible surrender to antisemitic terrorism.

De-weaponizing "bait" platforms: Mainstream social media platforms serving as "honeytraps" to recruit antisemitic lone wolves must be tackled:

- **TikTok**: US government conditions imposed on the sale of TikTok to a U.S. entity by ByteDance should include a provision demanding a quantifiable level of content moderation programming to substantially neutralize foreign & domestic sourced terrorist incitement, including foreign-sourced antisemitic incitement.

- **Telegram:** Last year France placed Pavel Durov -- Telegram's owner -- under house arrest for violating laws prohibiting Telegram from supporting illicit groups, such as ISIS and AQ. Congress and the Trump Administration should call on French authorities to demand Durov provide explicit and robust real-time content moderation standards verifiable by France, the EU, and the U.S. to curtail antisemitic and pro-Jihadi content on Telegram. Telegram was compelled to sanitize its site of Islamist content by the EU in 2015. Telegram's content moderation worked then. It can be resuscitated again now that the France has Durov under arrest.

National Corporate Advocacy Campaign: While AI software is globally available – too many U.S. companies unwittingly provide global antisemitic and terrorist groups "back of the house" technology and software support, such as access to anonymous cloud storage capacities necessary by ISIS and AQ to vector its antisemitic incitement. The extensive list includes major U.S. and European companies such as Cloudflare, RocketChat, and Eleven Labs, to name a few.

END

For additional information and examples of researched content referenced in this report visit www.coalitionsw.org

About: The Coalition for a Safer Web is a non-partisan non-profit foundation that exposes and counters online extremist activity and its funding.

About Ambassador Marc Ginsberg**:** Founding President of CSW, is one of the nation's leader experts on cyberterrorism and social media-fueled extremist violence. He was former White House Mideast Advisor to President Carter and a former U.S. ambassador to Morocco.

For more information or interviews contact: Adam Dubitsky, adam@coalitionsw.org, 202-922-6300 or Marc Ginsberg, ambginsberg@coalitionsw.org.

# # #